HEC MONTRÉAL

Mieux comprendre l'influence de la culture et du climat organisationnels sur les pratiques en sécurité de l'information

par

Cindy Nguyen

Sciences de la gestion

(Option Technologies de l'Information)

Mémoire présenté en vue de l'obtention du grade de maîtrise ès sciences en gestion

(M.Sc.)

Août 2017

© Cindy Nguyen, 2017

HEC MONTRÉAL

Comité d'éthique de la recherche

CERTIFICAT D'APPROBATION ÉTHIQUE

La présente atteste que le projet de recherche décrit ci-dessous a fait l'objet d'une évaluation en matière d'éthique de la recherche avec des êtres humains et qu'il satisfait aux exigences de notre politique en cette matière.

Projet # : 2017-2305

Titre du projet de recherche : Mieux comprendre la culture de la sécurité de l'information : Définition et mesure

Chercheur principal :
Cindy Nguyen, étudiante M. Sc.
HEC Montréal

Directeur/codirecteurs :
Alina-Maria Dulipovici; Line Dubé
Professeures - HEC Montréal

Date d'approbation du projet : 15 juin 2016

Date d'entrée en vigueur du certificat : 15 juin 2016

Date d'échéance du certificat : 01 juin 2017

Maurice Lemelin
Président du CER de HEC Montréal

HEC MONTRÉAL

Comité d'éthique de la recherche

ATTESTATION D'APPROBATION ÉTHIQUE COMPLÉTÉE

La présente atteste que le projet de recherche décrit ci-dessous a fait l'objet des approbations en matière d'éthique de la recherche avec des êtres humains nécessaires selon les exigences de HEC Montréal.

La période de validité du certificat d'approbation éthique émis pour ce projet est maintenant terminée. Si vous devez reprendre contact avec les participants ou reprendre une collecte de données pour ce projet, la certification éthique doit être réactivée préalablement. Vous devez alors prendre contact avec le secrétariat du CER de HEC Montréal.

Projet # : 2017-2305 **-** ISC2016

Titre du projet de recherche : Mieux comprendre la culture de la sécurité de l'information : Définition et mesure

Chercheur principal :
Cindy Nguyen

Directeur/codirecteurs :
Line Dube;
Alina-Maria Dulipovici

Date d'approbation initiale du projet : 15 juin 2016

Date de fermeture de l'approbation éthique : 25 juillet 2017

Maurice Lemelin
Président du CER de HEC Montréal

Sommaire

Avec l'accroissement des incidents informatiques dans les organisations, la sécurité de l'information occupe une place grandissante au sein de ces dernières. Afin de contrer ces incidents informatiques, les organisations offrent des programmes de formation et de sensibilisation à la sécurité de l'information à leurs employés. Cependant, l'efficience de ces programmes est largement questionnée car les employés demeurent la principale source d'incidents en sécurité de l'information.

Ainsi, pour avoir une influence à plus long terme les comportements des employés, les organisations doivent développer une culture et un climat de la sécurité de l'information. Ces deux composantes du contexte organisationnel exercent de manière conjointe une forte influence sur les actions des employés et pourraient, au final, les influencer à mettre en œuvre des pratiques sécuritaires.

Si les milieux scientifiques et pratiques s'accordent sur l'importance de cette culture et de ce climat de la sécurité de l'information, les construits demeurent encore flous à bien des égards. Par conséquent, ce mémoire vise donc, dans un premier temps à définir et à conceptualiser la culture et le climat de la sécurité de l'information et des éléments qui les composent. Dans un deuxième temps, il est question de déterminer, avec complétude et parcimonie, les éléments de la culture et du climat de la sécurité de l'information les plus susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés d'une organisation. Ce mémoire présente donc une conceptualisation de la culture et du climat de la sécurité de l'information, qui a fait l'objet d'un processus de validation auprès de professionnels en sécurité de l'information et permet d'informer des éléments du contexte organisationnel à prendre en compte et qui sont les plus susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés.

Mots-clés : culture de la sécurité de l'information, climat de la sécurité de l'information, pratiques en sécurité de l'information, croyances, valeurs, caractéristiques du climat.

Remerciements

Tout d'abord, je tiens à remercier mes directrices, Line Dubé et Alina Dulipovici, pour leur dévouement, leur soutien et leur patience à travers toutes les étapes de ma rédaction. Elles m'ont appris l'importance de la rigueur en recherche, et leurs précieux commentaires, leurs conseils et leurs idées me furent d'une grande aide et m'ont permis de me dépasser. Je m'estime extrêmement chanceuse d'avoir pu travailler avec des personnes aussi exceptionnelles. Les mots ne suffisent pas à exprimer l'admiration et l'immense gratitude que j'éprouve envers elles.

Je souhaite remercier Henri Barki et Suzanne Rivard, mes professeurs lors de l'atelier de recherche, pour leurs commentaires. J'aimerais également remercier les professeurs du département des technologies de l'information à HEC Montréal, qui, du baccalauréat à la maîtrise, m'ont tant appris et m'ont transmis leur passion pour notre domaine de prédilection. Je remercie également les trois professeurs qui ont accepté de faire partie du comité d'évaluation de ce mémoire.

Je suis aussi reconnaissante envers les répondants ayant accepté de participer à cette étude. Ils furent d'une grande générosité et n'ont pas hésité à m'accorder leur temps et à partager leurs expériences professionnelles avec moi. À travers nos échanges, j'ai pu me familiariser avec le domaine, répondre à ma problématique de recherche, mais aussialimenter la passion grandissante que je porte pour la sécurité de l'information.

Un grand merci à Andréanne Ostiguy, pour sa précieuse aide, ses conseils, ses relectures à la dernière minute, mais surtout pour sa gentillesse et ses mots d'encouragement. Je suis particulièrement reconnaissante envers ma famille, mes amis, et mes collègues pour leurs encouragements, leur présence au cours de ce travail de longue haleine. Enfin, je remercie particulièrement ma mère, Camille, Walter, Fleur, Danilo, Benoit et Emmanuelle; votre soutien moral me fut indispensable.

Table des matières

SOMMAIRE ..... **V**

REMERCIEMENTS ..... **VI**

LISTE DES FIGURES ..... **X**

LISTE DES TABLEAUX ..... **XI**

CHAPITRE 1 : INTRODUCTION **1**

1.1 Problématique **1**

1.2 Objectif et questions de recherche **3**

1.3 Structure du mémoire **5**

CHAPITRE 2 : REVUE DE LITTÉRATURE **7**

2.1 L'objectif visé : expliquer la mise en œuvre de pratiques sécuritaires par les employés **8**
2.1.1 Les objectifs des organisations en matière de sécurité de l'information 8
2.1.2 La mise en œuvre de pratiques sécuritaires par les employés : une définition 9

2.2 La culture et le climat organisationnels : sources d'influence de la mise en œuvre de pratiques sécuritaires par les employés **13**
2.2.1 La culture de la sécurité de l'information 14
2.2.1.1 Définitions de la culture de la sécurité de l'information tirées de la littérature 15
2.2.1.2 Culture de la sécurité de l'information : définition proposée 17
2.2.1.3 Les valeurs et les croyances au cœur de la culture organisationnelle 19
2.2.1.4 Les croyances et les valeurs de la culture de la sécurité de l'information susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés 21
2.2.2 Le climat de la sécurité de l'information 40
2.2.2.1 Définitions du climat de la sécurité de l'information telles que retrouvées dans la littérature 40
2.2.2.2 Le climat de la sécurité de l'information: définition proposée 42
2.2.2.3 Les caractéristiques du climat organisationnel 43

2.3 Les autres concepts du domaine de la sécurité de l'information pouvant enrichir notre compréhension des croyances, des valeurs et des caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés **57**

2.4 La culture et le climat organisationnels et leur influence sur la mise en œuvre de pratiques sécuritaires par les employés : le modèle initial **58**

CHAPITRE 3 : MÉTHODOLOGIE **79**

3.1 Étape A : Prétest – Rencontres individuelles avec des étudiants de la M.Sc. **79**

3.1.1 Cueillette des données....79
3.1.2 Analyse des données et résultats....81

3.2 Étape B : Rencontre avec un groupe de professionnels en sécurité de l'information – groupe de discussion....82
3.2.1 Cueillette des données....83
3.2.2 Analyse des données et résultats....85

3.3 Étape C : Rencontres individuelles avec des professionnels en sécurité de l'information....87
3.3.1 Cueillette des données....87
3.3.2 Analyse des données....88
3.3.2.1 Analyse des classements....88
3.3.2.2 Analyse des propos recueillis....89

3.4 Récapitulatif de l'approche méthodologique....91

CHAPITRE 4 : RESULTATS....93

4.1 Croyances : résultats et analyses....93
4.1.1 Croyances : résultats et analyses individuelles....94
4.1.1.1 Croyance #1 : Responsabilité d'assurer la sécurité de l'information....94
4.1.1.2 Croyance #2 : Vision de l'organisation quant à la nature des défis en termes de sécurité de l'information....100
4.1.1.3 Croyance #3 : Importance générale qu'a la sécurité de l'information dans l'organisation 104
4.1.1.4 Croyance #4 : Auto-efficacité organisationnelle face aux menaces....107
4.1.1.5 Croyance #5 : Responsabilité morale de protéger l'information....111
4.1.1.6 Croyance #6 : Nature générale de l'être humain....115
4.1.1.7 Croyance #7 : Le maillon faible en sécurité de l'information....121
4.1.2 Croyances : Analyse globale et décisions....128

4.2 Valeurs : résultats et analyses....132
4.2.1 Valeurs : résultats et analyses individuelles....132
4.2.1.1 Valeur #1 : Bases générales sur lesquelles les décisions sont prises dans l'organisation 132
4.2.1.2 Valeur #2 : Horizon temporel habituel de la planification dans l'organisation....140
4.2.1.3 Valeur #3 : Prédispositions éthiques dans l'organisation....144
4.2.1.4 Valeur #4 : Attitude des employés envers la conformité....148
4.2.1.5 Valeur #5 : Importance accordée au développement des ressources humaines....151
4.2.1.6 Valeur #6 : Attitude générale des employés face au changement....156
4.2.1.7 Valeur #7 : Force du réseau au sein de l'organisation....160
4.2.1.8 Valeur #8 : Réaction habituelle de l'organisation face aux problèmes....165
4.2.1.9 Valeur #9 : Réponse habituelle de l'organisation face aux pressions externes....171
4.2.10 Valeur #10 : Imputabilité....176
4.2.2 Valeurs : Analyse globale et décisions....180

4.3 Caractéristiques du climat : résultats et analyses....183
4.3.1 Caractéristiques du climat : résultats et analyses individuelles....183
4.3.1.1 Caractéristique du climat #1 : Soutien projeté par les gestionnaires....183
4.3.1.2 Caractéristique du climat #2 : Communication organisationnelle....188
4.3.1.3 Caractéristique du climat #3 : Soutien à l'apprentissage....193
4.3.1.4 Caractéristique du climat #4 : Implication des employés....198
4.3.1.5 Caractéristique du climat #5 : Adéquation au contexte organisationnel....202
4.3.1.6 Caractéristique du climat #6 : Adéquation aux tâches....207
4.3.1.7 Caractéristique du climat #7 : Engagement organisationnel....212

4.3.1.8 Caractéristique du climat #8 : Communication des problèmes/erreurs 216
4.3.1.9 Caractéristique du climat #9 : Récompenses/sanctions 221
4.3.1.10 Caractéristique du climat #10 : Façon dont le monitorage du respect des pratiques de sécurité se fait 229
4.3.1.11 Caractéristique du climat #11 : Importance réelle accordée à la sécurité de l'information 235
4.3.2 Caractéristiques du climat : Analyse globale et décisions 239

4.4 Résultat final de l'analyse des données 244

CHAPITRE 5 : DISCUSSION 248

5.1 Vers une meilleure compréhension de la culture et du climat de la sécurité de l'information 248
5.1.1 Éléments de la culture et du climat organisationnels retenus 248
5.1.2 Éléments de la culture et du climat organisationnels non retenus 255

CHAPITRE 6 : CONCLUSION 260

6.1 Rappel des questions de recherche 260

6.2 Rappel de la démarche méthodologique adoptée 260

6.3 Synthèse des principaux résultats 261

6.4 Contributions pratiques et théoriques du mémoire 262
6.4.1 Contributions théoriques 262
6.4.2 Contributions pratiques 263

6.5 Limites de la recherche 263

6.6 Pistes de recherche future 264

BIBLIOGRAPHIE 266

ANNEXES 272
Annexe 1 : Examen des autres concepts du domaine de la sécurité de l'information 272
Annexe 2 : Protocole A - Rencontres individuelles avec les étudiants de la M.Sc. 317
Annexe 3 : Protocole B – Groupe de discussion avec experts en sécurité de l'information 320
Annexe 4 : Protocole C – Rencontres individuelles avec les professionnels en sécurité de l'information 323
Annexe 5 : Cartes des exercices de priorisation de l'étape B 326
Annexe 6 : Cartes des exercices de priorisation de l'étape C 334

Liste des figures

Figure 2.1 : Influence des deux composantes du contexte organisationnel sur la variable dépendante 14
Figure 2.2 : L'influence des croyances et des valeurs sur la mise en œuvre de pratiques sécuritaires 20
Figure 2.3 : L'influence des caractéristiques du climat sur la mise en œuvre de pratiques sécuritaires par les employés 44
Figure 2.4 : La culture organisationnelle et le climat organisationnel comme sources d'influence de la mise en œuvre de pratiques sécuritaires par les employés 59
Figure 3.1 : Exemple d'enveloppe utilisée pour l'exercice de triage de l'étape A 80
Figure 3.2 : Exemple de carte utilisée pour l'exercice de triage de l'étape A 81
Figure 3.3 : Exemple de carte utilisée lors d'un exercice de priorisation de l'étape B 84
Figure 3.4 : Exemple de carte utilisée lors d'un exercice de priorisation de l'étape C 88
Figure 4.1 : Score obtenu pour chacune des croyances suite à l'ensemble des classements 128
Figure 4.2 : Score obtenu pour chacune des valeurs suite à l'ensemble des classements 181

Liste des tableaux

Tableau 2.1 : Variables utilisées dans la littérature en lien avec la mise en œuvre de pratiques sécuritaires par les employés 10
Tableau 2.2 : Définitions de la culture de la sécurité de l'information issues de la littérature 15
Tableau 2.3 : Les croyances susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés 24
Tableau 2.4 : Les valeurs susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés 31
Tableau 2.5 : Définitions du climat de la sécurité de l'information de la littérature 41
Tableau 2.6 Les caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires 46
Tableau 2.7 : Les croyances susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés 61
Tableau 2.8 : Les valeurs susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés 65
Tableau 2.9 : Les caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés 71
Tableau 3.1 : Résumé de l'approche méthodologie 88
Tableau 4.1 : Résultats (classements, points et commentaires) obtenus pour la croyance #1 96
Tableau 4.2 : Tableau des fréquences pour la croyance #1 99
Tableau 4.3 : Résultats (classements, points et commentaires) obtenus pour la croyance #2 101
Tableau 4.4 : Tableau des fréquences pour la croyance #2 103
Tableau 4.5 : Résultats (classements, points et commentaires) obtenus pour la croyance #3 105
Tableau 4.6 : Tableau des fréquences pour la croyance #3 106
Tableau 4.7 : Résultats (classements, points et commentaires) obtenus pour la croyance #4 108
Tableau 4.8 : Tableau des fréquences pour la croyance #4 110
Tableau 4.9 : Résultats (classements, points et commentaires) obtenus pour la croyance #5 112
Tableau 4.10 : Tableau des fréquences pour la croyance #5 114
Tableau 4.11 : Résultats (classements, points et commentaires) obtenus pour la croyance #6 116
Tableau 4.12 : Tableau des fréquences pour la croyance #6 120
Tableau 4.13 : Résultats (classements, points et commentaires) obtenus pour la croyance #7 122
Tableau 4.14 : Tableau des fréquences pour la croyance #7 126
Tableau 4.15 : Fusion des croyances #1 et #2 129
Tableau 4.16 : Résultats (classements, points et commentaires) obtenus pour la valeur #1 134
Tableau 4.17 : Tableau des fréquences pour la valeur #1 137
Tableau 4.18 : Résultats (classements, points et commentaires) obtenus pour la valeur #2 141
Tableau 4.19 : Tableau des fréquences pour la valeur #2 143
Tableau 4.20 : Résultats (classements, points et commentaires) obtenus pour la valeur #3 145
Tableau 4.21 : Tableau des fréquences pour la valeur #3 147
Tableau 4.22 : Résultats (classements, points et commentaires) obtenus pour la valeur #4 149
Tableau 4.23 : Tableau des fréquences pour la valeur #4 150
Tableau 4.24 : Résultats (classements, points et commentaires) obtenus pour la valeur #5 152
Tableau 4.25 : Tableau des fréquences pour la valeur #5 154
Tableau 4.26 : Résultats (classements, points et commentaires) obtenus pour la valeur #6 157
Tableau 4.27 : Tableau des fréquences pour la valeur #6 158
Tableau 4.28 : Résultats (classements, points et commentaires) obtenus pour la valeur #7 161
Tableau 4.29 : Tableau des fréquences pour la valeur #7 163
Tableau 4.30 : Résultats (classements, points et commentaires) obtenus pour la valeur #8 166
Tableau 4.31 : Tableau des fréquences pour la valeur #8 169

Tableau 4.32 : Résultats (classements, points et commentaires) obtenus pour la valeur #9 172
Tableau 4.33 : Tableau des fréquences pour la valeur #9 174
Tableau 4.34 : Résultats (classements, points et commentaires) obtenus pour la valeur #10 177
Tableau 4.35 : Tableau des fréquences pour la valeur #10 179
Tableau 4.36 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #1 185
Tableau 4.37 : Tableau des fréquences pour la caractéristique du climat #1 186
Tableau 4.38 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #2 190
Tableau 4.39 : Tableau des fréquences pour la caractéristique du climat #2 192
Tableau 4.40 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #3 194
Tableau 4.41 : Tableau des fréquences pour la caractéristique du climat #3 196
Tableau 4.42 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #4 199
Tableau 4.43 : Tableau des fréquences pour la caractéristique du climat #4 201
Tableau 4.44 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #5 204
Tableau 4.45 : Tableau des fréquences pour la caractéristique du climat #5 206
Tableau 4.46 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #6 209
Tableau 4.47 : Tableau des fréquences pour la caractéristique du climat #6 211
Tableau 4.48 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #7 213
Tableau 4.49 : Tableau des fréquences pour la caractéristique du climat #7 215
Tableau 4.50 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #8 218
Tableau 4.51 : Tableau des fréquences pour la caractéristique du climat #8 220
Tableau 4.52 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #9 223
Tableau 4.53 : Tableau des fréquences pour la caractéristique du climat #9 227
Tableau 4.54 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #10 230
Tableau 4.55 : Tableau des fréquences pour la caractéristique du climat #10 233
Tableau 4.56 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #11 236
Tableau 4.57 : Tableau des fréquences pour la caractéristique du climat #11 237
Tableau 4.58 : Fusion des caractéristiques du climat #5 et #6 242

Chapitre 1 : Introduction

1.1 Problématique

La sécurité de l'information occupe une place grandissante au sein des organisations. Et pour cause, la sécurité de l'information est, depuis quelques années, considérée comme étant l'une des principales priorités des organisations (Gartner, 2017). Cette tendance tire son origine de l'accroissement du nombre de brèches de données et des coûts faramineux qui leur sont associés. Au Canada seulement, le nombre de brèches de données rapportées a augmenté de 160 % entre 2015 et 2016 (PricewaterhouseCoopers, 2016). De plus, le coût que représente désormais une brèche de données s'élève en moyenne à 4 millions de dollars américains (Ponemon Institute, 2016).

L'objectif fondamental des organisations en sécurité de l'information, qui est de protéger l'information de l'accès, de l'utilisation, de la divulgation, de la modification et de la destruction non-autorisés (Bernard, 2007; Mellado et al., 2010), est mis à mal par les employés, car ils constituent la première source d'incidents touchant la sécurité de l'information. En effet, dans le rapport de PricewaterhouseCoopers (2016), 66 % des répondants ont déclaré que la majorité des brèches de données était attribuée à l'erreur humaine, car les employés ne mettent pas en œuvre les pratiques sécuritaires (par exemple, la non-divulgation de mot de passe du compte utilisateur, le verrouillage d'un poste de travail inutilisé, etc.) définies par leur organisation. De ce fait, la non-mise en œuvre des pratiques sécuritaires par les employés constituent encore un défi de taille pour les organisations (D'Arcy & Greene, 2014) puisque les employés demeurent au cœur des incidents liés à la sécurité de l'information dans les organisations (Da Veiga & Martins, 2015; Van Loenen, 2015). Étant critique pour assurer la sécurité de l'information, le fait de mieux comprendre la mise en œuvre de pratiques sécuritaires par les employés d'une organisation représente le point central de ce mémoire.

Afin d'encourager les employés à mettre en œuvre des pratiques sécuritaires, les organisations ont recours à des programmes de sensibilisation à la sécurité de l'information puisqu'ils sont traditionnellement considérés comme le moyen le plus efficace pour contrer les risques humains en matière de sécurité de l'information (Spears & Barki, 2010; Parsons et al., 2010). Cependant, l'efficience de ces programmes est maintenant largement questionnée puisque, malgré les nombreux programmes de sensibilisation ou de formation donnés en entreprise, les employés sont encore la principale source d'incidents de sécurité (Da Veiga & Martins, 2015; Van Loenen, 2015).

Pour avoir une influence à plus long terme sur les comportements des employés, il s'avère pertinent de se pencher davantage sur le rôle que peuvent jouer la culture et le climat organisationnels, deux composantes importantes du contexte organisationnel (Denison, 1996). En effet, la culture et le climat organisationnels exercent conjointement une très forte influence sur les actions et les comportements des employés (Schneider & Barbera, 2014). D'une part, la culture organisationnelle est un ensemble de manifestations visibles et non-visibles (Martin, 1992). Les manifestations visibles font non seulement référence à des artefacts tels que le code vestimentaire, les histoires ou encore les rituels, mais aussi à des pratiques formelles et informelles, qui comprennent par exemple, les règles comportementales et les normes. Les manifestations invisibles sont composées des valeurs, des croyances et des hypothèses que se sont appropriées les employés de l'organisation. Pour ce qui est du climat organisationnel, il correspond aux perceptions partagées au sein de l'organisation quant aux politiques organisationnelles, aux règles, aux normes et aux pratiques, formelles et informelles. Le climat organisationnel représente les perceptions partagées par les employés à propos de « comment les choses se passent chez nous » (James & Jones, 1974; Reichers & Schneider, 1990). Ce mémoire ne traite pas de l'intégralité de la culture et du climat organisationnels, mais vise plutôt à examiner les facettes de la culture et du climat organisationnels qui sont susceptibles d'influencer, positivement ou négativement, la mise en œuvre de pratiques sécuritaires par les employés au sein de l'organisation.

En effet, si la culture organisationnelle et le climat organisationnel influencent les actions et les comportements des employés, il est dès lors nécessaire de mieux les comprendre afin d'évaluer leur rôle pour appuyer la mise en œuvre des pratiques liées à la sécurité de l'information (Goo et al., 2013; Tang et al., 2015). En effet, une culture et un climat organisationnels qui font la promotion des comportements positifs envers la sécurité de l'information dans la routine quotidienne de l'organisation pourraient être bien plus efficaces qu'une régulation qui dicte les comportements à adopter (Alhogail, 2015; Herath & Rao, 2009). Néanmoins, peu d'organisations ont une idée précise de la nature et du rôle que peuvent jouer la culture et le climat en sécurité de l'information. Sans cette compréhension accrue, il est difficile, d'abord, de comprendre, et ensuite de poser des actions qui permettent de favoriser un contexte organisationnel qui soit propice à la mise en œuvre de pratiques sécuritaires (Chan et al., 2005; Da Veiga & Eloff, 2010). Par ailleurs, il faut noter que, dans la littérature scientifique et pratique, les écrits font souvent usage des expressions « culture de la sécurité de l'information » et « climat de la sécurité de l'information ». Pourtant, la culture et le climat de la sécurité de l'information sont indissociables de ce que constitue la culture de l'entreprise et le climat régnant dans l'organisation. En raison de leur popularité et afin d'alléger le texte, les

deux expressions seront employées tout au long de ce mémoire, mais dans le but précis de référer aux facettes de la culture et du climat organisationnels qui influencent les comportements en matière de sécurité de l'information.

La littérature demeure confuse à bien des égards et ne permet pas d'offrir une conceptualisation claire de chacun des points d'intérêt de ce mémoire. Premièrement, parmi les chercheurs, il y a peu de consensus quant à l'objectif final de la sécurité de l'information que vise le contexte organisationnel, à savoir la mise en œuvre de pratiques sécuritaires par les employés. En effet, dans la littérature, on constate une difficulté à identifier et à définir ce que doivent faire les employés afin de protéger l'information de l'organisation. Deuxièmement, la compréhension de la culture et du climat organisationnels ne fait pas l'uninamité dans la littérature, d'autant plus que cela est également notable lorsque l'on parle de culture et de climat de la sécurité de l'information. En somme, les points d'intérêt de ce mémoire souffrent d'un problème de conceptualisation puisqu'ils ne sont ni définis clairement, ni mesurés. Cela apporte son lot de problèmes, autant dans la recherche que dans la pratique. Sans une conceptualisation précise, il est difficile de bâtir une compréhension élargie de ces construits et de comparer les résultats d'une étude à l'autre. Au final, il devient alors difficile de bâtir une base de connaissances étendues établie sur des bases solides. Pour la pratique, ce problème de conceptualisation mène à la difficulté de savoir quel est l'objectif recherché en sécurité de l'information. D'une part, on peut se demander comment influencer la mise en œuvre de pratiques sécuritaires par les employés. D'autre part, si on ne s'entend pas sur ce que sont une culture et un climat de la sécurité de l'information, il est en effet difficile d'évaluer si les moyens et les pratiques mis en place en font ou non la promotion et si, au final, celle-ci est essentielle en plus d'être un aspect important pour protéger la confidentialité, l'intégrité et la disponibilité de l'information (Da Veiga & Martins, 2015).

Ainsi dans un premier temps, afin de paver le chemin vers une compréhension accrue du rôle du contexte organisationnel dans la mise en œuvre de pratiques sécuritaires pour diminuer le nombre d'incidents de sécurité au sein des organisations, il s'avère pertinent de conceptualiser de la culture et du climat de la sécurité de l'information de façon valide et rigoureuse.

1.2 Objectif et questions de recherche

L'objectif de la présente étude est d'investiguer deux composantes du contexte organisationnel qui sont susceptibles d'inflluencer la mise en oeuvre des pratiques sécuritaires en matière de sécurité de l'information par les employés au sein des organisations. Plus précisément, cette étude cherche à conceptualiser la culture de la sécurité de l'information et le climat de la

sécurité de l'information. Cette conceptualisation inclut une définition des construits étudiés et a pour optique d'identifier de manière à la fois complète et parcimonieuse tous les éléments qui les composent et qui sont susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés dans l'organisation.

En exploitant au maximum la connaissance reliée à la culture de la sécurité de l'information, une nouvelle conceptualisation est présentée dans ce mémoire. Cette conceptualisation, observant les principes de complétude et de parcimonie, permet alors de répondre à la question de recherche suivante :

1. ***Quels sont les éléments de la culture organisationnelle les plus susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés dans l'organisation ?***

Le même traitement sera apporté à la nouvelle conceptualisation du climat de la sécurité de l'information et permettra de répondre à la question de recherche qui suit :

2. ***Quelles sont les caractéristiques du climat organisationnel qui sont les plus susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés dans l'organisation ?***

Il faut noter que les réponses à ces deux questions représentent la première étape dans le processus de développement d'un instrument de mesure (MacKenzie et al., 2011). L'objectif initial de ce mémoire était le développement d'un instrument de mesure permettant de mesurer les caractéristiques du contexte organisationnel susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés. Or, rapidement, la caractérisation du contexte a mené aux construits très complexes de culture et de climat organisationnels. En poursuivant l'objectif initial, les résultats du premier prétest, dont il sera question dans le chapitre 3, ont tout de suite démontré qu'il était beaucoup trop tôt dans le processus de développement d'un instrument pour en arriver à un instrument valide et fiable. Il a donc été décidé d'investir plus d'efforts à la première étape du processus de développement d'un instrument, soit la conceptualisation des construits à mesurer. Dès lors, l'objectif du présent mémoire a été ajusté afin que tous les efforts soient dédiés à cette première étape, et de cet ajustement, découlent les deux nouvelles questions de recherche présentées.

Ainsi, pour répondre à ces deux questions, la littérature du domaine de la sécurité de l'information ainsi que les littératures connexes ont été recensées et ont fait l'objet d'une analyse détaillée afin de relever tous les éléments de la culture et du climat organisationnels susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés. Une fois

relevés dans la littérature, ces éléments ont été illustrés avec des définitions, des propositions et des items, dans le but de mieux en comprendre le sens. Suite à quoi des professionnels en sécurité de l'information ont non seulement validé la complétude de cette liste, mais en ont aussi priorisé le contenu en indiquant les éléments qui, selon eux, étaient les plus susceptibles d'influencer la mise en oeuvre des pratiques sécuritaires par les employés. Au final, le livrable est un modèle dans lequel on retrouve la liste, à la fois complète et parcimonieuse, des éléments de la culture organisationnelle (les croyances et les valeurs) et des caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés au sein d'une organisation.

Ce mémoire contribue à l'avancement des connaissances dans le domaine puisque la littérature scientifique et professionnelle est confuse et anecdotique lorsqu'il est sujet de la culture et du climat de la sécurité de l'information. Dans la littérature scientifique, peu d'auteurs se sont essayés à la conceptualisation de la culture et du climat de l'information. À cela s'ajoute le fait que leurs travaux s'avèrent limités car leur conceptualisation se restreint à un fragment de la culture et du climat de la sécurité de l'information. Le mémoire vise donc à pallier les limites de ces écrits en proposant une conceptualisation plus complète de ces construits, qui a fait l'objet d'un processus de validation auprès de professionnels en sécurité de l'information. Ainsi, cette conceptualisation représente un premier pas vers le développement d'un instrument de mesure de la culture et du climat de la sécurité de l'information. En ce qui concerne la pratique, à ce point-ci, les résultats de ce mémoire représentent un outil de réflexion qui peut aider les professionnels en sécurité de l'information dans leur compréhension de ce qui est susceptible d'influencer la mise en œuvre de pratiques sécuritaires par leurs employés. Ces résultats pourront aider ces professionnels à déterminer un point de référence en termes de culture et de climat de la sécurité de l'information, en leur exposant les éléments déterminants constituant ces deux contruits.

1.3 Structure du mémoire

La suite de ce mémoire s'articule autour de cinq chapitres. Le chapitre 2 permet de présenter comment la culture et le climat de la sécurité de l'information sont présentement conceptualisés dans la littérature, mais permet aussi de relever les connaissances pour établir une conceptualisation plus complète de ces construits. Ce chapitre se clôt sur la présentation du modèle initial (qui représente l'influence de la culture et du climat organisationnels sur la variable dépendante, soit la mise en œuvre de pratiques sécuritaires par les employés). Le chapitre 3 aborde la méthodologie employée dans le cadre de ce mémoire. Il explique le déroulement du prétest auprès d'étudiants de la M.Sc., du groupe de discussion et des entrevues

individuelles auprès des professionnels de la sécurité de l'information afin de valider la conceptualisation qui découle du chapitre 2. Le chapitre 4 présente l'analyse des données recueillies au cours des entrevues individuelles, l'étape principale de collecte des données. Ces résultats sont par la suite discutés dans le chapitre 5. Enfin, le chapitre 6 conclut le mémoire en présentant les principales conclusions, les contributions et les limites ainsi qu'en exposant des pistes des futures recherches.

Chapitre 2 : Revue de la littérature

L'objectif de ce chapitre est de recenser les écrits pertinents afin de comprendre les composantes du contexte organisationnel, et plus spécifiquement de la culture et du climat organisationnels, et leur potentielle influence sur la mise en œuvre de pratiques sécuritaires par les employés dans les organisations. Avant de poursuivre avec l'introduction de la méthodologie de cette revue de la littérature, il est important de rappeler les questions de recherche de ce mémoire :

1. Quels sont les éléments de la culture organisationnelle les plus susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés dans l'organisation ?

2. Quelles sont les caractéristiques du climat organisationnel qui sont les plus susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés dans l'organisation ?

Pour réaliser la recension des références de ce chapitre, plusieurs sources de données ont été consultées. Les bases de données électroniques telles *que ABI/Inform Complete (ProQuest)*, *Emerald*, *ACM Digital Library, IEEE Xplore* ainsi que *Web of Science* ont permis l'obtention d'articles scientifiques liés au sujet de recherche. Des bases de données professionnelles telles que *Gartner* et *Forrester* ont également été consultées afin d'élargir le bassin de références de cette revue de la littérature. En ce qui concerne la prospection de livres, elle a été effectuée grâce au site de la bibliothèque de HEC Montréal. Le moteur de recherche *Google Scholar* a également permis de s'assurer qu'aucun document de base n'avait été omis. De plus, des écrits tels que les comptes rendus de conférences ainsi que les guides de bonnes pratiques se sont avérés être des sources précieuses. Les principes de « *backward search* » et de « *forward search* » ont été appliqués sur les références jugées de qualité et ont favorisé l'identification de nouvelles références. Cette collecte de références a été guidée par plusieurs mots-clés, dont « information security culture », « information security value(s) », « information security norm(s) », « information security belief(s) » et « information security climate ».

La revue de la littérature débute par l'introduction de la variable dépendante au cœur de ce mémoire, soit la mise en œuvre des pratiques sécuritaires par les employés. Dans cette première section, les objectifs des organisations en sécurité de l'information et les variables utilisées dans la littérature pour expliquer la mise en œuvre de pratiques sécuritaires par les employés sont présentés. Cela a enrichi la compréhension du sujet et a permis de conceptualiser la variable dépendante dans la section qui suit. Dans la deuxième section de ce chapitre, l'accent est mis sur le contexte organisationnel et sur son influence sur la

variable dépendante. C'est dans cette section que sont introduits les concepts de la culture organisationnelle et du climat organisationnel ainsi que leur influence sur la variable dépendante. Dans la sous-section suivante, la culture de la sécurité de l'information est présentée par les définitions issues de la littérature. Compte tenu des lacunes que celles-ci présentent, une définition plus claire, qui se base sur des fondements théoriques, est développée et présentée. Par la suite, l'approche méthodologique adoptée pour recenser les éléments de la culture susceptibles d'influencer la variable dépendante est exposée. La sous-section suivante porte sur le climat de la sécurité de l'information et suit le même schéma que la précédente. Enfin, cette revue de la littérature se conclut avec la présentation de l'extrant de ce chapitre, soit un modèle conceptuel formalisant l'influence potentielle de la culture organisationnelle et du climat organisationnel sur la mise en œuvre de pratiques sécuritaires.

2.1 L'objectif visé : expliquer la mise en œuvre de pratiques sécuritaires par les employés

Avant même de pouvoir définir les éléments du contexte organisationnel d'intérêt pour la sécurité de l'information, il est nécessaire de s'interroger sur ce que l'on tente d'expliquer. L'identification et la définition de la cible visée ne sont pas toujours claires, car la littérature en sécurité de l'information en démontre une compréhension fragmentée, voire superficielle (Karlsson et al., 2013). Pourtant, pour traiter de l'influence du contexte organisationnel et pour conceptualiser la culture et le climat de la sécurité de l'information, il faut être en mesure de mieux circonscrire l'objectif visé, soit la variable dépendante. Cette section présente donc un recensement d'une liste de définitions de la variable dépendante afin d'atténuer la confusion existante et pour en arriver à la présentation de la définition de la variable dépendante adoptée dans le cadre de ce mémoire.

2.1.1 Les objectifs des organisations en matière de sécurité de l'information

L'objectif fondamental des organisations en sécurité de l'information est de protéger l'information de l'accès, de l'utilisation, de la divulgation, de la modification et de la destruction non-autorisés (Bernard, 2007; Mellado et al., 2010a). En d'autres termes, les organisations visent à maintenir la confidentialité, l'intégrité et la disponibilité de l'information (Erlich & Zviran, 2010). Pour ce faire, elles disposent d'outils technologiques (par exemple, des anti-virus ou des pare-feu), mais ceux-ci ne peuvent garantir à eux seuls un environnement sécuritaire pour l'information car l'aspect humain doit aussi être pris en considération (Bulgurcu, 2010; Herath & Rao, 2009; Safa et al, 2016; Spears & Barki, 2010).

Pour adresser cet aspect humain de la sécurité de l'information, les organisations définissent donc des politiques et des pratiques sécuritaires que les employés sont appelés à adopter, mais force est de constater qu'elles ne sont pas toujours mises en œuvre par ces derniers (Vroom & Von Solms, 2004). Il est également reconnu que les employés sont le maillon faible en sécurité de l'information et que les pirates informatiques exploitent souvent leur vulnérabilité afin de compromettre la sécurité de l'information d'une organisation (Flores & Eksted, 2016). Cela s'avère être une principale préoccupation pour les organisations (Chan et al., 2005; Dhillon & Torkzadeh, 2006), car cela contribue à l'augmentation du risque et du nombre d'incidents en sécurité de l'information et, au final, à amener des répercussions nuisibles sur l'organisation, telles que des pertes monétaires faramineuses ou encore une réputation entachée (Safa et al., 2016). Ainsi, la mise en œuvre de pratiques sécuritaires par les employés est critique pour les organisations et représente l'objectif visé par toute organisation soucieuse de protéger son information. Compte tenu de l'enjeu qu'elle représente pour les organisations, la mise en œuvre de pratiques sécuritaires par les employés est la variable dépendante de ce mémoire.

2.1.2 La mise en œuvre de pratiques sécuritaires par les employés : une définition

Afin de mieux définir la variable dépendante, une revue de la littérature a été conduite. La variable dépendante se situe au niveau individuel puisqu'elle concerne les comportements et les actions des employés d'une organisation. Puisque qu'il n'existe aucun consensus quant à la variable dépendante d'intérêt, et à cause de la confusion extrême qui existe dans cette littérature, les articles utilisant des variables similaires, qui ont trait à la mise en œuvre de pratiques sécuritaires par les employés, et leur définition, ont été répertoriés et inclus dans le tableau 2.1. Ce tableau inclut également la nature de chaque variable dépendante étudiée. En effet, il a été remarqué que ces variables avaient toutes trait à la conformité, mais à des degrés différents. De ce fait, le tableau spécifie si la variable évoque une « idée de conformité » ou une « idée qui va au-delà de la conformité ».

Tableau 2.1 : Variables utilisées dans la littérature en lien avec la mise en œuvre de pratiques sécuritaires par les employés

Auteur(s)	Variable dépendante utilisée	Définition de la variable dépendante utilisée	Angle de la variable	Nature de la variable
Batteau (2011)	Intelligence	"In these efforts at cultural sensitizing, managers are treated as intelligent beings who, once aware of an issue, can adapt." (p. 43)	Comportement	Idée qui va au-delà de la conformité
Chan et al. (2005)	Compliant information security behavior	"Compliant information security behavior refers the set of core information security activities that need to be carried out by individuals to maintain information security as defined by information security policies." (p. 22)	Comportement	Idée de conformité
D'Arcy et Greene (2014)	Security compliance intention	[Non définie]	Intention	Idée de conformité (suggérée par les items)
Hu et al. (2012)	Policy compliance intention	"Individual's intention to comply with organizational information security policies." (p. 622)	Intention	Idée de conformité
Myyry et al. (2009)	Hypothetical/actual compliance with information security policy	"Employee's adherence to information security policies." (p. 126)	Intention et comportement	Idée de conformité
Safa et al. (2016)	Information security organizational policies and procedures compliance behavioral intentions	[Non définie]	Intention	Idée de conformité (suggérée par les items)
Bulgurcu et al. (2010)	Intention to comply with the information security policy (ISP)	"An employee's intention to protect the information and technology resources of the organization from potential security breaches." (p. 529)	Intention	Idée de conformité
Ng et al. (2009)	Computer security behavior	"[Computer security behavior] is broader than compliance to organizational policies." (p. 816)	Comportement	Idée qui va au-delà de la conformité
Rhee et al. (2009)	Self-efficacy in information security practice	"Security practice can be defined as individuals' information security risk management behavior involving two aspects: the adoption of security technology and security conscious care behavior related to computer and Internet usage." (p. 818)	Comportement	Idée de conformité et idée qui va au-delà de la conformité
Williams et al. (2014)	Security behaviour intentions	"Refer to the extent to which an individual intends to adopt certain behaviors that serve to minimize or eliminate potential information security threats." (p. 28)	Intention	Idée qui va au-delà de la conformité

Une analyse approfondie de ce tableau permet de formuler certains constats. Pour parler de la mise en œuvre de pratiques sécuritaires par les employés, les auteurs recensés adoptent plusieurs angles. Certains auteurs parlent de comportements sécuritaires (par exemple, Batteau et al., 2011; Chan et al., 2005; Myyry et al., 2009; Ng et al., 2009; Rhee et al., 2009) tandis que d'autres réfèrent à l'intention de se conformer à des pratiques sécuritaires (par exemple, D'Arcy & Greene, 2014; Hu et al., 2012; Myyry et al., 2009; Safa et al., 2016; Bulgurcu et al., 2010; Williams et al., 2014). D'autre part, la nature même de la variable ne fait pas consensus entre les auteurs recensés. En effet, pour plusieurs de ces auteurs, la variable dépendante évoque une idée de conformité (par exemple, Chan et al., 2005; D'Arcy & Greene, 2014; Hu et al., 2012; Myyry et al., 2009; Safa et al., 2016; Bulgurcu et al., 2010). Pour ces derniers, la mise en œuvre de pratiques sécuritaires par les employés consiste simplement à respecter les politiques de sécurité de l'organisation. Le reste des auteurs recensés affirment que la variable dépendante outrepasse l'idée de conformité (par exemple, Batteau et al., 2011; Ng et al., 2009; Rhee et al., 2009; Williams et al., 2014). D'après eux, la mise en œuvre de pratiques sécuritaires ne consiste pas uniquement à respecter les politiques dictées par l'organisation, mais il faut aussi que les employés fassent preuve de réflexion, de jugement et qu'ils acquièrent le réflexe d'agir, que ce soit en prenant action (par exemple, remarquer une faille de sécurité dans un système ou dans un processus d'affaires) ou en rapportant une situation potentiellement problématique à qui de droit (par exemple, à son supérieur ou au département informatique de l'organisation). En effet, l'augmentation et la sophistication perpétuelle des menaces en sécurité de l'information obligent les organisations à renouveler leurs pratiques sécuritaires (Rhee et al., 2009; Williams et al., 2014). Néanmoins, les organisations peinent à adapter les pratiques sécuritaires à mettre en œuvre en raison du rythme effréné auquel évoluent ces menaces (Bauer et al., 2017). Les employés doivent donc développer une « deuxième nature » face à la sécurité de l'information.

Par conséquent, l'analyse des différentes variables ayant trait à la mise en œuvre de pratiques sécuritaires démontre que celle-ci est constituée de deux composantes : la conformité et, ce qu'il est convenu d'appeler l'intelligence. Dans un premier temps, les organisations visent la conformité, car elles souhaitent que leurs employés respectent et adoptent les pratiques sécuritaires définies. Leur respect relève souvent d'obligations légales ou est parfois sanctionné par des certifications (Von Solms, 2000; Knapp et al., 2006). Les travaux de Bulgurcu et al. (2010), de Chan et al. (2005), de Myyry et al. (2009), de Hu et al. (2012) et de Williams et al. (2014) ont servi de base pour définir cette composante. Ainsi, la conformité est définie comme étant le respect des pratiques de sécurité de l'information définies par l'entreprise.

Au-delà de la conformité, les organisations souhaitent que leurs employés fassent preuve de jugement vis-à-vis de la sécurité de l'information. Étant donné que cette idée d'outrepasser la conformité est nommée de manière différente dans la littérature, on propose le terme « intelligence » de Batteau (2011) pour y référer, car de toutes les variables recensées, c'est le terme le plus adéquat pour se rapporter à ce type de comportement. En se basant sur la pensée de Batteau (2011), Ng et al. (2009) et de Rhee et al. (2009), l'intelligence est donc définie comme étant le réflexe d'assurer la protection de l'information en jugeant de manière éclairée les activités du quotidien et en prenant, au besoin, les mesures appropriées.

Ainsi donc, en matière de sécurité de l'information, il est important de préciser que pour encourager la mise en œuvre de pratiques sécuritaires par les employés, il faut d'abord que les actions des employés soient conformes aux politiques de sécurité de l'information de l'organisation. Une fois que la conformité est atteinte, les organisations aspirent à ce que leurs employés soient « intelligents » par rapport à la sécurité de l'information, c'est-à-dire qu'ils agissent de manière réfléchie. Il est possible qu'un employé respecte les règles organisationnelles définies (et, par conséquent, atteigne la conformité) sans être intelligent. En outre, l'idéal serait que l'employé respecte les règles organisationnelles définies et qu'il fasse aussi preuve d'intelligence. Ainsi, la conformité est un objectif précis alors que l'intelligence s'opère à différents degrés. Les organisations peuvent donc viser la conformité, mais aussi le développement des réflexes d'intelligence chez leurs employés. La mise en œuvre de pratiques sécuritaires et ses composantes sont définies comme:

*« La **mise en œuvre de pratiques sécuritaires** concerne l'application de mesures permettant de protéger l'information d'une organisation. Elle est composée de la **conformité** (le respect des pratiques de sécurité de l'information définies par l'organisation) et de l'**intelligence** (le réflexe d'assurer la protection de l'information en jugeant de manière éclairée les activités du quotidien et en prenant, au besoin, les mesures appropriées). »*

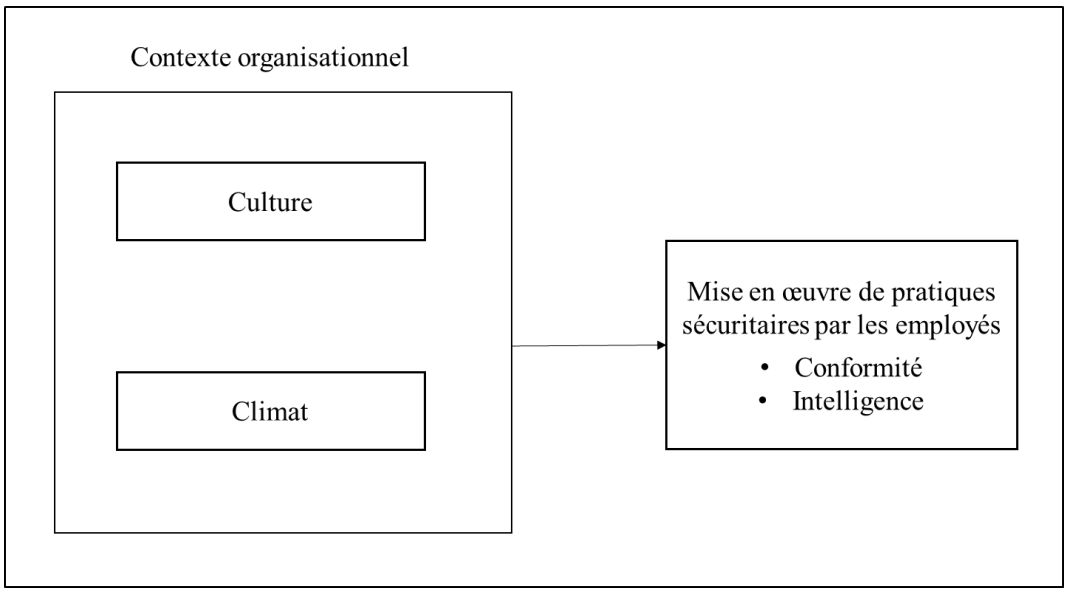
Cette définition articulée de la variable dépendante permet ensuite d'orchestrer l'ensemble de la réflexion visant la conceptualisation de la variable indépendante, soit les éléments de la culture organisationnelle et du climat organisationnel pouvant l'influencer.

2.2 La culture et le climat organisationnels : sources d'influence de la mise en œuvre de pratiques sécuritaires par les employés

Dans le but d'encourager les employés à mettre en œuvre des pratiques sécuritaires, les organisations ont recours à des programmes de sensibilisation à la sécurité de l'information, car ils sont traditionnellement considérés comme les moyens les plus efficaces pour contrer les risques humains en matière de sécurité de l'information (Spears & Barki, 2010; Parsons et al., 2010). Cependant, l'efficience de ces programmes est maintenant largement questionnée puisque malgré les nombreux programmes de sensibilisation offerts dans les organisations, les employés sont encore la principale source d'incidents de sécurité de l'information (Da Veiga & Martins, 2015; Van Loenen, 2015).En effet, les programmes de sensibilisation semblent n'avoir qu'un effet à court terme. Après un certain temps, les employés deviennent moins vigilants vis-à-vis de la sécurité de l'information et tendent à reprendre leurs « mauvaises habitudes » (Alhogail, 2015). Ainsi, les organisations sont à la recherche de moyens qui ont des effets plus durables pour assurer la sécurité de l'information. Elles se tournent vers le rôle que le contexte organisationnel peut y jouer, de mieux en mieux compris.

Pour influencer les comportements des employés à plus long terme, il s'avère pertinent de se pencher davantage sur la culture et sur le climat, deux composantes importantes du contexte organisationnel (Denison, 1996). D'après Schneider & Barbera (2014), la culture et le climat organisationnels exercent à eux deux la plus forte influence sur les actions et les comportements des employés. Il faut donc traiter la culture et le climat organisationnels conjointement si l'on souhaite influencer de manière significative la mise en œuvre de pratiques sécuritaires par les employés (Ashkanasy et al., 2011). La figure 2.1 représente le modèle général illustrant l'influence du contexte organisationnel qui est composé de la culture et du climat, sur la mise en œuvre de pratiques sécuritaires par les employés.

Figure 2.1 : Influence des deux composantes du contexte organisationnel sur la variable dépendante



Puisque ce mémoire met l'accent sur la sécurité de l'information, il n'est pas question de traiter de l'intégralité de la culture et du climat organisationnels, mais plutôt d'examiner les éléments de la culture et du climat organisationnels qui sont susceptibles d'influencer la variable dépendante d'intérêt. Il faut également noter qu'il n'existe pas de culture de la sécurité de l'information et de climat de la sécurité de l'information en soi, mais plutôt une culture organisationnelle ou un climat organisationnel qui contribue ou qui nuit à la sécurité de l'information (Alnatheer, 2015). Tel que souligné dans la problématique, les expressions « culture de la sécurité de l'information » et « climat de la sécurité de l'information » sont utilisées dans ce mémoire afin d'en alléger la lecture, mais aussi parce qu'elles sont largement utilisées dans la littérature actuelle et par les praticiens. De ce fait, pour mieux comprendre et ensuite influencer la mise en œuvre de pratiques sécuritaires par les employés, les sections suivantes ont pour objectif de présenter en détail les construits de la culture et du climat organisationnels.

2.2.1 La culture de la sécurité de l'information

Cette sous-section vise à mieux comprendre la culture de la sécurité de l'information et son influence sur la variable dépendante. Pour cela, elle présente les définitions issues de la littérature de la culture de la sécurité de l'information, mais examine aussi de façon plus générale la littérature sur la culture organisationnelle. Sur la base de celles-ci, une définition plus claire sera formulée. Ensuite, les croyances et les valeurs liées à la sécurité de l'information, qui sont les manifestations centrales de la culture organisationnelle, seront exposées. Cette sous-section fait office de premier pas vers la conceptualisation de la culture de la sécurité de l'information.

2.2.1.1 Définitions de la culture de la sécurité de l'information tirées de la littérature

Si les milieux scientifiques et pratiques s'accordent sur l'importance de la culture de la sécurité de l'information, le construit demeure encore flou à bien des égards. Cette section a donc pour principal objectif de présenter les définitions du construit qui existent présentement dans la littérature. Le tableau 2.2 présente ces définitions en fonction de la perspective abordée.

Tableau 2.2 : Définitions de la culture de la sécurité de l'information issues de la littérature

Pers-pective	Auteur(s)	Définition
Employés	Astakhova (2014)	"Information security culture is a specific mode of the organization and development of a subject's information activity, which is represented in the value oriented models of his information interaction as a sender and receiver of information, under which he determines and controls the unity of existence and development of information objects in their cognitive and communicative manifestations." (p. 6)
	Da Veiga & Eloff (2010)	"The attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organisation's systems and procedures at any point in time" (p. 3)
	Da Veiga & Martins (2015)	"A culture in which the protection of information and upholding of privacy are part of the way things are done in an organization. It is a culture in which employees illustrate attitudes, assumptions, beliefs, values and knowledge that contribute to the protection and privacy of information when processing it at any point in time in the information life cycle, resulting in ethical and compliant behavior." (p. 249)
	Dhillon (1997)	"Security culture is the totality of patterns of behaviour in an organisation that contribute to the protection of information of all kinds." (p. 59)
	Helokunnas & Kuusisto (2003)	"Information security culture as a system consisting of interacting framework and content components. […] Content includes people's attitude, motivation, knowledge and mental models about information security." (p. 193)
	Martins & Eloff (2002)	"Information security culture can thus be defined as the assumption about which type of information security behaviour is accepted and encouraged in order to incorporate information security characteristics as the way in which things are done in an organisation." (p. 205-206)
	Ngo et al. (2005)	"Information security culture can be understood as how things are done (i.e. accepted behaviour and actions) by employees and the organisation as a whole, in relation to information security" (p.68)
	Ross (2011)	"A culture of security is a pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things that promotes security." (p. 18)
	Schlienger & Teufel (2003)	"Security culture encompasses all socio-cultural measures that support technical security measures, so that information security becomes a natural aspect in the daily activities of every employee." (p.1)

Pers-pective	Auteur(s)	Définition
Organisation	Helokunnas & Kuusisto (2003)	"Information security culture as a system consisting of interacting framework and content components. Framework contains standardization, certification and measurement of information security. […]."(p. 193)
	Ruighaver et al. (2006)	"Information security is, in general, a management problem and the security culture reflects how management handles this problem." (p. 1)
	Von Solms (2000)	"[…] corporate information security culture that support the information security policies, procedures, methods and responsibilities of the company, in such a way that information security becomes a natural aspect of the day to day activities of all employees of the company, and endures long after those who originally created these infrastructures, have gone " (p. 2)
	Vroom & Von Solms (2004)	"A utopian information security culture would be where the employees of the organization follow the guidelines of the organization voluntarily as part of their second nature." (p. 5)

Tableau 2.2 : Définitions de la culture de la sécurité de l'information issues de la littérature (suite)

À la lecture des définitions de la culture de la sécurité de l'information recensées, il est possible de les classer selon deux perspectives, à savoir les perspectives « Employés » et « Organisation ». Ainsi, la plupart des définitions de la culture de la sécurité de l'information sont placées dans la perspective « Employés », car elles se rapportent principalement aux comportements ou à l'attitude des employés. Pour ce qui est des autres définitions, qui relèvent de la perspective « Organisation », elles s'intéressent plutôt aux activités conduites par l'organisation en termes de sécurité de l'information. Cette disparité de perspectives montre déjà qu'il existe de la confusion quant à la culture de la sécurité de l'information. Pour mieux comprendre cette confusion, chacune des définitions est présentée ici.

La majorité des définitions de la culture de la sécurité de l'information s'inscrit selon la perspective des employés. Astakhova (2014) stipule que la culture de la sécurité de l'information est la réception et l'envoi de modèles de valeurs relatifs à la sécurité de l'information entre un employé et l'organisation. Da Veiga & Eloff (2010) écrivent dans leur étude que la culture de la sécurité de l'information regroupe les attitudes, les hypothèses, les croyances, les valeurs et les connaissances relatives à la sécurité de l'information que les employés et les parties prenantes d'une organisation utilisent pour interagir avec les systèmes informatiques d'une organisation. Da Veiga & Martins (2015) et Ross (2011), pour leur part, définissent la culture de la sécurité de l'information en mettant l'accent sur la protection de la vie privée. Ils définissent la culture de la sécurité de l'information comme étant les attitudes, les hypothèses, les croyances, les valeurs et les connaissances qui contribuent à la protection de l'information et de la vie privée. Pour

Helokunnas & Kuusisto (2003), la culture de la sécurité de l'information est un système de composantes qui comprend les attitudes des individus, leurs motivations, leurs connaissances et leurs modèles mentaux à l'égard de la sécurité de l'information. Martins & Eloff (2002), Ngo et al. (2005) et Ross (2011) perçoivent la culture de la sécurité de l'information telle que la manière dont les choses sont faites au sein d'une organisation, c'est-à-dire les comportements acceptées vis-à-vis de la sécurité de l'information. Quant à Schlienger & Teufel, la culture de la sécurité de l'information concerne toutes les mesures socio-culturelles qui soutiennent l'aspect technique de la sécurité, de sorte que cette dernière soit naturellement intégrée dans les activités quotidiennes des employés.

La culture de la sécurité de l'information a aussi été définie selon la perspective de l'organisation. Helokunnas & Kuusisto (2003) définissent la culture de la sécurité de l'information comme l'application d'un cadre qui contient des composantes telles que la standardisation, la certification et la mesure de la sécurité de l'information. Ruighaver et al. (2006) expliquent que la culture de la sécurité de l'information reflète comment la direction d'une organisation gère la sécurité de l'information. Pour Von Solms (2000), une culture de la sécurité de l'information est une culture organisationnelle qui soutient les politiques et les procédures de sécurité, les méthodes et les responsabilités de l'organisation afin que la sécurité de l'information devienne naturelle dans la réalisation des tâches des employés. La définition de Vroom et Von Solms (2004) soutient ce dernier point puisqu'elle décrit la culture de la sécurité de l'information comme étant une culture utopique où les employés suivent les règles organisationnelles comme si elles faisaient partie de leur seconde nature.

L'hétérogénéité des définitions et des perspectives présentées dans la littérature apporte son lot de problèmes, autant dans la recherche que dans la pratique. Sans une définition précise, il est difficile de bâtir une conceptualisation précise d'un construit et de comparer les résultats d'une étude à l'autre. À la fin, il devient alors difficile de bâtir une base de connaissances partageables établie sur des bases solides et, de ce fait, de donner des conseils solides aux praticiens. Il faut donc retourner aux fondements théoriques de la culture organisationnelle afin de développer la définition de la culture de la sécurité de l'information.

2.2.1.2 Culture de la sécurité de l'information : définition proposée

Bien que la culture de la sécurité de l'information reçoive beaucoup d'attention au sein de la communauté de chercheurs, la littérature scientifique est encore émergente. À cela s'ajoute le fait que la compréhension du construit est encore très limitée et qu'elle souffre d'une grande hétérogénéité. Cette section vise donc à enrichir la compréhension du construit en puisant dans les fondements théoriques liés à la culture organisationnelle. Elle s'articule autour de la présentation de la culture organisationnelle, avant d'examiner la

littérature en culture de la sécurité de l'information et de présenter tous les éléments de la culture liés à la sécurité de l'information.

La recherche en culture de la sécurité de l'information est passablement récente puisque les premières publications à ce sujet remontent vers la fin des années 1990. Par exemple, Dhillon (1997) ou encore Von Solms (2000) comptent parmi les premiers auteurs à aborder ce sujet. Pour ce qui est de la culture organisationnelle, elle est assidûment étudiée depuis les années 1980 (Smircich, 1983). Il s'avère alors très pertinent de mettre à profit une solide base de connaissance pour voir comment celle-ci peut venir alimenter et enrichir le travail de compréhension de ce qu'est la culture de la sécurité de l'information. Et pour cause, la culture de la sécurité de l'information n'est qu'un des aspects de la culture organisationnelle.

Ce mémoire s'appuiera donc sur la conceptualisation de la culture organisationnelle de Martin (1992) afin de mieux comprendre et de définir la culture de la sécurité de l'organisation. Le cadre de Martin (1992) a été choisi non seulement pour sa renommée scientifique (il a été cité dans 2899 publications[1]), mais aussi pour sa grande utilisation en systèmes d'information. En effet, l'ouvrage de Martin (1992) a été cité dans maintes publications du domaine, telles que celles de Dubé & Robey (1999), Kappos & Rivard (2008), Leidner & Kayworth (2006), Pentland (1995) ou encore Robey et al. (2002).

Martin (1992) conceptualise la culture organisationnelle comme étant un ensemble d'interprétations qui sous-tendent une variété de manifestations. Ces dites manifestations peuvent être visibles lorsque l'on fait non seulement référence à des artefacts tels que le code vestimentaire, les histoires ou encore les rituels, mais aussi à des pratiques formelles et informelles, qui comprennent, par exemple, les règles comportementales et les normes. D'autres manifestations sont, quant à elles, non visibles. Il s'agit des valeurs, des croyances et des hypothèses que les employés de l'organisation se sont appropriés.

L'analyse conduite dans la section 2.2.1.1 sur les définitions de la culture de la sécurité de l'information issues de la littérature montre que le construit souffre de l'absence d'une définition claire et complète. En se basant sur le cadre de la culture organisationnelle de Martin (1992), une définition claire de la culture de la sécurité de l'information peut être développée:

[1] Source : Google Scholar (Septembre 2016). Récupéré de : <https://scholar.google.ca/scholar?cites=6449340711625254341&as_sdt=2005&sciodt=0,5&hl=en>

*« **La culture de la sécurité de l'information** au sein d'une organisation est constituée d'un ensemble de manifestations visibles et invisibles partagées par les membres de l'organisation. Ces manifestations incluent les croyances, les valeurs, les hypothèses, les artéfacts et les pratiques formelles et informelles qui influencent les décisions et les comportements des employés quant à la protection de l'information. Ces manifestations viennent aussi teinter le climat organisationnel. »*

Cette définition devient un maillon important de la conceptualisation de ce qu'est la culture de la sécurité de l'information car elle permet d'identifier les éléments qui pourraient s'avérer particulièrement importants pour expliquer la mise en œuvre de pratiques sécuritaires par les employés. Cette définition permet aussi de donner un éclairage différent quant au libellé de la variable dépendante d'intérêt (section 2.1.2); en effet, même si on y met l'accent sur les pratiques de sécurité, celles-ci doivent être comprises comme les comportements que les employés d'une organisation adoptent et qui sont influencés par les éléments de la culture organisationnelle.

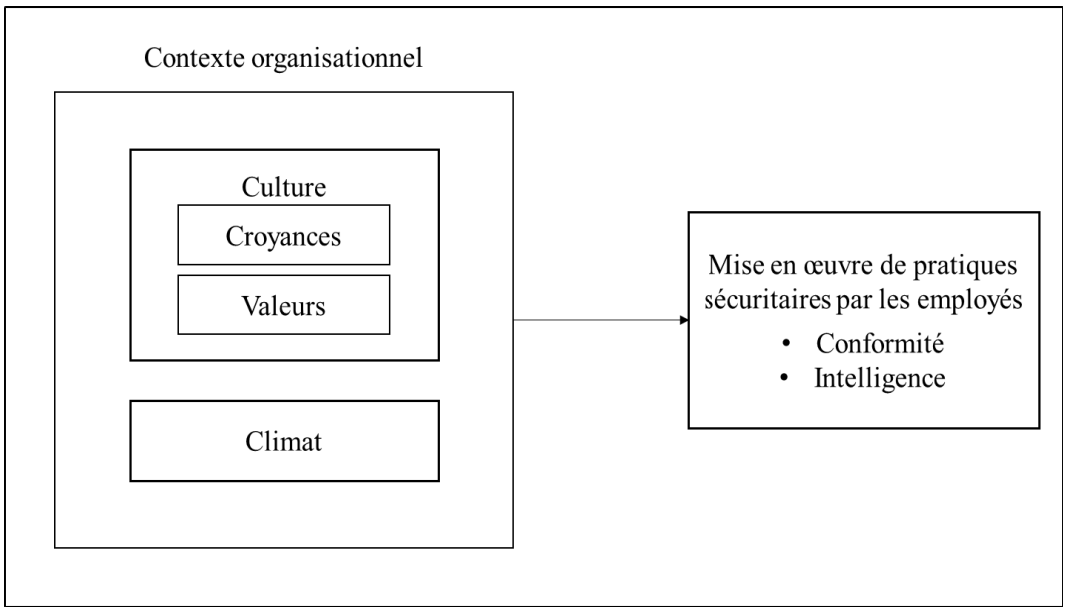
2.2.1.3 Les valeurs et les croyances au cœur de la culture organisationnelle

De toutes les manifestations possibles, ce mémoire met l'accent sur les croyances et les valeurs puisque ce sont non seulement les manifestations centrales de la culture organisationnelle (Alvesson & Sveningsson, 2016; Ashkanasy et al., 2011; Ott, 1989), mais car elles constituent aussi les forces-clé qui influencent les autres manifestations de la culture organisationnelle. En outre, les pratiques formelles et informelles et les artefacts ne sont que le reflet et la matérialisation des valeurs et des croyances d'une organisation (Schein, 1985; Trice & Beyer, 1993). Pour ce qui est des hypothèses, elles ne feront pas l'objet de ce mémoire car elles sont difficilement identifiables et mesurables. Selon Ott (1989), recenser les hypothèses d'une organisation s'avère être un défi de taille en recherche. L'exercice requiert une longue implication du chercheur avec une organisation, un accès quasi-illimité aux employés et aux archives ainsi que l'utilisation de multiples stratégies de collecte de données. Les chercheurs qui ont tenté de le faire ont connu plus ou moins de succès (Ott, 1989). Par exemple, Siehl & Martin (1984) se sont résignés à identifier les histoires organisationnelles au lieu des hypothèses, car l'identification de ces dernières leur imposait trop de contraintes méthodologiques.

Ainsi, l'influence des croyances et des valeurs (les manifestations de la culture étudiées dans ce mémoire) sur la mise en œuvre de pratiques sécuritaires par les employés est représentée dans la figure 2.2. Ott (1989) mentionne d'ailleurs que les croyances et les valeurs s'influencent mutuellement. Bien que l'on reconnaisse l'existence de ces

influences, elles ne sont pas représentées dans le présent mémoire parce qu'à ce stade-ci, l'objectif en est un d'identification des éléments et non d'investigation des relations entre les éléments.

Figure 2.2 : L'influence des croyances et des valeurs sur la mise en œuvre de pratiques sécuritaires



Malgré l'importance que leur accordent les auteurs, on définit rarement ce qu'est une croyance ou une valeur dans la littérature et ce, même dans la littérature en gestion où le concept de culture organisationnelle a été intensivement étudié (par exemple, Martin, 1992; 2002; Schein, 1985; Ott, 1989). On semble prendre pour acquis que la compréhension de ces construits est universelle. Des bribes de connaissances (tirées des études de Fishbein & Azjen (1975), de Schein (1985) et d'Ott (1989)) ont donc été exploitées afin de formuler des définitions permettant de mieux comprendre ces manifestations et d'aiguiller la réflexion:

- *« Les* ***croyances*** *reflètent des convictions profondes, qui existent souvent universellement au-delà des murs de l'entreprise et que l'entreprise a faites siennes. »*
- *« Les* **valeurs** *reflètent des idées implicites ou explicites partagées au sein de l'organisation sur ce qui est important pour l'organisation ou à quoi l'organisation tient beaucoup. »*

Maintenant que les croyances et les valeurs sont clairement définies, il devient plus aisé de déterminer les croyances et les valeurs de la culture organisationnelle susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés.

2.2.1.4 Les croyances et les valeurs de la culture de la sécurité de l'information susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés

Tel qu'annoncé, au niveau de la culture organisationnelle, ce mémoire se concentre sur les croyances et les valeurs susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés. Dans un premier temps, cette section présente l'approche méthodologique employée pour identifier ces croyances et ces valeurs dans la littérature de la culture de la sécurité de l'information. L'inventaire découlant de cette revue de la littérature est ensuite présenté.

Approche méthodologique utilisée pour identifier les croyances et les valeurs susceptibles d'influencer la mise en œuvre de pratiques sécuritaires

Afin d'identifier les croyances et les valeurs susceptibles d'influencer la mise en œuvre de pratiques sécuritaires, une revue de la littérature a été conduite. Dans la base de données ABI/Inform, les articles qui contiennent, dans leur titre ou dans leur résumé, les termes « information security culture », « information security value », « information security norm », ou encore « information security belief » ont été recensés. En addition à cette liste, d'autres références jugées pertinentes (tels que les actes de conférence, des chapitres de livre, etc.) ont été ajoutées pour recenser de manière exhaustive les valeurs et les croyances recherchées.

Il faut néanmoins préciser que la littérature en culture de la sécurité de l'information est anecdotique et souffre d'un manque de validation. Relever les croyances et les valeurs de la culture de la sécurité de l'information a donc été un exercice complexe puisqu'elles ne sont pas aisément accessibles dans la littérature. En outre, aucune des publications recensées ne dresse une liste exhaustive de croyances et de valeurs liées à la sécurité de l'information. De plus, la plupart des publications n'identifie pas clairement ces croyances et ces valeurs. Ainsi, les définitions de la culture de la sécurité de l'information, des croyances et des valeurs (de la section 2.2.1.3.) ont été utilisées afin d'identifier ces éléments.

Toute cette connaissance a ensuite dû être classifiée et analysée. Grâce à un exercice d'extraction et de codage, toutes les publications recensées ont été analysées pour en relever les passages qui font référence à une croyance ou à une valeur en lien avec la sécurité de l'information et qui sont susceptibles d'influencer la mise en œuvre de pratiques de sécurité par les employés. Le codage consistait ensuite à assigner ce passage à une croyance ou à une valeur spécifique. Par exemple, la citation « *Management needs to encourage shared beliefs that information security makes sense and is actually good for the business.* » (p. 40) de Knapp & Ferrante (2014) fait référence à la croyance qui a, par la suite, été nommée « Importance générale qu'a la sécurité de l'information dans l'organisation ». Il faut

toutefois noter que l'exercice s'est avéré parfois difficile. Ainsi, dans certains textes, l'idée sous-jacente à une croyance ou à une valeur était clairement exprimée; dans d'autres, il fallait plutôt se pencher sur l'idée générale émise par les auteurs. Dans certains textes, l'idée était conceptuellement énoncée, mais jamais empiriquement testée. Afin que la présente étude soit aussi complète que possible, chaque idée a été codée et incluse dans la liste initiale des croyances et des valeurs susceptibles d'influencer la variable dépendante, qu'elle ait été explicitement ou implicitement énoncée et empiriquement testée ou non.

Les références ont également contribué à définir chaque croyance ou valeur. Par exemple, sur la base des études de Chen et al. (2015), de Flores & Ekstedt (2016) et de Knapp & Ferrante (2014), la croyance « Importance générale qu'a la sécurité de l'information dans l'organisation » est définie comme ceci : « *Croyance partagée dans l'organisation qui réfère à l'importance générale que l'on accorde à la sécurité de l'information.* ».

Par ailleurs, il a été remarqué que les auteurs exposaient parfois plusieurs idées par rapport à une croyance ou à une valeur. Il s'est dès lors avéré pertinent de spécifier, pour chaque élément, les points de vue possibles. À titre d'illustration, la croyance « Importance générale qu'a la sécurité de l'information dans l'organisation » englobe deux points de vue. D'une part, plusieurs auteurs (par exemple, Chen et al., 2015; Flores & Ekstedt, 2016; Knapp & Ferrante, 2014) avancent l'idée que dans certaines organisations, la sécurité de l'information doit être perçue comme étant importante pour influencer les employés à agir de manière sécuritaire. D'autre part, d'autres auteurs (par exemple, Chia et al., 2002; Thomson & Von Solms, 2005) ont observé que dans certaines organisations, la sécurité de l'information était perçue comme étant non-importante et que cela n'incitait pas les employés à mettre en œuvre des pratiques sécuritaires. À partir de ces idées, des propositions liées à chacune des croyances et des valeurs ont été élaborées. Par conséquent, les propositions liées à la croyance « Importance générale qu'a la sécurité de l'information dans l'organisation » sont les suivantes : « *Plus on croit dans l'organisation que la sécurité de l'information est importante, plus les employés sentiront la nécessité de mettre en œuvre des pratiques sécuritaires. À l'opposé, si on croit dans l'organisation que la sécurité de l'information n'est pas importante, moins élevées sont les chances que les employés mettent en œuvre des pratiques sécuritaires. »*

À partir de ces propositions et dans le respect de l'objectif initial de ce mémoire (soit le développement d'un instrument de mesure), quatre items ont également été formulés pour chacune des croyances et des valeurs. Par exemple, pour la croyance « Importance générale qu'a la sécurité de l'information dans l'organisation », les items sont les suivants :

• *« Dans mon environnement de travail, la sécurité de l'information est en bas de la liste de priorité. »*

• *« Dans mon environnement de travail, personne ne s'intéresse au fait que les pratiques de sécurité de l'information soient respectées ou non. »*

• *« Dans mon environnement de travail, un manquement aux pratiques de sécurité de l'information est considéré comme étant inacceptable. »*

• *« Dans mon environnement de travail, la sécurité de l'information est une priorité. »*

En plus d'illustrer l'esprit de la croyance ou de la valeur, en lien avec l'objectif initial de ce mémoire, ces items pourraient ensuite être utilisés lors de l'élaboration de l'instrument de mesure.

En somme, ce recensement et cet exercice d'extraction et de codage ont donné lieu à une liste de sept croyances et de neuf valeurs susceptibles d'influencer les employés à mettre en œuvre des pratiques sécuritaires. La section suivante présente les éléments de cette liste.

Inventaire des valeurs et des croyances tirées de la littérature

Ce recensement a ultimement abouti à l'identification de sept croyances et de neuf valeurs tirées de la littérature. Le tableau 2.3 présente les croyances identifiées, leur définition (A), les propositions (B) et, à titre illustratif, les quatre items formulés (C). Les auteurs ayant servi de sources pour chacune de ces croyances figurent dans la dernière colonne. Le tableau 2.4 présente les valeurs tirées de la littérature qui sont susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés. Il suit le même schéma de présentation que le tableau 2.3.

Tableau 2.3 : Les croyances susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés

Croyance	Définition (A), propositions (B) et items (C) liés à la croyance	Auteur(s)
RESPONSABILITÉ D'ASSURER LA SÉCURITÉ DE L'INFORMATION	(A) Croyance partagée dans l'organisation qui indique qui a la responsabilité d'assurer la sécurité de l'information. (B) Plus on croit dans l'organisation que la sécurité de l'information est du ressort exclusif du département informatique, moins les employés se sentiront responsables de mettre en œuvre des pratiques sécuritaires. À l'opposé, si on croit que tout le monde dans l'organisation a une responsabilité quant à la sécurité de l'information, plus les employés se sentiront responsables de mettre en œuvre des pratiques sécuritaires. (C) • Dans mon organisation, on croit que c'est le département informatique (ou l'équivalent) qui a la responsabilité d'assurer la sécurité de l'information. • Dans mon organisation, on croit que la sécurité de l'information est l'affaire de tous. • Dans mon organisation, on croit que la sécurité de l'information est une responsabilité partagée entre les unités fonctionnelles et le département informatique (ou l'équivalent). • Dans mon organisation, on croit que la sécurité de l'information est une responsabilité partagée par tous les employés de l'organisation.	Alhogail (2015); Chia et al. (2002); Da Veiga & Eloff (2007); D'Arcy & Greene (2014); Dhillon & Torkzadeh (2006); Flores & Ekstedt (2016); Gaunt (2000); Knapp & Ferrante (2014); Koh et al. (2005); Lim et al. (2010); Mishra (2015); Ruighaver et al. (2007).

Tableau 2.3 : Les croyances susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite)

Croyance	Définition (A), propositions (B) et items (C) liés à la croyance	Auteur(s)
VISION DE L'ORGANISATION QUANT À LA NATURE DES DÉFIS EN TERMES DE SÉCURITÉ DE L'INFORMATION	(A) Croyance partagée dans l'organisation qui indique la nature des défis rencontrés en sécurité de l'information. (B) Plus on croit dans l'organisation que la sécurité de l'information est avant tout un défi d'ordre technique, moins les employés sentiront la nécessité de mettre en œuvre des pratiques sécuritaires parce qu'ils se fieront aux solutions technologiques. À l'opposé, plus on a la conviction dans l'organisation qu'il y a des composantes humaine, technique et managériale à la sécurité de l'information, plus élevées sont les chances que tout le monde jouera le rôle qu'il a à jouer afin de protéger l'information. (C) • Dans mon organisation, on croit qu'assurer la sécurité de l'information représente avant tout un défi d'ordre technique. • Dans mon organisation, on croit que la sécurité de l'information passe par la considération des aspects techniques, humains et managériaux. • Dans mon organisation, on croit que la sécurité de l'information doit être traitée comme un problème technique. • Dans mon organisation, on croit que la sécurité de l'information nécessite une vision globale qui inclut des aspects techniques, humains et managériaux.	Alhogail (2015); Batteau (2011); Bulgurcu et al. (2010); Chang & Lin (2007); Da Veiga & Eloff (2007, 2010); Da Veiga & Martins (2015); Dhillon & Torkzadeh (2006); Dhillon et al. (2016); Lacey (2010); Lim et al. (2012); Martins & Eloff (2002); Mishra (2015); Nosworthy (2000); Rhee et al. (2009); Schlienger & Teufel (2002); Von Solms (2000); Vroom & Von Solms (2004).

Tableau 2.3 : Les croyances susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite)

Croyance	Définition (A), propositions (B) et items (C) liés à la croyance	Auteur(s)
IMPORTANCE GÉNÉRALE QU'A LA SÉCURITÉ DE L'INFORMATION DANS L'ORGANISATION	(A) Croyance partagée dans l'organisation qui réfère à l'importance générale que l'on accorde à la sécurité de l'information. (B) Plus on croit dans l'organisation que la sécurité de l'information est importante, plus les employés sentiront la nécessité de mettre en œuvre des pratiques sécuritaires. À l'opposé, si on croit dans l'organisation que la sécurité de l'information n'est pas importante, moins élevées sont les chances que les employés mettent en œuvre des pratiques sécuritaires. (C) • Dans mon organisation, on croit que la sécurité de l'information doit être une priorité. • Dans mon organisation, on croit que la sécurité de l'information est peu importante parce que les problèmes de sécurité n'arrivent qu'aux autres. • Dans mon organisation, on a de la difficulté à prendre au sérieux les menaces à la sécurité de l'information. • Dans mon organisation, on croit que l'argent investi en sécurité de l'information représente une dépense inutile.	Chen et al. (2015); Chia et al. (2002); Dojkovski et al. (2010); Flores & Ekstedt (2016); Knapp & Ferrante (2014); Ross (2011); Ruighaver et al. (2007); Schlienger & Teufel (2002); Nosworthy (2000); Thomson & Von Solms (2005).

Tableau 2.3 : Les croyances susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite)

Croyance	Définition (A), propositions (B) et items (C) liés à la croyance	Auteur(s)
AUTO-EFFICACITÉ ORGANISATIONNELLE FACE AUX MENACES	(A) Croyance partagée dans l'organisation qui réfère à la capacité de l'organisation à se défendre contre les menaces à la sécurité de l'information. (B) Plus on croit dans l'organisation qu'il est fondamentalement impossible d'assurer vraiment la protection de l'information, moins les employés seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si on est convaincus dans l'organisation qu'il est possible de prendre des actions préventives et de protéger l'information, plus élevées sont les chances que les employés mettront en œuvre des pratiques sécuritaires. (C) • Dans mon organisation, on croit qu'il est possible de protéger l'information contre des actes malicieux. • Dans mon organisation, on croit qu'il est possible de mettre en place un ensemble de moyens pour contrer les menaces à la sécurité de l'information. • Dans mon organisation, on croit qu'il est impossible de se prémunir contre les menaces liées à la sécurité de l'information. • Dans mon organisation, on pense que, malgré tous les moyens mis en place, l'entreprise reste très vulnérable et les personnes malveillantes gagneront toujours.	Alhogail (2015); Chang & Lin (2007); Chen et al. (2015); Da Veiga & Eloff (2007); Hu et al. (2012); Lim et al. (2012); Vroom & Von Solms (2004).

Tableau 2.3 : Les croyances susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite)

Croyance	Définition (A), propositions (B) et items (C) liés à la croyance	Auteur(s)
RESPONSABILITÉ MORALE DE PROTÉGER L'INFORMATION	(A) Croyance partagée dans l'organisation quant à la responsabilité morale que l'entreprise a de protéger les informations. (B) Plus on croit que l'organisation a la responsabilité morale de protéger l'information, plus les employés seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si on ne croit pas que l'organisation a cette responsabilité morale, moins élevées sont les chances que les employés mettent en œuvre des pratiques sécuritaires. (C) • Dans mon organisation, on croit qu'on a l'obligation morale de faire ce que l'on peut pour protéger l'information. • Dans mon organisation, on croit qu'on a l'obligation de protéger l'information malgré les contraintes que cela impose • Dans mon organisation, on croit qu'on a l'obligation de protéger l'information afin de défendre les intérêts de l'organisation. • Dans mon organisation, on croit qu'on a l'obligation d'assurer la sécurité de l'information afin de protéger les intérêts de ceux qui souffriraient d'un tel incident.	Chia et al. (2002); Faily & Flechais (2010); Ruighaver et al. (2007).

Tableau 2.3 : Les croyances susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite)

Croyance	Définition (A), propositions (B) et items (C) liés à la croyance	Auteur(s)
NATURE GÉNÉRALE DE L'ÊTRE HUMAIN (SES MOTIVATIONS PROFONDES)	(A) Croyance partagée dans l'organisation quant à la nature générale de l'être humain et, plus spécifiquement, en ce qui a trait aux raisons qui motivent ses actions. (B) Plus on croit dans l'organisation que les gens agissent dans le meilleur intérêt de l'organisation et qu'on peut leur faire confiance, plus ils seront responsables et motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si on croit que les gens sont fondamentalement mauvais et qu'on les déresponsabilise en les contrôlant comme des enfants, moins les gens mettront en œuvre des pratiques sécuritaires. (C) • Dans mon organisation, on croit qu'on ne peut faire confiance à personne. • Dans mon organisation, on croit que faire confiance aux gens, permet d'agir dans le meilleur intérêt de l'entreprise. • Dans mon organisation, on croit qu'exercer un contrôle très strict est le seul moyen de s'assurer que les gens font ce qu'ils sont censés faire. • Dans mon organisation, on croit que les gens agissent dans le meilleur intérêt de l'organisation quand on leur fait confiance.	Batteau (2011); Bulgurcu et al. (2010); Chang & Lin (2007); Chia et al. (2002, 2003); Da Veiga & Eloff (2007, 2010); Da Veiga & Martins (2015); Dhillon & Torkzadeh (2006); Flores & Ekstedt (2016); Lacey (2010); Lim et al. (2012); Mishra (2015); Myyry et al. (2009); Rastogi & Von Solms (2012); Ross (2011); Ruighaver et al. (2007); Schlienger & Teufel (2002); Vroom & Von Solms (2004).

Tableau 2.3 : Les croyances susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite et fin)

Croyance	Définition (A), propositions (B) et items (C) liés à la croyance	Auteur(s)
LE MAILLON FAIBLE EN SÉCURITÉ DE L'INFORMATION	(A) Croyance partagée dans l'organisation quant au rôle que joue l'être humain dans la sécurité de l'information. (B) Plus on croit dans l'organisation que les gens représentent le maillon faible en sécurité de l'information, moins les employés seront motivés à mettre en œuvre des pratiques sécuritaires parce que l'entreprise mettra en place des outils menant à une déresponsabilisation. À l'opposé, si on croit que les gens sont des maillons importants de la sécurité de l'information, plus élevées sont les chances que l'organisation leur fera confiance, les responsabilisera et que les employés agiront dans le meilleur intérêt de l'organisation en mettant en œuvre des pratiques sécuritaires. (C) • Dans mon organisation, on croit que les gens constituent le maillon faible en sécurité de l'information. • Dans mon organisation, on croit que les gens sont des joueurs-clé dans la protection de l'information. • Dans mon organisation, on considère les gens comme étant la principale cause des incidents liés à la sécurité de l'information. • Dans mon organisation, on croit que les gens peuvent jouer un rôle essentiel pour minimiser les risques liés à la sécurité de l'information.	Bulgurcu et al. (2010); Chen et al. (2015); Chia et al. (2002); Da Veiga & Eloff (2007); Schlienger & Teufel (2002); Van Niekerk & Von Solms (2010); Vroom & Von Solms (2004).

Tableau 2.4 : Les valeurs susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés

Valeurs	Définition (A), propositions (B) et items (C) liés à la valeur	Auteur(s)
BASES GÉNÉRALES SUR LESQUELLES LES DÉCISIONS SONT PRISES DANS L'ORGANISATION	(A) Valeur partagée dans l'organisation quant aux bases sur lesquelles les décisions doivent être prises au sein de l'organisation. (B) Plus l'organisation privilégie les bases quantitatives pour asseoir ses décisions (analyses quantitatives, métriques, benchmarking, etc.), plus élevées sont les chances qu'elle évaluera les aspects liés à la sécurité de l'information d'une manière globale et complète menant à la mise en place d'outils stimulant davantage les employés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si on tend à privilégier des décisions basées sur l'intuition et les émotions (« gut feelings »), plus élevées sont les chances que l'on négligera de conduire une évaluation rigoureuse des aspects liés à la sécurité de l'information, menant ainsi à l'absence d'outils favorisant la mise en œuvre de pratiques sécuritaires. (C) Dans mon environnement de travail, on privilégie l'intuition et les émotions (« gut feelings ») plutôt que les « chiffres » (analyses quantitatives, métriques, benchmarking, etc.) au moment de prendre une décision. • Dans mon environnement de travail, on pense qu'accorder une grande importance à l'intuition et aux émotions (« gut feelings ») au moment de prendre des décisions mène à de mauvaises décisions. • Dans mon environnement de travail, les « chiffres » (analyses quantitatives, métriques, benchmarking, etc.) sont toujours les critères les plus importants au moment de prendre une décision. • Dans mon environnement de travail, une décision ne peut être prise que sur la base de « chiffres » solides (analyses quantitatives, métriques, benchmarking, etc.).	Da Veiga & Martins (2015); D'Arcy & Green (2014); Dhillon & Torkzadeh (2006); Lacey (2010); Lim et al. (2015); Martins & Eloff (2002); Mishra (2015); Parsons (2010, 2015); Ross (2011); Von Solms (2000).

Tableau 2.4 : Les valeurs susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite)

Valeurs	Définition (A), propositions (B) et items (C) liés à la valeur	Auteur(s)
HORIZON TEMPOREL HABITUEL DE LA PLANIFICATION DANS L'ORGANISATION	(A) Valeur partagée dans l'organisation qui reflète les habitudes de planification de l'organisation. (B) Plus l'organisation a l'habitude de planifier à long terme, plus élevées sont les chances qu'elle le fera aussi en sécurité de l'information, ce qui l'amènera à faire les investissements requis afin de favoriser la mise en œuvre de pratiques sécuritaires. À l'opposé, si le focus de l'organisation est surtout à court terme, moins élevées sont les chances que la sécurité de l'information fera l'objet des investissements nécessaires à la mise en œuvre de pratiques sécuritaires. (C) • Dans mon environnement de travail, on se concentre principalement sur l'atteinte d'objectifs à court terme. • Dans mon environnement de travail, on croit aux bénéfices de la planification à long terme (3 ans et plus). • Dans mon environnement de travail, on pense que de planifier à long terme (3 ans et plus) est une perte de temps. • On peut affirmer que, dans mon environnement de travail, on a un focus « court terme ».	Chang & Lin (2007); Chia et al. (2002, 2003); Da Veiga & Eloff (2010); Lacey (2010); Ruighaver et al. (2007); Thomson & Von Solms (2005).

Tableau 2.4 : Les valeurs susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite)

Valeurs	Définition (A), propositions (B) et items (C) liés à la valeur	Auteur(s)
PRÉDISPOSITIONS ÉTHIQUES DE L'ORGANISATION	(A) Valeur partagée dans l'organisation quant à la place de l'éthique dans l'organisation. (B) Plus l'organisation adopte une position éthique dans la conduite générale de ses affaires, plus élevées sont les chances qu'elle le fera aussi pour protéger les informations, menant ainsi à la mise en œuvre de pratiques sécuritaires. À l'opposé, si l'éthique n'est pas une valeur importante dans l'organisation, cela affectera négativement la mise en œuvre de pratiques peu sécuritaires. (C) • Les comportements éthiques sont la norme dans mon environnement de travail. • Dans mon environnement de travail, les gestionnaires guident les processus décisionnels dans une direction éthique. • Dans mon environnement de travail, les gestionnaires ne sont pas des modèles de décision éthique. • Dans mon environnement de travail, les gestionnaires adhèrent à des normes éthiques élevées.	Da Veiga & Martins (2015); Dhillon & Torkzadeh (2006); Gaunt (2000).

Tableau 2.4 : Les valeurs susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite)

Valeurs	Définition (A), propositions (B) et items (C) liés à la valeur	Auteur(s)
ATTITUDE DES EMPLOYÉS ENVERS LA CONFORMITÉ	(A) Valeur partagée dans l'organisation quant au respect des règles et des politiques définies au sein de l'organisation. (B) Plus il existe dans l'organisation une prédisposition à respecter les règles et les politiques définies, plus élevées sont les chances que les employés respecteront aussi les pratiques de sécurité de l'information définies. À l'opposé, s'il existe un mépris généralisé envers les règles et les politiques organisationnelles, les chances sont que la même chose se produira pour la mise en œuvre des pratiques de sécurité de l'information définies par l'entreprise. (C) • Dans mon environnement de travail, l'autonomie individuelle est plus valorisée que le respect des politiques et règlements de l'organisation. • Dans mon environnement de travail, il est laissé au bon jugement de chacun des employés de décider si le respect des politiques et règlements est la meilleure chose à faire à un certain moment. • Dans mon environnement de travail, le respect des politiques et règlements de l'organisation est très important. • Dans mon environnement de travail, suivre à la lettre les politiques et règlements de l'organisation est considéré comme étant très important.	Batteau (2011); Chang & Lin (2007); Chia et al. (2002, 2003); Da Veiga & Martins (2015); Gaunt (2000); Lim et al. (2012, 2015); Mishra (2015); Rantos et al. (2012); Ruighaver et al. (2007); Tang et al. (2016); Vroom & Von Solms (2004).

Tableau 2.4 : Les valeurs susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite)

Valeurs	Définition (A), propositions (B) et items (C) liés à la valeur	Auteur(s)
IMPORTANCE ACCORDÉE AU DÉVELOPPEMENT DES RESSOURCES HUMAINES	(A) Valeur partagée dans l'organisation qui réfère à l'importance qu'a le développement des connaissances et des habiletés des employés dans l'organisation. (B) Plus il existe dans l'organisation une valorisation du développement des ressources humaines, plus élevées sont les chances que le même sentiment sera instauré par rapport à la sécurité de l'information et que les employés recevront tout le soutien nécessaire à la mise en œuvre de pratiques sécuritaires. À l'opposé, si le développement n'est pas valorisé, moins les employés mettront en œuvre des pratiques sécuritaires parce qu'ils seront livrés à eux-mêmes, sans soutien, ni formation. (C) • Dans mon environnement de travail, on appuie fortement la formation continue des employés. • Dans mon environnement de travail, le développement de la main-d'œuvre n'est pas une priorité. • Dans mon environnement de travail, on prend au sérieux le développement continu des habiletés de chaque employé afin de maximiser sa contribution au succès de l'organisation. • Dans mon environnement de travail, la formation continue de ses employés ne figure pas sur la liste de priorités.	Chia et al. (2002); Dhillon & Torkzadeh (2006); Dojkovski et al. (2010); Flores & Ekstedt (2012); Lim et al. (2010); Mishra (2015); Ruighaver et al. (2007).

Tableau 2.4 : Les valeurs susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite)

Valeurs	Définition (A), propositions (B) et items (C) liés à la valeur	Auteur(s)
ATTITUDE GÉNÉRALE DES EMPLOYÉS FACE AU CHANGEMENT	(A) Valeur partagée dans l'organisation quant à la façon de réagir au changement organisationnel. (B) Plus on valorise l'ouverture au changement dans l'organisation, plus il sera facile de changer les pratiques organisationnelles afin que les employés mettent en œuvre des pratiques de plus en plus sécuritaires. À l'opposé, si on tend à résister au changement, les chances sont plus élevées que les changements engendrés par la mise en œuvre de pratiques de plus en plus sécuritaires seront difficiles à accepter. (C) • Dans mon environnement de travail, on tend à résister aux changements dans les façons de faire. • Dans mon environnement de travail, on adopte facilement les changements aux façons de faire. • Dans mon environnement de travail, on accepte facilement que les façons de faire évoluent et changent. • Dans mon environnement de travail, le changement rend les gens très inconfortables.	Batteau (2011); Chang & Lin (2007); Chia et al. (2002, 2003); Da Veiga & Martins (2015); Gaunt (2000); Lim et al. (2012, 2015); Mishra (2015); Rantos et al. (2012); Ruighaver et al. (2007); Tang et al. (2016); Vroom & Von Solms (2004).

Tableau 2.4 : Les valeurs susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite)

Valeurs	Définition (A), propositions (B) et items (C) liés à la valeur	Auteur(s)
FORCE DU RÉSEAU AU SEIN DE L'ORGANISATION	(A) Valeur partagée dans l'organisation quant à la façon dont les gens travaillent ensemble (force du réseau intra-organisationnel). (B) Plus un réseau fort existe entre les membres de l'organisation, plus élevées sont les chances que les employés s'appuieront, se conseilleront et discuteront les problématiques liées à la sécurité de l'information, le tout favorisant la mise en œuvre de pratiques sécuritaires. À l'opposé, si les employés évoluent dans un environnement « en silo », l'individu sera livré à lui-même, ce qui aura pour effet de nuire à la mise en œuvre de pratiques sécuritaires. (C) • Mon environnement de travail est caractérisé par un véritable esprit d'équipe. • La coopération et le partage de l'information sont deux mots qui décrivent très bien mon environnement de travail. • Dans mon environnement de travail, on peut toujours compter sur les autres pour obtenir de l'aide et de bons conseils. • Dans mon environnement de travail, les gens se soutiennent les uns les autres dans l'exécution de leur travail.	Chang & Lin (2007); Chia et al. (2002, 2003); Dhillon & Torkzadeh (2006); Flores & Ekstedt (2016) Mishra (2015); Ruighaver et al. (2007); Safa et al. (2016).

Tableau 2.4 : Les valeurs susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite)

Valeurs	Définition (A), propositions (B) et items (C) liés à la valeur	Auteur(s)
RÉACTION HABITUELLE DE L'ORGANISATION FACE AUX PROBLÈMES	(A) Valeur partagée dans l'organisation quant à la réaction première de l'organisation face à un problème ou à un incident. (B) Plus la réaction instinctive de l'organisation face à un problème ou à un incident est de pointer un coupable, moins les employés seront motivés à partager les problèmes/incidents/difficultés entre eux et plus élevées sont les chances que les employés mettront en œuvre des pratiques non sécuritaires. À l'opposé, si la réaction est plutôt d'encourager les employés à partager leurs problèmes/incidents/difficultés, plus les chances sont élevées que ce sera aussi la même chose dans le cas de la sécurité de l'information, menant ainsi à la mise en œuvre de pratiques plus sécuritaires. (C) • Dans mon environnement de travail, lorsque qu'un problème survient, le premier réflexe est de chercher un coupable. • Dans mon environnement de travail, lorsque survient un problème, on tend à vouloir se protéger en identifiant un bouc émissaire. • Dans mon environnement de travail, on nous encourage à partager nos problèmes plutôt que de les cacher. • Mon environnement de travail a une atmosphère où les problèmes peuvent être exprimés et discutés.	Batteau (2011); Lacey (2010); Mishra (2015); Tang et al. (2016).

Tableau 2.4 : Les valeurs susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite et fin)

Valeurs	Définition (A), propositions (B) et items (C) liés à la valeur	Auteur(s)
RÉPONSE HABITUELLE DE L'ORGANISATION FACE AUX PRESSIONS EXTERNES	(A) Valeur partagée dans l'organisation qui réfère à la réponse habituelle de l'organisation face aux pressions provenant des clients, gouvernement, standards nationaux et internationaux, etc. (B) Plus l'organisation a tendance à adopter des comportements symboliques face aux obligations externes (clients, gouvernements, standards, etc.), plus élevées sont les chances qu'elle fera la même chose en ce qui a trait à la sécurité de l'information, au total menant à la mise en œuvre de pratiques moins sécuritaires. Au contraire, si l'organisation tend à prendre ces obligations/recommandations comme une occasion d'améliorer ses pratiques internes, les chances sont qu'elle fera la même chose en sécurité de l'information, ce qui mènera à la mise en œuvre de pratiques plus sécuritaires. (C) • Dans mon environnement de travail, publiciser à l'externe que nos pratiques internes de sécurité de l'information sont solides est plus important que les pratiques elles-mêmes. • Dans mon environnement de travail, on prend au sérieux les pratiques de sécurité imposées/recommandées par les organismes externes en nous assurant que des pratiques internes correspondantes soient implantées. • Dans mon environnement de travail, on croit que l'objectif en sécurité de l'information est de faire le minimum qui permet de passer les tests de conformité. • Dans mon environnement de travail, on pense que le respect des pratiques de sécurité imposées par des organismes externes représente des occasions d'améliorer nos pratiques internes.	Batteau (2011); Chia et al. (2002); Chang & Lin (2007); Lim et al. (2015); Mishra (2015); Parsons et al. (2015); Ross (2011); Ruighaver et al. (2007).

L'élaboration d'une définition claire de la culture de la sécurité de l'information basée sur des fondements théoriques a contribué au recensement des croyances et des valeurs susceptibles d'influencer la mise en œuvre de pratiques sécuritaires. Le chapitre 3 présentera la méthodologie qui sera utilisée pour la validation de cette liste de sept croyances et de neuf valeurs par des professionnels en sécurité de l'information.

2.2.2 Le climat de la sécurité de l'information

Cette section vise à mieux comprendre le climat de la sécurité de l'information et son influence sur la variable dépendante. Cette sous-section suit la même structure que la sous-section 2.2.1, portant sur la culture de la sécurité de l'information. À l'issue de cette sous-section, une conceptualisation du climat de la sécurité de l'information sera présentée.

2.2.2.1 Définitions du climat de la sécurité de l'information telles que retrouvées dans la littérature

Les chercheurs ne se sont intéressés à l'étude du climat de la sécurité de l'information que très récemment. Les premiers écrits concernant ce construit remontent aux années 2000, avec Chan et al. (2005) qui en proposent une première conceptualisation. Ce n'est que durant la dernière décennie que le construit a bénéficié d'une attention plus particulière de la part des chercheurs (par exemple, Goo et al., 2013; Dang-Pham et al., 2015; Padayachee, 2012).

Une revue de la littérature a été conduite dans l'optique de recueillir des définitions du climat de la sécurité de l'information. Celles-ci permettent d'obtenir un premier éclairage quant à la façon de le définir et son influence potentielle sur la variable dépendante. Le tableau 2.5 présente donc les définitions du climat de la sécurité de l'information qui ont été tirées de la littérature et les auteurs qui les ont formulées.

Tableau 2.5 : Définitions du climat de la sécurité de l'information de la littérature

Auteur(s)	Définition du climat de la sécurité de l'information	Angle du construit
Chan et al. (2005)	"Perceived information security climate is defined as the employee's perception of the current organizational state in terms of information security as evidenced through dealings with internal and external stakeholders." (p.25)	Perception des employés
Dang-Pham et al. (2015)	"Information security climate construct may have four dimensions, namely (1) leadership, (2) job & role, (3) workgroup, and (4) organisational systems." (p.2)	Ensemble de pratiques
Goo et al. (2013)	"We believe that information security climate is a high-order factor composed of a collective effort of four organizational security practices. […] They are top management attention, security enforcement, security awareness program, and security policies." (p. 2960)	Ensemble de pratiques
Jaafar & Ajis (2013)	"Climate in this approach is viewed as a summary or global perception held by individuals about their organisational environment. […] There are three factors [composing information security climate], namely, Upper Management Practice (UMP), Direct Supervisory Practice (DSP) and Co-worker Socialization (CWS)." (p. 120)	Perception des employés et ensemble de pratiques
Padayachee (2012)	"The social climate class includes peer behavior, management practices and social disapproval, and may persuade an individual to maintain security controls so as to protect his/her self-esteem." (p.676-677)	Ensemble de pratiques

Le recensement des définitions du climat de la sécurité de l'information a permis de constater que le construit ne fait pas consensus parmi les auteurs l'ayant étudié. On remarque, d'une part, que certains auteurs le perçoivent comme étant la perception des employés quant à leur environnement organisationnel. En effet, Chan et al. (2005) et Jaafar & Ajis (2013) stipulent que le climat de la sécurité de l'information consiste en la perception qu'ont les employés quant à l'état de leur environnement organisationnel. Jaafar & Ajis (2013) précisent que le construit est constitué des perceptions basées sur les pratiques organisationnelles (par exemple, les pratiques de la haute direction, les pratiques du supérieur immédiat ainsi que les pratiques de socialisation des employés).

À l'instar de Jaafar & Ajis (2013), Dang-Pham et al. (2015), Goo et al. (2013) et Padayachee (2012) définissent le construit de climat de la sécurité de l'information comme étant un ensemble de pratiques et de normes organisationnelles qui vont influencer la mise en œuvre de pratiques sécuritaires par les employés. Selon Dang-Pham et al. (2015), le construit est composé de quatre dimensions, soit le *leadership*, le poste et le rôle des employés, le travail d'équipe ainsi que les systèmes organisationnels. Ces dimensions catégorisent les pratiques et les normes organisationnelles à mettre en place afin d'encourager les employés à mettre en œuvre des pratiques sécuritaires. Goo et al. (2013),

quant à eux, se concentrent sur l'attention de la haute direction envers la sécurité de l'information, la mise en place de la sécurité de l'information, le programme de sensibilisation à la sécurité de l'information ainsi que les politiques de sécurité de l'information. Enfin, d'après Padayachee (2012), le climat de la sécurité de l'information est constitué de la pression des pairs, de la désapprobation sociale ainsi que des pratiques organisationnelles visant à influencer les employés à mettre en œuvre des pratiques sécuritaires.

À la lumière des définitions recensées, on constate que ces dernières partagent des points communs. D'une part, certaines de ces définitions s'intéressent à la perception des employés quant à leur environnement organisationnel (par exemple, Chan et al., 2005; Jaafar & Ajis, 2013). D'autre part, contrairement aux définitions de la culture de la sécurité de l'information, la plupart d'entre elles semblent mettre davantage l'accent sur les pratiques organisationnelles (par exemple, Dang-Pham et al., 2015; Goo et al., 2013; Jaafar & Ajis, 2013; Padayachee, 2012). Il peut dès lors s'avérer pertinent de consulter la littérature du climat organisationnel et d'en examiner les fondements théoriques afin de relever toute connaissance additionnelle qui pourrait bonifier la définition du climat de la sécurité de l'information que l'on souhaite développer.

2.2.2.2 Le climat de la sécurité de l'information: définition proposée

La section précédente a permis de s'apercevoir que les définitions du climat de la sécurité de l'information recueillies adressaient des idées communes.. Cette section a donc pour objectif d'enrichir la compréhension du construit en étudiant les fondements théoriques liés au climat organisationnel afin de relever toute connaissance additionnelle permettant de bonifier la compréhension du construit et de développer une définition qui soit fondée sur des bases théoriques solides.

Tel que mentionné dans la sous-section précédente, les chercheurs ne se sont intéressés au climat de la sécurité de l'information que très récemment. Cette littérature trouve ancrage dans la littérature portant sur le climat organisationnel et qui a été très prolifique au cours des années 1970. En effet, Campbell (1970), James & Jones (1974) ou encore Schneider (1975) comptent parmi les chercheurs qui ont contribué au développement des connaissances sur le sujet. Il s'avère dont pertinent de consulter la littérature sur le climat organisationnel dans l'optique de comprendre, et ainsi, de conceptualiser le climat de la sécurité de l'information.

Dès lors, ce mémoire exploitera la conceptualisation du climat organisationnel de James & Jones (1974) afin de mieux comprendre le construit, mais aussi pour développer une nouvelle définition du climat de la sécurité de l'information. La conceptualisation de James & Jones (1974) a été choisie, car elle est considérée comme étant le fondement théorique

incontournable dans la littérature traitant du climat organisationnel (Ashkanasy et al., 2011). De plus, la conceptualisation proposée par ces auteurs a été citée dans plusieurs études en technologies de l'information, telles que celles de Pliskin et al. (1993), Potosky & Ramakrishna (2002) et de Romm et al. (1991).

Selon James & Jones (1974), le climat organisationnel réfère aux perceptions des employés quant à ce représente leur organisation en termes de pratiques, de politiques, de procédures organisationnelles, mais aussi de règles, de normes, de routines ainsi que de récompenses.

L'examen des définitions du climat de la sécurité de l'information tirées de la littérature (figurant à la section 2.2.2.1) montre que ces dernières couvrent des idées similaires. Il s'est avéré pertinent de consulter les fondements théoriques concernant le climat organisationnel afin de relever des connaissances pouvant bonifier les définitions existantes. Par conséquent, la conceptualisation de James & Jones (1974) a été mise à profit au service de l'élaboration d'une définition du climat de la sécurité de l'information qui se veut plus précise :

*« Le **climat de la sécurité de l'information** correspond aux perceptions partagées au sein de l'organisation quant aux politiques organisationnelles, aux règles, aux normes et aux pratiques de sécurité mises en œuvre. Le climat de la sécurité de l'information représente les perceptions partagées par les employés à propos de « comment les choses se passent chez nous. »*

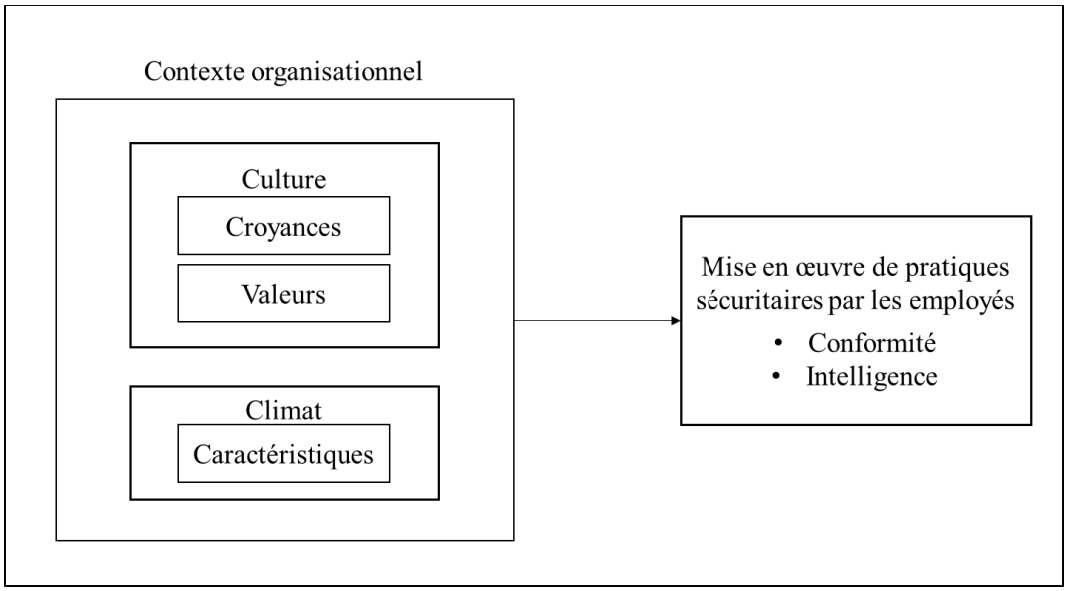
Cette définition est donc essentielle dans la conceptualisation de ce qu'est le climat de la sécurité de l'information. Elle permet ensuite de déterminer les aspects du climat organisationnel qui seraient susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés.

2.2.2.3 Les caractéristiques du climat organisationnel

Dans leur étude, Forehand & Von Haller (1964) se sont intéressés à la matérialisation du climat organisationnel. Selon eux, le climat organisationnel prend forme à travers différents aspects qu'ils nomment « caractéristiques du climat ». Ces dernières décrivent l'état actuel d'une organisation, permettent de la distinguer des autres organisations, sont stables à long terme et exercent une influence sur les comportements des employés (Forehand & Von Haller, 1964). D'ailleurs, Campbell et al. (1970) et Ashkanasy et al. (2011) reconnaissent que les caractéristiques du climat sont les forces clés qui influencent les actions et les comportements des employés d'une organisation. Par exemple, pour expliquer la motivation des employés au travail, Litwin & Stringer (1968) ont considéré la collaboration, l'engagement, les systèmes de récompenses, la compétence des employés et l'appui des gestionnaires comme des caractéristiques du climat et, par conséquent, comme

des sources d'influence sur les comportements des employés. Ainsi, pour mieux comprendre comment influencer la mise en œuvre de pratiques sécuritaires par les employés, il faut se pencher sur les caractéristiques du climat de la sécurité de l'information. L'influence de ces caractéristiques du climat sur la variable dépendante est représentée dans la figure 2.3.

Figure 2.3 : L'influence des caractéristiques du climat sur la mise en œuvre de pratiques sécuritaires par les employés



Tout comme pour les croyances et les valeurs de la sécurité de l'information, afin d'atteindre l'objectif de recherche de ce mémoire, il était nécessaire de dresser une liste exhaustive des caractéristiques du climat en sécurité de l'information pour expliquer la mise en œuvre de pratiques sécuritaires par les employés.

Approche méthodologique utilisée pour identifier les caractéristiques du climat organisationnel susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés

Pour identifier les caractéristiques du climat, la même approche que celle utilisée pour l'identification des valeurs et croyances a été utilisée. Ainsi, une revue de la littérature et un exercice d'extractions et de codage ont été réalisés. Dans la base de données ABI/Inform, le terme « *information security climate* » a été utilisé afin de recueillir des publications relatives au climat de la sécurité de l'information. Il a toutefois été possible de constater que plusieurs aspects classiquement considérés comme des caractéristiques du climat étaient utilisés ou intégrés à la littérature portant sur la culture de la sécurité de l'information. Il a donc fallu conduire une recherche étendue afin de relever autant que possible toutes les caractéristiques inhérentes au climat de la sécurité de l'information qui s'avéraient importantes pour expliquer la variable dépendante. À l'instar des croyances et des valeurs, identifier les caractéristiques du climat de la sécurité de l'information dans les publications s'est avéré grandement laborieux. En effet, les caractéristiques du climat ne

sont pas explicitement identifiées dans les écrits. Malgré tout, la littérature est riche en anecdotes et a permis de relever la connaissance pertinente. Les articles recensés ont donc été soumis à une analyse minutieuse afin d'identifier les caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés. Sur la base de la définition élaborée dans la section 2.2.2.2, il a fallu identifier toutes « *les politiques organisationnelles, les règles, les normes et les pratiques de sécurité* » qui pourraient influencer la mise en œuvre de pratiques sécuritaires par les employés.

Inventaire des caractéristiques du climat organisationnel tirées de la littérature

Le recensement a permis d'identifier 11 caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires et de formuler leur définition et les items qui leur sont associés. Le tableau 2.6 expose ces caractéristiques du climat, leur définition (A), leurs propositions (B) et leurs items (C) ainsi que les auteurs dont les études ont servi de base à ce travail.

Tableau 2.6 : Les caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires

Caractéristique du climat	Définition (A), propositions (B) et items (C) liés à la caractéristique du climat	Auteur(s)
SOUTIEN PROJETÉ PAR LES GESTIONNAIRES	(A) Cette caractéristique du climat réfère aux gestes et comportements des gestionnaires par rapport à la sécurité de l'information. (B) Plus les gestionnaires ont tendance à montrer un appui à la sécurité de l'information (par leurs gestes, paroles, décisions et appuis concrets (comme des ressources financières), plus les employés comprendront que la sécurité de l'information est importante dans leur environnement de travail et seront motivés à mettre eux aussi en œuvre des pratiques sécuritaires. À l'opposé, si le message reçu des gestionnaires est que la sécurité de l'information a peu d'importance dans leur environnement de travail, plus les chances sont élevées que les pratiques sécuritaires ne seront pas mises en œuvre. (C) • Dans mon environnement de travail, les gestionnaires montrent l'exemple en respectant les pratiques de sécurité de l'information définies. • Dans mon environnement de travail, les gestionnaires tendent à ne pas respecter une pratique de sécurité de l'information si elle empêche un projet ou une décision qui leur tient à cœur d'aller de l'avant. • Dans mon environnement de travail, les gestionnaires nous demandent parfois de faire des choses qui vont à l'encontre des pratiques de sécurité de l'information définies. • Dans mon environnement de travail, les gestionnaires octroient les ressources (temps, budget, personnel, etc.) nécessaires pour mettre en œuvre les pratiques permettant une protection adéquate de l'information.	Batteau (2011); Chan et al. (2005); D'Arcy & Green (2014); Dojkovski et al. (2010); Flores & Ekstedt (2012); Knapp & Ferrante (2014); Jalal-Karim (2013); Lacey (2010); Lim et al. (2009); Lim et al. (2010); Martins & Eloff (2002); Mishra (2015); Ngo et al. (2005); Parsons et al. (2015); Schlienger & Teufel (2002); Von Solms (2000) .

Tableau 2.6 : Les caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires (suite)

Caractéristique du climat	Définition (A), propositions (B) et items (C) liés à la caractéristique du climat	Auteur(s)
COMMUNICATION ORGANISATION-NELLE	(A) Cette caractéristique du climat réfère à la capacité de l'organisation à communiquer des messages clairs par rapport à la sécurité de l'information. (B) Plus l'organisation arrive à communiquer des messages clairs quant à la sécurité de l'information (objectifs, importance, attentes, etc.), plus les employés seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si les messages sont absents ou confus, plus les chances sont élevées que les pratiques sécuritaires ne seront pas mises en œuvre. (C) • Mon organisation communique aux employés une vision claire de la sécurité de l'information et de ses objectifs. • Dans mon environnement de travail, le rôle que les employés jouent dans l'effort global de protection de l'information est clairement communiqué. • Dans mon environnement de travail, les attentes en termes de sécurité de l'information sont clairement communiquées. • Dans mon environnement de travail, on nous explique clairement l'importance de la sécurité de l'information.	Alhogail (2015); Batteau (2011); Bulgurcu et al. (2010); Chan et al. (2005); Chen et al. (2015); Da Veiga & Eloff (2007); Da Vega & Martins (2015); D'Arcy & Green (2014); Dhillon & Torkzadeh (2006); Dojkovski et al. (2010); Faily & Fléchais (2010); Flores & Ekstedt (2012); Gaunt (2000); Helokunnas & Kuusisto (2003); Lim et al. (2009); Lim et al. (2010); Lim et al. (2012); Martins & Eloff (2002); Mishra (2015); Myyry et al. (2009); Nosworthy (2000); Ngo et al. (2005); Safa et al. (2016); Schlienger & Teufel (2002); Siponen (2000); Tang et al. (2015); Vroom & Von Solms (2004); Williams et al. (2014).

Tableau 2.6 : Les caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires (suite)

Caractéristique du climat	Définition (A), propositions (B) et items (C) liés à la caractéristique du climat	Auteur(s)
SOUTIEN À L'APPRENTISSAGE	(A) Cette caractéristique du climat réfère aux moyens mis en place pour soutenir les employés dans la mise en œuvre des pratiques de sécurité. (B) Plus l'organisation met en place les outils qui permettent de soutenir la formation et le développement de connaissances en sécurité de l'information, plus les employés seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si les employés ne reçoivent pas le soutien nécessaire, plus les chances sont élevées que les pratiques sécuritaires ne seront pas mises en œuvre. (C) • Mon organisation met en place les moyens assurant que chaque employé comprenne bien les pratiques de sécurité de l'information dont il a la responsabilité. • Dans mon environnement de travail, les employés reçoivent le soutien nécessaire (en termes de formation, assistance, documents de référence, etc.) afin de pouvoir mettre en œuvre les pratiques de sécurité de l'information dont ils ont la responsabilité. • Dans mon environnement de travail, on donne aux employés les moyens d'améliorer leurs habiletés pour faire face aux défis de la sécurité de l'information. • Dans mon environnement de travail, les employés se sentent bien outillés face aux défis que représente la sécurité de l'information.	Albrechtsen & Hovden (2010); Batteau (2011); Bulgurcu et al. (2010); Chan et al. (2005); Chang et al. (2007); Chen et al. (2015); Da Vega & Martins (2015); D'Arcy & Green (2014); Dhillon & Torkzadeh (2006); Dojkovski et al. (2010); Flores & Ekstedt (2012); Gaunt (2000); Helokunnas & Kuusisto (2003); Lacey (2010); Lim et al. (2009); Lim et al. (2010); Lim et al. (2012); Lyu & Zhang (2015); Martins & Eloff (2002); Mishra (2015); Nosworthy (2000); Ng et al. (2009); Parsons et al. (2010); Rhee et al. (2009); Safa et al. (2016); Schlienger & Teufel (2002); Siponen (2000); Tang et al. (2015); Williams et al. (2014).

Tableau 2.6 : Les caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires (suite)

Caractéristique du climat	Définition (A), propositions (B) et items (C) liés à la caractéristique du climat	Auteur(s)
IMPLICATION DES EMPLOYÉS	(A) Cette caractéristique du climat renvoie à l'implication des employés aux étapes du cycle de vie des pratiques de sécurité de l'information. (B) Plus les employés se sentent impliqués dans l'élaboration et l'évolution des pratiques de sécurité, plus les employés seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si les employés ne se sentent pas impliqués, plus élevées sont les chances que les pratiques sécuritaires ne seront pas mises en œuvre. (C) • Dans mon environnement de travail, les employés se sentent impliqués dans l'évolution des pratiques de sécurité de l'information. • Dans mon environnement de travail, les suggestions des employés pour améliorer les pratiques de sécurité de l'information sont prises au sérieux. • Dans mon environnement de travail, l'implication des employés dans l'évolution des pratiques de sécurité de l'information est considérée comme étant incontournable. • Dans mon environnement de travail, les employés ne se sentent pas consultés sur les pratiques de sécurité à mettre en place.	Batteau (2011); Bulgurcu et al. (2010); Chen et al. (2015); D'Arcy & Green (2014); Dhillon & Torkzadeh (2006); Faily & Fléchais (2010); Flores & Ekstedt (2012); Gaunt (2000); Lacey (2010); Lim et al. (2012); Mishra (2015); Myyry et al. (2009); Ngo et al. (2005); Parsons et al. (2010); Parsons et al. (2015); Safa et al. (2016); Siponen (2000); Schlienger & Teufel (2002).

Tableau 2.6 : Les caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires (suite)

Caractéristique du climat	Définition (A), propositions (B) et items (C) liés à la caractéristique du climat	Auteur(s)
ADÉQUATION AU CONTEXTE ORGANISATION-NEL	(A) Cette caractéristique du climat réfère à l'adéquation (le « fit ») entre les pratiques de sécurité de l'information dans l'organisation et les caractéristiques du contexte organisationnel. (B) Plus les pratiques de sécurité de l'information définies sont en adéquation avec les caractéristiques du contexte organisationnel comme la culture et les pratiques d'affaires, plus les employés seront enclins à mettre en œuvre ces pratiques sécuritaires. À l'opposé, s'il y a un « misfit » entre les pratiques de sécurité de l'information et les caractéristiques du contexte organisationnel, plus élevées sont les chances que les pratiques sécuritaires ne seront pas mises en œuvre. (C) • Les pratiques de sécurité de l'information sont bien alignées sur les pratiques d'affaires de mon organisation. • Les pratiques de sécurité de l'information respectent la culture de mon organisation. • Les pratiques de sécurité de l'information sont souvent en contradiction avec la façon dont mon organisation mène ses affaires. (reverse) • Dans mon environnement de travail, la culture de mon organisation représente un obstacle à la mise en œuvre de certaines pratiques de sécurité de l'information.	Alhogail (2015); Chang et al. (2007); Flores & Ekstedt (2016); Helokunnas & Kuusisto (2003); Mishra (2015).

Tableau 2.6 : Les caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires (suite)

Caractéristique du climat	Définition (A), propositions (B) et items (C) liés à la caractéristique du climat	Auteur(s)
ADÉQUATION AUX TÂCHES	(A) Cette caractéristique du climat réfère à l'adéquation (le « fit ») entre les pratiques de sécurité de l'information dans l'organisation et les tâches à réaliser. (B) Plus les pratiques de sécurité de l'information définies sont en adéquation avec la tâche (effort minimal, impact marginal sur le rendement, etc.), plus les employés seront enclins à mettre ces pratiques sécuritaires en œuvre. À l'opposé, si les pratiques ajoutent une lourdeur au travail quotidien, plus les chances sont élevées que les pratiques sécuritaires ne seront pas mises en œuvre. (C) • Dans mon environnement de travail, les pratiques de sécurité de l'information sont définies par des personnes qui ne comprennent pas le travail sur le terrain. • Dans mon environnement de travail, les employés croient que les pratiques de sécurité sont définies sans prendre en considération les impacts qu'elles ont sur leur travail. • Dans mon environnement de travail, on pense qu'il est difficile de respecter les pratiques de sécurité de l'information si on veut accomplir le travail demandé. • Dans mon environnement de travail, les pratiques de sécurité de l'information ont été définies de façon à ne pas nuire au rendement au travail.	Batteau (2011); Flores & Ekstedt (2016); Gaunt (2000); Lim et al. (2012).

Tableau 2.6 : Les caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires (suite)

Caractéristique du climat	Définition (A), propositions (B) et items (C) liés à la caractéristique du climat	Auteur(s)
ENGAGEMENT ORGANISATION-NEL	(A) Cette caractéristique du climat renvoie au lien affectif qui unit les employés à l'organisation. (B) Plus les employés ont un sentiment partagé d'attachement à l'organisation, plus ils seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, plus un désengagement général est présent, plus les chances sont élevées que les pratiques sécuritaires ne seront pas mises en œuvre. (C) • Dans mon environnement de travail, les employés sont prêts à mettre beaucoup d'effort pour aider notre organisation à connaître le succès. • Dans mon environnement de travail, les employés tendent à parler très positivement de notre organisation. • Dans mon environnement de travail, les employés sont émotionnellement attachés à notre organisation. • Dans mon environnement de travail, les employés font preuve de peu de loyauté envers notre organisation.	Batteau (2011); Dhillon & Torkzadeh (2006); Gaunt (2000); Hu et al. (2012); Knapp et al. (2006); Nosworthy (2000); Parsons et al. (2010); Parsons et al. (2015); Safa et al. (2016).

Tableau 2.6 : Les caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires (suite)

Caractéristique du climat	Définition (A), propositions (B) et items (C) liés à la caractéristique du climat	Auteur(s)
COMMUNICATION DES PROBLÈMES/ ERREURS	(A) Cette caractéristique du climat réfère à la possibilité de discuter ouvertement dans l'environnement de travail des problèmes/erreurs liés à la mise en œuvre des pratiques de sécurité de l'information. (B) Plus l'environnement de travail permet de discuter ouvertement des problèmes/erreurs liés à la mise en œuvre des pratiques de sécurité, plus les employés seront enclins à communiquer les problèmes/erreurs rencontrés, le tout favorisant la mise en œuvre de pratiques sécuritaires. À l'opposé, si l'environnement favorise plutôt de ne pas révéler et même de cacher les problèmes/erreurs, moins élevées sont les chances que les employés mettront en œuvre de pratiques sécuritaires. (C) • Dans mon environnement de travail, les problèmes liés à l'application des pratiques de sécurité peuvent être ouvertement discutés. • Dans mon environnement de travail, les erreurs qui sont commises dans l'application des pratiques de sécurité sont discutées en groupe afin qu'elles servent de sources d'apprentissage collectif. • Dans mon environnement de travail, il vaut mieux ne pas communiquer les problèmes rencontrés dans l'application des pratiques de sécurité. • Dans mon environnement de travail, les problèmes liés à l'application quotidienne des pratiques de sécurité sont rarement discutées.	Batteau (2011); Dhillon & Torkzadeh (2006); Dojkovski et al. (2010); Flores & Ekstedt (2012); Knapp & Ferrante (2014); Lacey (2010); Lim et al. (2009); Martins & Eloff (2002); Nosworthy (2000); Parsons et al. (2010); Rantos et al. (2012); Safa et al. (2016); Tang et al. (2015); Williams et al. (2014).

Tableau 2.6 : Les caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires (suite)

Caractéristique du climat	Définition (A), propositions (B) et items (C) liés à la caractéristique du climat	Auteur(s)
RÉCOMPENSES/ SANCTIONS	(A) Cette caractéristique du climat réfère à la façon dont le respect des pratiques de sécurité de l'information est encouragé ou le manque de respect de celles-ci est réprimandé. (B) Plus l'organisation récompense le respect des pratiques de sécurité de l'information définies, plus les employés seront motivés à mettre en œuvre ces pratiques. Plus l'organisation sanctionne vraiment le non-respect des pratiques de sécurité de l'information, plus les chances sont élevées que les employés mettront en œuvre les pratiques sécuritaires définies. (C) • Dans mon environnement de travail, le système de récompense encourage le respect des pratiques de sécurité de l'information. • Dans mon environnement de travail, le respect des pratiques de sécurité de l'information est un élément sérieusement considéré dans l'évaluation de la performance des employés. • Dans mon environnement de travail, si une pratique de sécurité de l'information n'est pas respectée, les sanctions sont sévères. • Dans mon environnement de travail, que l'on respecte ou non les pratiques de sécurité de l'information n'a aucune influence sur l'évaluation qui sera faite du travail effectué.	Bulgurcu et al. (2010);Chan et al. (2005); Chen et al. (2015); Da Veiga & Eloff (2007); Dhillon & Torkzadeh (2006); Dojkovski et al. (2010); Florest & Ekstedt (2012); Knapp et al. (2006); Lacey (2010); Lim et al. (2010); Martins & Eloff (2002); Mishra (2015); Myyry et al. (2009); Ng et al. (2009); Nosworthy (2000); Parsons et al. (2015); Schlienger & Teufel (2002); Siponen (2000).

Tableau 2.6 : Les caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires (suite)

Caractéristique du climat	Définition (A), propositions (B) et items (C) liés à la caractéristique du climat	Auteur(s)
FACON DONT LE MONITORAGE DU RESPECT DES PRATIQUES DE SÉCURITÉ SE FAIT	(A) Cette caractéristique du climat réfère à la façon (confiance et/ou contrôle) privilégiée par l'organisation pour s'assurer du respect des pratiques de sécurité. (B) Plus l'organisation fait confiance aux employés qu'ils feront tout en leur pouvoir pour protéger l'information, plus ils seront engagés dans la protection de l'information et mettront en œuvre des pratiques sécuritaires. À l'opposé, plus l'organisation fait le monitorage continu du respect des pratiques, moins les employés se sentent responsabilisés et auront plutôt tendance à faire fi des pratiques de sécurité. (C) • Dans mon environnement de travail, on surveille en continu si les employés respectent ou non les pratiques de sécurité de l'information. • Dans mon environnement de travail, le respect de chacune des pratiques de sécurité de l'information est minutieusement contrôlé. • Dans mon environnement de travail, on tend à prendre pour acquis que les employés respectent les pratiques de sécurité de l'information parce qu'on leur fait confiance. • Dans mon environnement de travail, on pense que si on ne surveille pas les employés en continu, ils ne respecteront pas les pratiques de sécurité de l'information définies.	Alhogail (2015); Batteau (2011); Chang et al. (2007); Chen et al. (2015); D'Arcy & Green (2014); Dhillon & Torkzadeh (2006); Dojkovski et al. (2010); Lacey (2010); Martins & Eloff (2002); Mishra (2015); Myyry et al. (2009); Von Solms (2000); Vroom & Von Solms (2004).

Tableau 2.6 : Les caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires (suite)

Caractéristique du climat	Définition (A), propositions (B) et items (C) liés à la caractéristique du climat	Auteur(s)
IMPORTANCE RÉELLE ACCORDÉE À LA SÉCURITÉ DE L'INFORMATION	(A) Cette caractéristique du climat réfère à l'importance qui est accordée au quotidien à la sécurité de l'information dans l'environnement de travail. (B) Dans un environnement de travail donné, plus on accorde de l'importance à la sécurité de l'information, plus les employés seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, moins on accorde d'importance à la sécurité de l'information, moins élevées sont les chances que les employés mettent en œuvre des pratiques sécuritaires. (C) • Dans mon environnement de travail, la sécurité de l'information est en bas de la liste de priorité. • Dans mon environnement de travail, personne ne s'intéresse au fait que les pratiques de sécurité de l'information soient respectées ou non. • Dans mon environnement de travail, un manquement aux pratiques de sécurité de l'information est considéré comme étant inacceptable. • Dans mon environnement de travail, la sécurité de l'information est une priorité.	Batteau (2011); Chan et al. (2005); Da Vega & Martins (2015); Dhillon & Torkzadeh (2006); Gaunt (2000); Hu et al. (2012); Knapp & Ferrante (2014); Lacey (2010); Lim et al. (2010); Martins & Eloff (2002); Mishra (2015); Nosworthy (2000); Rastogi & Von Solms (2012); Siponen (2000); Tang et al. (2015).

Cette section a permis de développer une définition du climat de la sécurité de l'information qui se base sur la littérature traitant du climat de la sécurité de l'information et du climat organisationnel. Cette définition a permis d'avoir un regard éclairé lors de l'identification des caractéristiques du climat susceptibles d'influencer sur la mise en œuvre de pratiques sécuritaires par les employés. Tout comme le cas des croyances et des valeurs, les 11 caractéristiques du climat feront l'objet d'une validation telle que présentée dans le chapitre 3.

2.3 Les autres concepts du domaine de la sécurité de l'information pouvant enrichir notre compréhension des croyances, des valeurs et des caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés

Tel qu'il a été mentionné, puisque les croyances, les valeurs et les caractéristiques du climat susceptibles de jouer un rôle dans la sécurité de l'information sont difficilement accessibles dans la littérature et tel que recommandé par MacKenzie et al. (2011), l'examen des concepts connexes permet d'exploiter au maximum la littérature existante afin de s'assurer que des croyances, des valeurs et des caractéristiques du climat discutées dans la littérature n'ont pas été omises. Pour cela, il est ici question de recenser les instruments de mesure et les cadres de référence liés à des concepts connexes.

Pour ce faire, une revue de la littérature a d'abord été effectuée et a permis de recenser les instruments de mesure et les cadres de référence. Si l'on se base sur la définition d'une mesure (*measurement*) élaborée par Campbell (1920), un instrument de mesure peut être défini comme étant un outil permettant d'assigner des valeurs quantitatives à des dimensions. Ces dimensions sont des aspects nécessaires à l'évaluation d'un concept (Larousse, 2017) et sont composées d'items, qui sont généralement des questions. D'autre part, le cadre de référence est un document regroupant des processus d'affaires détaillés, permettant de définir les politiques et les procédures qui encadrent la mise en place et la gestion des activités d'une organisation (TechTarget, 2017).

Ainsi, la revue de la littérature a également porté sur les instruments de mesure et les cadres de référence de la culture de la sécurité de l'information et de ses construits connexes, soit la maturité de la sécurité de l'information et la sensibilisation à la sécurité de l'information, car ces derniers sont considérés comme étant étroitement liés à la culture et au climat de la sécurité de l'information. Par ailleurs, il faut préciser que l'examen d'instruments de

mesure et de cadres de référence du climat de la sécurité de l'information se serait avéré pertinent, mais il n'en existe pas dans la littérature.

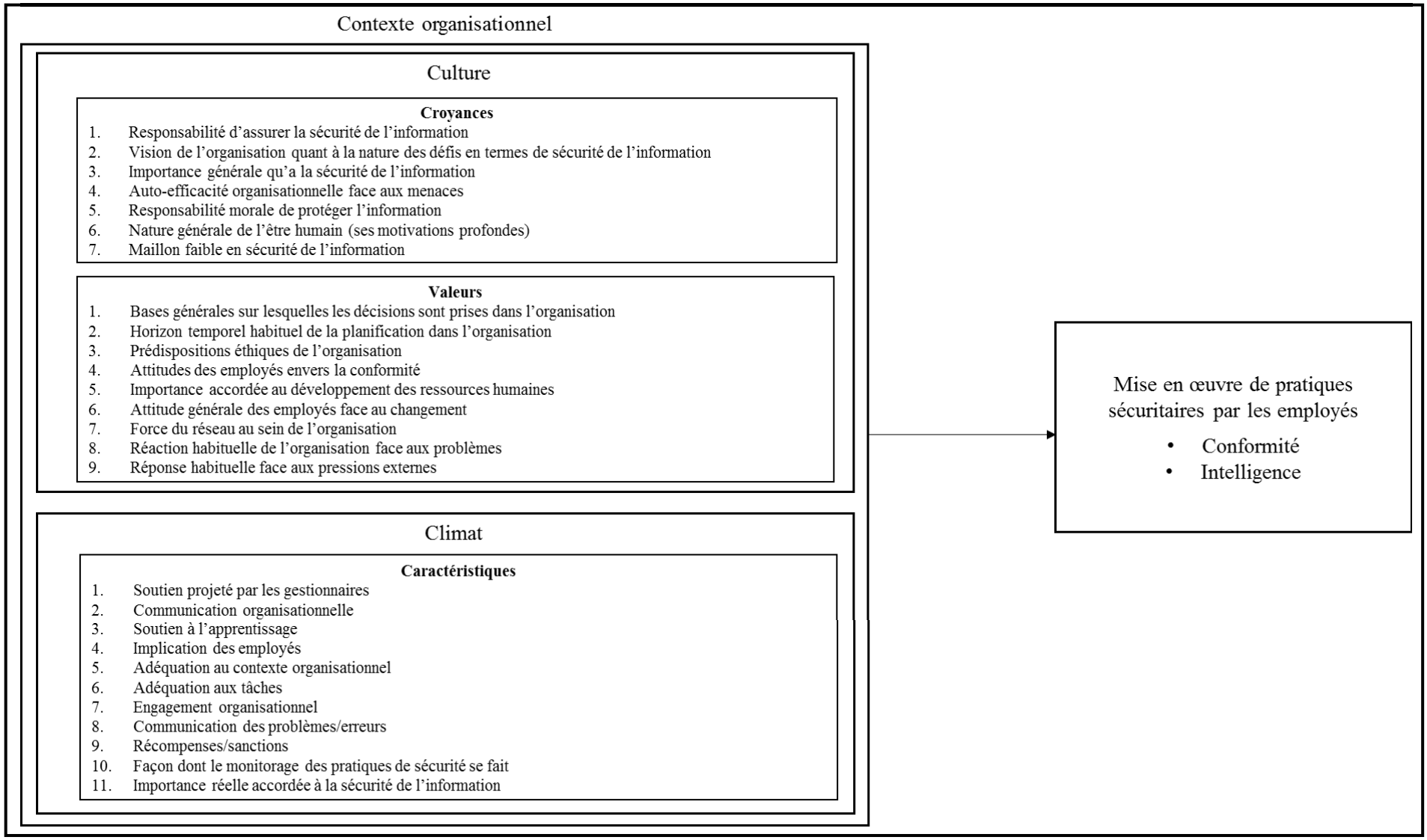
Lors de l'examen des instruments de mesure et des cadres de référence, l'attention était mise sur les dimensions susceptibles d'enrichir la liste des croyances, des valeurs et des caractéristiques du climat liées à la sécurité de l'information qui a été élaborée jusqu'ici. Ainsi, les instruments de mesure et les cadres de référence de la culture de la sécurité de l'information, de la maturité de la sécurité de l'information et de la sensibilisation à la sécurité de l'information ont fait l'objet de cet examen. Les résultats de cette analyse sont présentés à l'annexe 1.

Qu'ils s'intéressent à la culture de la sécurité de l'information ou à ses construits connexes (tels que la maturité de la sécurité de l'information et la sensibilisation à la sécurité de l'information), les instruments de mesure et les cadres de référence analysés n'ont eu aucune contribution directe à la liste de croyances, de valeurs et de caractéristiques du climat de la sécurité de l'information déjà établie dans le présent chapitre. En effet, il a été possible d'observer que certains de ces outils faisaient toute de même référence à certaines des croyances, des valeurs et des caractéristiques du climat de la sécurité de l'information incluses dans notre liste initiale par l'intermédiaire de leurs dimensions ou de leurs items. De plus, aucun des instruments de mesure ni des cadres de référence analysés ne se rapportaient à des aspects liés au climat ou à la culture mais mettaient plutôt l'accent sur les pratiques formelles et opérationnelles en sécurité de l'information. Certains instruments étaient d'un plus grand intérêt, mais il s'est avéré impossible d'accéder au contenu détaillé.

2.4 La culture et le climat organisationnels et leur influence sur la mise en œuvre de pratiques sécuritaires par les employés : le modèle initial

Tout le travail d'analyse réalisé dans ce chapitre permet maintenant de proposer un modèle conceptuel (voir figure 2.4) qui présente les éléments de la culture organisationnelle et du climat organisationnel comme sources d'influence sur la mise en œuvre de pratiques sécuritaires par les employés au sein de l'organisation. De plus, le modèle inclut la liste des sept croyances, des neuf valeurs et des 11 caractéristiques du climat qui, selon la littérature, sont susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés au sein de l'organisation, autant au niveau de la conformité que de l'intelligence.

Figure 2.4 : La culture organisationnelle et le climat organisationnel comme sources d'influence de la mise en œuvre de pratiques sécuritaires par les employés



La partie gauche du modèle présente les composantes du contexte organisationnel, la culture ainsi que le climat organisationnel. Selon le modèle, ces derniers exercent une influence directe sur la mise en œuvre de pratiques sécuritaires par les employés, qui est la variable dépendante du modèle. Pour rappel, les définitions de ces concepts sont les suivantes :

- *« **La culture de la sécurité de l'information** au sein d'une organisation est un ensemble de manifestations visibles et invisibles partagées par les membres de l'organisation. Ces manifestations incluent les croyances, les valeurs, les hypothèses, les artéfacts et les pratiques formelles et informelles qui influencent les décisions et les comportements des employés quant à la protection de l'information. Ces manifestations viennent aussi teinter le climat organisationnel. »*
- *« **Les croyances** reflètent des convictions profondes, qui existent souvent universellement au-delà des murs de l'entreprise et que l'entreprise a faites siennes. »*
- *« **Les valeurs** reflètent des idées implicites ou explicites partagées au sein de l'organisation sur ce qui est important pour l'organisation ou à quoi l'organisation tient beaucoup. »*
- *« Le **climat de la sécurité de l'information** correspond aux perceptions partagées au sein de l'organisation quant aux politiques organisationnelles, aux règles, aux normes et aux pratiques de sécurité mises en œuvre. Le climat de la sécurité de l'information représente les perceptions partagées par les employés à propos de « comment les choses se passent chez nous. »*

Le modèle présente aussi les sept croyances et les neuf valeurs recensées au cours de ce chapitre. Étant des composantes de la culture organisationnelle, elles sont susceptibles d'influencer la variable dépendante. Chacune des croyances ainsi que leur définition, leurs propositions et leurs items sont présentés dans le tableau 2.7. La même présentation est appliquée aux valeurs dans le tableau 2.8. Finalement, le climat et ses caractéristiques figurent également dans ce modèle puisqu'ils sont susceptibles d'influencer la variable dépendante. Ainsi, toutes les caractéristiques du climat, leur définition, leurs propositions et leurs items sont exposés dans le tableau 2.9.

Chacun de ces éléments sont susceptibles d'exercer une influence sur la mise en œuvre de pratiques sécuritaires par les employés. Il faut également mentionner que certains d'entre eux peuvent s'influencer mutuellement. En outre, les croyances et les valeurs organisationnelles s'influencent mutuellement (Ott, 1989) et il en est de même pour la culture organisationnelle et le climat organisationnel. Bien que l'on reconnaisse l'existence de ces influences, elles ne

sont pas représentées dans le présent mémoire parce qu'à ce stade-ci, l'objectif d'identifier ces éléments et non d'investiguer les relations entre ceux-ci.

Tableau 2.7 : Les croyances susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés

Croyance	Définition (A), propositions (B) et items (C)
RESPONSABILITÉ D'ASSURER LA SÉCURITÉ DE L'INFORMATION	(A) Croyance partagée dans l'organisation qui indique qui a la responsabilité d'assurer la sécurité de l'information. (B) Plus on croit dans l'organisation que la sécurité de l'information est du ressort exclusif du département informatique, moins les employés se sentiront responsables de mettre en œuvre des pratiques sécuritaires. À l'opposé, si on croit que tout le monde dans l'organisation a une responsabilité quant à la sécurité de l'information, plus les employés se sentiront responsables de mettre en œuvre des pratiques sécuritaires. (C) • Dans mon organisation, on croit que c'est le département informatique (ou l'équivalent) qui a la responsabilité d'assurer la sécurité de l'information. • Dans mon organisation, on croit que la sécurité de l'information est l'affaire de tous. • Dans mon organisation, on croit que la sécurité de l'information est une responsabilité partagée entre les unités fonctionnelles et le département informatique (ou l'équivalent). • Dans mon organisation, on croit que la sécurité de l'information est une responsabilité partagée par tous les employés de l'organisation.
VISION DE L'ORGANISATION QUANT À LA NATURE DES DÉFIS EN TERMES DE SÉCURITÉ DE L'INFORMATION	(A) Croyance partagée dans l'organisation qui indique la nature des défis rencontrés en sécurité de l'information. (B) Plus on croit dans l'organisation que la sécurité de l'information est avant tout un défi d'ordre technique, moins les employés sentiront la nécessité de mettre en œuvre des pratiques sécuritaires parce qu'ils se fieront aux solutions technologiques. À l'opposé, plus on a la conviction dans l'organisation qu'il y a des composantes humaine, technique et managériale à la sécurité de l'information, plus élevées sont les chances que tout le monde jouera le rôle qu'il a à jouer afin de protéger l'information. (C) • Dans mon organisation, on croit qu'assurer la sécurité de l'information représente avant tout un défi d'ordre technique. • Dans mon organisation, on croit que la sécurité de l'information passe par la considération des aspects techniques, humains et managériaux. • Dans mon organisation, on croit que la sécurité de l'information doit être traitée comme un problème technique. • Dans mon organisation, on croit que la sécurité de l'information nécessite une vision globale qui inclut des aspects techniques, humains et managériaux.

Tableau 2.7 : Les croyances susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite)

Croyance	Définition (A), propositions (B) et items (C)
IMPORTANCE GÉNÉRALE QU'A LA SÉCURITÉ DE L'INFORMATION DANS L'ORGANISATION	(A) Croyance partagée dans l'organisation qui réfère à l'importance générale que l'on accorde à la sécurité de l'information. (B) Plus on croit dans l'organisation que la sécurité de l'information est importante, plus les employés sentiront la nécessité de mettre en œuvre des pratiques sécuritaires. À l'opposé, si on croit dans l'organisation que la sécurité de l'information n'est pas importante, moins élevées sont les chances que les employés mettent en œuvre des pratiques sécuritaires. (C) • Dans mon organisation, on croit que la sécurité de l'information doit être une priorité. • Dans mon organisation, on croit que la sécurité de l'information est peu importante parce que les problèmes de sécurité n'arrivent qu'aux autres. • Dans mon organisation, on a de la difficulté à prendre au sérieux les menaces à la sécurité de l'information. • Dans mon organisation, on croit que l'argent investi en sécurité de l'information représente une dépense inutile.
AUTO-EFFICACITÉ ORGANISATION-NELLE FACE AUX MENACES	(A) Croyance partagée dans l'organisation qui réfère à la capacité de l'organisation à se défendre contre les menaces à la sécurité de l'information. (B) Plus on croit dans l'organisation qu'il est fondamentalement impossible d'assurer vraiment la protection de l'information, moins les employés seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si on est convaincus dans l'organisation qu'il est possible de prendre des actions préventives et de protéger l'information, plus élevées sont les chances que les employés mettront en œuvre des pratiques sécuritaires. (C) • Dans mon organisation, on croit qu'il est possible de protéger l'information contre des actes malicieux. • Dans mon organisation, on croit qu'il est possible de mettre en place un ensemble de moyens pour contrer les menaces à la sécurité de l'information. • Dans mon organisation, on croit qu'il est impossible de se prémunir contre les menaces liées à la sécurité de l'information. • Dans mon organisation, on pense que, malgré tous les moyens mis en place, l'entreprise reste très vulnérable et les personnes malveillantes gagneront toujours.

Tableau 2.7 : Les croyances susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite)

RESPONSABILITÉ MORALE DE PROTÉGER L'INFORMATION	(A) Croyance partagée dans l'organisation quant à la responsabilité morale que l'entreprise a de protéger les informations. (B) Plus on croit que l'organisation a la responsabilité morale de protéger l'information, plus les employés seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si on ne croit pas que l'organisation a cette responsabilité morale, moins élevées sont les chances que les employés mettent en œuvre des pratiques sécuritaires. (C) • Dans mon organisation, on croit qu'on a l'obligation morale de faire ce que l'on peut pour protéger l'information. • Dans mon organisation, on croit qu'on a l'obligation de protéger l'information malgré les contraintes que cela impose • Dans mon organisation, on croit qu'on a l'obligation de protéger l'information afin de défendre les intérêts de l'organisation. • Dans mon organisation, on croit qu'on a l'obligation d'assurer la sécurité de l'information afin de protéger les intérêts de ceux qui souffriraient d'un tel incident.
NATURE GÉNÉRALE DE L'ÊTRE HUMAIN (SES MOTIVATIONS PROFONDES)	(A) Croyance partagée dans l'organisation quant à la nature générale de l'être humain et, plus spécifiquement, en ce qui a trait aux raisons qui motivent ses actions. (B) Plus on croit dans l'organisation que les gens agissent dans le meilleur intérêt de l'organisation et qu'on peut leur faire confiance, plus ils seront responsables et motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si on croit que les gens sont fondamentalement mauvais et qu'on les déresponsabilise en les contrôlant comme des enfants, moins les gens mettront en œuvre des pratiques sécuritaires. (C) • Dans mon organisation, on croit qu'on ne peut faire confiance à personne. • Dans mon organisation, on croit que faire confiance aux gens, permet d'agir dans le meilleur intérêt de l'entreprise. • Dans mon organisation, on croit qu'exercer un contrôle très strict est le seul moyen de s'assurer que les gens font ce qu'ils sont censés faire. • Dans mon organisation, on croit que les gens agissent dans le meilleur intérêt de l'organisation quand on leur fait confiance.

Tableau 2.7 : Les croyances susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite et fin)

LE MAILLON FAIBLE EN SÉCURITÉ DE L'INFORMATION	(A) Croyance partagée dans l'organisation quant au rôle que joue l'être humain dans la sécurité de l'information. (B) Plus on croit dans l'organisation que les gens représentent le maillon faible en sécurité de l'information, moins les employés seront motivés à mettre en œuvre des pratiques sécuritaires parce que l'entreprise mettra en place des outils menant à une déresponsabilisation. À l'opposé, si on croit que les gens sont des maillons importants de la sécurité de l'information, plus élevées sont les chances que l'organisation leur fera confiance, les responsabilisera et que les employés agiront dans le meilleur intérêt de l'organisation en mettant en œuvre des pratiques sécuritaires. (C) • Dans mon organisation, on croit que les gens constituent le maillon faible en sécurité de l'information. • Dans mon organisation, on croit que les gens sont des joueurs-clé dans la protection de l'information. • Dans mon organisation, on considère les gens comme étant la principale cause des incidents liés à la sécurité de l'information. • Dans mon organisation, on croit que les gens peuvent jouer un rôle essentiel pour minimiser les risques liés à la sécurité de l'information.

Tableau 2.8 : Les valeurs susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés

Valeur	Définition (A), propositions (B) et items (C)
BASES GÉNÉRALES SUR LESQUELLES LES DÉCISIONS SONT PRISES DANS L'ORGANISATION	(A) Valeur partagée dans l'organisation quant aux bases sur lesquelles les décisions doivent être prises au sein de l'organisation. (B) Plus l'organisation privilégie les bases quantitatives pour asseoir ses décisions (analyses quantitatives, métriques, benchmarking, etc.), plus élevées sont les chances qu'elle évaluera les aspects liés à la sécurité de l'information d'une manière globale et complète menant à la mise en place d'outils stimulant davantage les employés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si on tend à privilégier des décisions basées sur l'intuition et les émotions (« gut feelings »), plus élevées sont les chances que l'on négligera de conduire une évaluation rigoureuse des aspects liés à la sécurité de l'information, menant ainsi à l'absence d'outils favorisant la mise en œuvre de pratiques sécuritaires. (C) • Dans mon environnement de travail, on privilégie l'intuition et les émotions (« gut feelings ») plutôt que les « chiffres » (analyses quantitatives, métriques, benchmarking, etc.) au moment de prendre une décision. • Dans mon environnement de travail, on pense qu'accorder une grande importance à l'intuition et aux émotions (« gut feelings ») au moment de prendre des décisions mène à de mauvaises décisions. • Dans mon environnement de travail, les « chiffres » (analyses quantitatives, métriques, benchmarking, etc.) sont toujours les critères les plus importants au moment de prendre une décision. • Dans mon environnement de travail, une décision ne peut être prise que sur la base de « chiffres » solides (analyses quantitatives, métriques, benchmarking, etc.).

Tableau 2.8 : Les valeurs susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite)

Valeur	Définition (A), propositions (B) et items (C)
HORIZON TEMPOREL HABITUEL DE LA PLANIFICATION DANS L'ORGANISATION	(A) Valeur partagée dans l'organisation qui reflète les habitudes de planification de l'organisation. (B) Plus l'organisation a l'habitude de planifier à long terme, plus élevées sont les chances qu'elle le fera aussi en sécurité de l'information, ce qui l'amènera à faire les investissements requis afin de favoriser la mise en œuvre de pratiques sécuritaires. À l'opposé, si le focus de l'organisation est surtout à court terme, moins élevées sont les chances que la sécurité de l'information fera l'objet des investissements nécessaires à la mise en œuvre de pratiques sécuritaires. (C) • Dans mon environnement de travail, on se concentre principalement sur l'atteinte d'objectifs à court terme. • Dans mon environnement de travail, on croit aux bénéfices de la planification à long terme (3 ans et plus). • Dans mon environnement de travail, on pense que de planifier à long terme (3 ans et plus) est une perte de temps. • On peut affirmer que, dans mon environnement de travail, on a un focus « court terme ».
PRÉDISPOSITIONS ÉTHIQUES DE L'ORGANISATION	(A) Valeur partagée dans l'organisation quant à la place de l'éthique dans l'organisation. (B) Plus l'organisation adopte une position éthique dans la conduite générale de ses affaires, plus élevées sont les chances qu'elle le fera aussi pour protéger les informations, menant ainsi à la mise en œuvre de pratiques sécuritaires. À l'opposé, si l'éthique n'est pas une valeur importante dans l'organisation, cela affectera négativement la mise en œuvre de pratiques peu sécuritaires. (C) • Les comportements éthiques sont la norme dans mon environnement de travail. • Dans mon environnement de travail, les gestionnaires guident les processus décisionnels dans une direction éthique. • Dans mon environnement de travail, les gestionnaires ne sont pas des modèles de décision éthique. • Dans mon environnement de travail, les gestionnaires adhèrent à des normes éthiques élevées.

Tableau 2.8 : Les valeurs susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite)

Valeur	Définition (A), propositions (B) et items (C)
ATTITUDE DES EMPLOYÉS ENVERS LA CONFORMITÉ	(A) Valeur partagée dans l'organisation quant au respect des règles et des politiques définies au sein de l'organisation. (B) Plus il existe dans l'organisation une prédisposition à respecter les règles et les politiques définies, plus élevées sont les chances que les employés respecteront aussi les pratiques de sécurité de l'information définies. À l'opposé, s'il existe un mépris généralisé envers les règles et les politiques organisationnelles, les chances sont que la même chose se produira pour la mise en œuvre des pratiques de sécurité de l'information définies par l'entreprise. (C) • Dans mon environnement de travail, l'autonomie individuelle est plus valorisée que le respect des politiques et règlements de l'organisation. • Dans mon environnement de travail, il est laissé au bon jugement de chacun des employés de décider si le respect des politiques et règlements est la meilleure chose à faire à un certain moment. • Dans mon environnement de travail, le respect des politiques et règlements de l'organisation est très important. • Dans mon environnement de travail, suivre à la lettre les politiques et règlements de l'organisation est considéré comme étant très important.
IMPORTANCE ACCORDÉE AU DÉVELOPPEMENT DES RESSOURCES HUMAINES	(A) Valeur partagée dans l'organisation qui réfère à l'importance qu'a le développement des connaissances et des habiletés des employés dans l'organisation. (B) Plus il existe dans l'organisation une valorisation du développement des ressources humaines, plus élevées sont les chances que le même sentiment sera instauré par rapport à la sécurité de l'information et que les employés recevront tout le soutien nécessaire à la mise en œuvre de pratiques sécuritaires. À l'opposé, si le développement n'est pas valorisé, moins les employés mettront en œuvre des pratiques sécuritaires parce qu'ils seront livrés à eux-mêmes, sans soutien, ni formation. (C) • Dans mon environnement de travail, on appuie fortement la formation continue des employés. • Dans mon environnement de travail, le développement de la main-d'œuvre n'est pas une priorité. • Dans mon environnement de travail, on prend au sérieux le développement continu des habiletés de chaque employé afin de maximiser sa contribution au succès de l'organisation. • Dans mon environnement de travail, la formation continue de ses employés ne figure pas sur la liste de priorités.

Tableau 2.8 : Les valeurs susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite)

Valeur	Définition (A), propositions (B) et items (C)
ATTITUDE GÉNÉRALE DES EMPLOYÉS FACE AU CHANGEMENT	(A) Valeur partagée dans l'organisation quant à la façon de réagir au changement organisationnel. (B) Plus on valorise l'ouverture au changement dans l'organisation, plus il sera facile de changer les pratiques organisationnelles afin que les employés mettent en œuvre des pratiques de plus en plus sécuritaires. À l'opposé, si on tend à résister au changement, les chances sont plus élevées que les changements engendrés par la mise en œuvre de pratiques de plus en plus sécuritaires seront difficiles à accepter. (C) • Dans mon environnement de travail, on tend à résister aux changements dans les façons de faire. • Dans mon environnement de travail, on adopte facilement les changements aux façons de faire. • Dans mon environnement de travail, on accepte facilement que les façons de faire évoluent et changent. • Dans mon environnement de travail, le changement rend les gens très inconfortables.
FORCE DU RÉSEAU AU SEIN DE L'ORGANISATION	(A) Valeur partagée dans l'organisation quant à la façon de réagir au changement organisationnel. (B) Plus on valorise l'ouverture au changement dans l'organisation, plus il sera facile de changer les pratiques organisationnelles afin que les employés mettent en œuvre des pratiques de plus en plus sécuritaires. À l'opposé, si on tend à résister au changement, les chances sont plus élevées que les changements engendrés par la mise en œuvre de pratiques de plus en plus sécuritaires seront difficiles à accepter. (C) • Dans mon environnement de travail, on tend à résister aux changements dans les façons de faire. • Dans mon environnement de travail, on adopte facilement les changements aux façons de faire. • Dans mon environnement de travail, on accepte facilement que les façons de faire évoluent et changent. • Dans mon environnement de travail, le changement rend les gens très inconfortables.

Tableau 2.8 : Les valeurs susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite)

Valeur	Définition (A), propositions (B) et items (C)
RÉACTION HABITUELLE DE L'ORGANISATION FACE AUX PROBLÈMES	(A) Valeur partagée dans l'organisation quant à la réaction première de l'organisation face à un problème ou à un incident. (B) Plus la réaction instinctive de l'organisation face à un problème ou à un incident est de pointer un coupable, moins les employés seront motivés à partager les problèmes/incidents/difficultés entre eux et plus élevées sont les chances que les employés mettront en œuvre des pratiques non sécuritaires. À l'opposé, si la réaction est plutôt d'encourager les employés à partager leurs problèmes/incidents/difficultés, plus les chances sont élevées que ce sera aussi la même chose dans le cas de la sécurité de l'information, menant ainsi à la mise en œuvre de pratiques plus sécuritaires. (C) • Dans mon environnement de travail, lorsque qu'un problème survient, le premier réflexe est de chercher un coupable. • Dans mon environnement de travail, lorsque survient un problème, on tend à vouloir se protéger en identifiant un bouc émissaire. • Dans mon environnement de travail, on nous encourage à partager nos problèmes plutôt que de les cacher. • Mon environnement de travail a une atmosphère où les problèmes peuvent être exprimés et discutés.

Tableau 2.8 : Les valeurs susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite et fin)

Valeur	Définition (A), propositions (B) et items (C)
RÉPONSE HABITUELLE DE L'ORGANISATION FACE AUX PRESSIONS EXTERNES	(A) Valeur partagée dans l'organisation qui réfère à la réponse habituelle de l'organisation face aux pressions provenant des clients, gouvernement, standards nationaux et internationaux, etc. (B) Plus l'organisation a tendance à adopter des comportements symboliques face aux obligations externes (clients, gouvernements, standards, etc.), plus élevées sont les chances qu'elle fera la même chose en ce qui a trait à la sécurité de l'information, au total menant à la mise en œuvre de pratiques moins sécuritaires. Au contraire, si l'organisation tend à prendre ces obligations/recommandations comme une occasion d'améliorer ses pratiques internes, les chances sont qu'elle fera la même chose en sécurité de l'information, ce qui mènera à la mise en œuvre de pratiques plus sécuritaires. (C) • Dans mon environnement de travail, publiciser à l'externe que nos pratiques internes de sécurité de l'information sont solides est plus important que les pratiques elles-mêmes. • Dans mon environnement de travail, on prend au sérieux les pratiques de sécurité imposées/recommandées par les organismes externes en nous assurant que des pratiques internes correspondantes soient implantées. • Dans mon environnement de travail, on croit que l'objectif en sécurité de l'information est de faire le minimum qui permet de passer les tests de conformité. • Dans mon environnement de travail, on pense que le respect des pratiques de sécurité imposées par des organismes externes représente des occasions d'améliorer nos pratiques internes.

Tableau 2.9 : Les caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés

Caract. du climat	Définition (A), proposition (B) et items (C)
SOUTIEN PROJETÉ PAR LES GESTIONNAIRES	(A) Cette caractéristique du climat réfère aux gestes et comportements des gestionnaires par rapport à la sécurité de l'information. (B) Plus les gestionnaires ont tendance à montrer un appui à la sécurité de l'information (par leurs gestes, paroles, décisions et appuis concrets (comme des ressources financières), plus les employés comprendront que la sécurité de l'information est importante dans leur environnement de travail et seront motivés à mettre eux aussi en œuvre des pratiques sécuritaires. À l'opposé, si le message reçu des gestionnaires est que la sécurité de l'information a peu d'importance dans leur environnement de travail, plus les chances sont élevées que les pratiques sécuritaires ne seront pas mises en œuvre. (C) • Dans mon environnement de travail, les gestionnaires montrent l'exemple en respectant les pratiques de sécurité de l'information définies. • Dans mon environnement de travail, les gestionnaires tendent à ne pas respecter une pratique de sécurité de l'information si elle empêche un projet ou une décision qui leur tient à cœur d'aller de l'avant. • Dans mon environnement de travail, les gestionnaires nous demandent parfois de faire des choses qui vont à l'encontre des pratiques de sécurité de l'information définies. • Dans mon environnement de travail, les gestionnaires octroient les ressources (temps, budget, personnel, etc.) nécessaires pour mettre en œuvre les pratiques permettant une protection adéquate de l'information.

Tableau 2.9 : Les caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite)

Caract. du climat	Définition (A), proposition (B) et items (C)
COMMUNICATION ORGANISATION-NELLE	(A) Cette caractéristique du climat réfère à la capacité de l'organisation à communiquer des messages clairs par rapport à la sécurité de l'information. (B) Plus l'organisation arrive à communiquer des messages clairs quant à la sécurité de l'information (objectifs, importance, attentes, etc.), plus les employés seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si les messages sont absents ou confus, plus les chances sont élevées que les pratiques sécuritaires ne seront pas mises en œuvre. (C) • Mon organisation communique aux employés une vision claire de la sécurité de l'information et de ses objectifs. • Dans mon environnement de travail, le rôle que les employés jouent dans l'effort global de protection de l'information est clairement communiqué. • Dans mon environnement de travail, les attentes en termes de sécurité de l'information sont clairement communiquées. • Dans mon environnement de travail, on nous explique clairement l'importance de la sécurité de l'information.
SOUTIEN À L'APPRENTISSAGE	(A) Cette caractéristique du climat réfère aux moyens mis en place pour soutenir les employés dans la mise en œuvre des pratiques de sécurité. (B) Plus l'organisation met en place les outils qui permettent de soutenir la formation et le développement de connaissances en sécurité de l'information, plus les employés seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si les employés ne reçoivent pas le soutien nécessaire, plus les chances sont élevées que les pratiques sécuritaires ne seront pas mises en œuvre. (C) • Mon organisation met en place les moyens assurant que chaque employé comprenne bien les pratiques de sécurité de l'information dont il a la responsabilité. • Dans mon environnement de travail, les employés reçoivent le soutien nécessaire (en termes de formation, assistance, documents de référence, etc.) afin de pouvoir mettre en œuvre les pratiques de sécurité de l'information dont ils ont la responsabilité. • Dans mon environnement de travail, on donne aux employés les moyens d'améliorer leurs habiletés pour faire face aux défis de la sécurité de l'information. • Dans mon environnement de travail, les employés se sentent bien outillés face aux défis que représente la sécurité de l'information.

Tableau 2.9 : Les caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite)

Caract. du climat	Définition (A), proposition (B) et items (C)
IMPLICATION DES EMPLOYÉS	(A) Cette caractéristique du climat renvoie à l'implication des employés aux étapes du cycle de vie des pratiques de sécurité de l'information. (B) Plus les employés se sentent impliqués dans l'élaboration et l'évolution des pratiques de sécurité, plus les employés seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si les employés ne se sentent pas impliqués, plus élevées sont les chances que les pratiques sécuritaires ne seront pas mises en œuvre. (C) • Dans mon environnement de travail, les employés se sentent impliqués dans l'évolution des pratiques de sécurité de l'information. • Dans mon environnement de travail, les suggestions des employés pour améliorer les pratiques de sécurité de l'information sont prises au sérieux. • Dans mon environnement de travail, l'implication des employés dans l'évolution des pratiques de sécurité de l'information est considérée comme étant incontournable. • Dans mon environnement de travail, les employés ne se sentent pas consultés sur les pratiques de sécurité à mettre en place.
ADÉQUATION AU CONTEXTE ORGANISATION-NEL	(A) Cette caractéristique du climat réfère à l'adéquation (le « fit ») entre les pratiques de sécurité de l'information dans l'organisation et les caractéristiques du contexte organisationnel. (B) Plus les pratiques de sécurité de l'information définies sont en adéquation avec les caractéristiques du contexte organisationnel comme la culture et les pratiques d'affaires, plus les employés seront enclins à mettre en œuvre ces pratiques sécuritaires. À l'opposé, s'il y a un « misfit » entre les pratiques de sécurité de l'information et les caractéristiques du contexte organisationnel, plus élevées sont les chances que les pratiques sécuritaires ne seront pas mises en œuvre. (C) • Les pratiques de sécurité de l'information sont bien alignées sur les pratiques d'affaires de mon organisation. • Les pratiques de sécurité de l'information respectent la culture de mon organisation. • Les pratiques de sécurité de l'information sont souvent en contradiction avec la façon dont mon organisation mène ses affaires. (reverse) • Dans mon environnement de travail, la culture de mon organisation représente un obstacle à la mise en œuvre de certaines pratiques de sécurité de l'information.

Tableau 2.9 : Les caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite)

Caract. du climat	Définition (A), proposition (B) et items (C)
ADÉQUATION AUX TÂCHES	(A) Cette caractéristique du climat réfère à l'adéquation (le « fit ») entre les pratiques de sécurité de l'information dans l'organisation et les tâches à réaliser. (B) Plus les pratiques de sécurité de l'information définies sont en adéquation avec la tâche (effort minimal, impact marginal sur le rendement, etc.), plus les employés seront enclins à mettre ces pratiques sécuritaires en œuvre. À l'opposé, si les pratiques ajoutent une lourdeur au travail quotidien, plus les chances sont élevées que les pratiques sécuritaires ne seront pas mises en œuvre. (C) • Dans mon environnement de travail, les pratiques de sécurité de l'information sont définies par des personnes qui ne comprennent pas le travail sur le terrain. • Dans mon environnement de travail, les employés croient que les pratiques de sécurité sont définies sans prendre en considération les impacts qu'elles ont sur leur travail. • Dans mon environnement de travail, on pense qu'il est difficile de respecter les pratiques de sécurité de l'information si on veut accomplir le travail demandé. • Dans mon environnement de travail, les pratiques de sécurité de l'information ont été définies de façon à ne pas nuire au rendement au travail.
ENGAGEMENT ORGANISATION-NEL	(A) Cette caractéristique du climat renvoie au lien affectif qui unit les employés à l'organisation. (B) Plus les employés ont un sentiment partagé d'attachement à l'organisation, plus ils seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, plus un désengagement général est présent, plus les chances sont élevées que les pratiques sécuritaires ne seront pas mises en œuvre. (C) • Dans mon environnement de travail, les employés sont prêts à mettre beaucoup d'effort pour aider notre organisation à connaître le succès. • Dans mon environnement de travail, les employés tendent à parler très positivement de notre organisation. • Dans mon environnement de travail, les employés sont émotionnellement attachés à notre organisation. • Dans mon environnement de travail, les employés font preuve de peu de loyauté envers notre organisation.

Tableau 2.9 : Les caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite)

Caract. du climat	Définition (A), proposition (B) et items (C)
COMMUNICATION DES PROBLÈMES/ ERREURS	*(*A) Cette caractéristique du climat réfère à la possibilité de discuter ouvertement dans l'environnement de travail des problèmes/erreurs liés à la mise en œuvre des pratiques de sécurité de l'information. (B) Plus l'environnement de travail permet de discuter ouvertement des problèmes/erreurs liés à la mise en œuvre des pratiques de sécurité, plus les employés seront enclins à communiquer les problèmes/erreurs rencontrés, le tout favorisant la mise en œuvre de pratiques sécuritaires. À l'opposé, si l'environnement favorise plutôt de ne pas révéler et même de cacher les problèmes/erreurs, moins élevées sont les chances que les employés mettront en œuvre de pratiques sécuritaires. (C) • Dans mon environnement de travail, les problèmes liés à l'application des pratiques de sécurité peuvent être ouvertement discutés. • Dans mon environnement de travail, les erreurs qui sont commises dans l'application des pratiques de sécurité sont discutées en groupe afin qu'elles servent de sources d'apprentissage collectif. • Dans mon environnement de travail, il vaut mieux ne pas communiquer les problèmes rencontrés dans l'application des pratiques de sécurité. • Dans mon environnement de travail, les problèmes liés à l'application quotidienne des pratiques de sécurité sont rarement discutées.

Tableau 2.9 : Les caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite)

Caract. du climat	Définition (A), proposition (B) et items (C)
RÉCOMPENSES/ SANCTIONS	(A) Cette caractéristique du climat réfère à la façon dont le respect des pratiques de sécurité de l'information est encouragé ou le manque de respect de celles-ci est réprimandé. (B) Plus l'organisation récompense le respect des pratiques de sécurité de l'information définies, plus les employés seront motivés à mettre en œuvre ces pratiques. Plus l'organisation sanctionne vraiment le non-respect des pratiques de sécurité de l'information, plus les chances sont élevées que les employés mettront en œuvre les pratiques sécuritaires définies. (C) • Dans mon environnement de travail, le système de récompense encourage le respect des pratiques de sécurité de l'information. • Dans mon environnement de travail, le respect des pratiques de sécurité de l'information est un élément sérieusement considéré dans l'évaluation de la performance des employés. • Dans mon environnement de travail, si une pratique de sécurité de l'information n'est pas respectée, les sanctions sont sévères. • Dans mon environnement de travail, que l'on respecte ou non les pratiques de sécurité de l'information n'a aucune influence sur l'évaluation qui sera faite du travail effectué.
FACON DONT LE MONITORAGE DU RESPECT DES PRATIQUES DE SÉCURITÉ SE FAIT	(A) Cette caractéristique du climat réfère à la façon (confiance et/ou contrôle) privilégiée par l'organisation pour s'assurer du respect des pratiques de sécurité. (B) Plus l'organisation fait confiance aux employés qu'ils feront tout en leur pouvoir pour protéger l'information, plus ils seront engagés dans la protection de l'information et mettront en œuvre des pratiques sécuritaires. À l'opposé, plus l'organisation fait le monitorage continu du respect des pratiques, moins les employés se sentent responsabilisés et auront plutôt tendance à faire fi des pratiques de sécurité. (C) • Dans mon environnement de travail, on surveille en continu si les employés respectent ou non les pratiques de sécurité de l'information. • Dans mon environnement de travail, le respect de chacune des pratiques de sécurité de l'information est minutieusement contrôlé. • Dans mon environnement de travail, on tend à prendre pour acquis que les employés respectent les pratiques de sécurité de l'information parce qu'on leur fait confiance. • Dans mon environnement de travail, on pense que si on ne surveille pas les employés en continu, ils ne respecteront pas les pratiques de sécurité de l'information définies.

Tableau 2.9 : Les caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (suite)

Caract. du climat	Définition (A), proposition (B) et items (C)
IMPORTANCE RÉELLE ACCORDÉE À LA SÉCURITÉ DE L'INFORMATION	(A) Cette caractéristique du climat réfère à l'importance qui est accordée au quotidien à la sécurité de l'information dans l'environnement de travail. (B) Dans un environnement de travail donné, plus on accorde de l'importance à la sécurité de l'information, plus les employés seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, moins on accorde d'importance à la sécurité de l'information, moins élevées sont les chances que les employés mettent en œuvre des pratiques sécuritaires. (C) • Dans mon environnement de travail, la sécurité de l'information est en bas de la liste de priorité. • Dans mon environnement de travail, personne ne s'intéresse au fait que les pratiques de sécurité de l'information soient respectées ou non. • Dans mon environnement de travail, un manquement aux pratiques de sécurité de l'information est considéré comme étant inacceptable. • Dans mon environnement de travail, la sécurité de l'information est une priorité.

Maintenant qu'une liste exhaustive des croyances, valeurs et caractéristiques du climat a été élaborée, le prochain chapitre présente la méthodologie qui sera utilisée pour en faire une première validation empirique. Cette validation est nécessaire puisque cette liste se base sur une littérature souvent anecdotique et qui souffre d'un manque de validation empirique rigoureuse. Compte tenu du nombre de croyances, de valeurs et de caractéristiques du climat, il s'avère également pertinent d'en dresser une liste qui soit à la fois complète et parcimonieuse puisque le but de cette étude est de contribuer ultimement au développement d'un instrument de mesure.

Chapitre 3 : Méthodologie

Ce mémoire a pour objectif de déterminer, avec complétude et parcimonie, les croyances, les valeurs et les caractéristiques du climat susceptibles d'influencer la mise en oeuvre de pratiques sécuritaires par les employés. Sur la base de la littérature, le chapitre précédent a permis de générer une liste de croyances, de valeurs et de caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés, la variable dépendante au cœur de ce mémoire. Néanmoins, il a été constaté que la littérature, sur laquelle est établie cette liste, est confuse et anecdotique. C'est pourquoi il s'avère pertinent de confronter cette liste à des professionnels d'expérience en sécurité de l'information à des fins de validation.

La collecte de données était déclinée en trois étapes distinctes, soient le prétest auprès d'étudiants de la M.Sc. en T.I., le groupe de discussion auprès de professionnels en sécurité de l'information et les rencontres individuelles auprès de professionnels en sécurité de l'information. Ces étapes ont essentiellement visé à conceptualiser la culture et du climat de la sécurité de l'information, par la validation de la liste de croyances, de valeurs et de caractéristiques du climat. L'objectif final était d'avoir en main une liste de croyances, de valeurs et de caractéristiques du climat qui se voulait à la fois complète et parcimonieuse.

Ce chapitre décrit donc l'approche méthodologique adoptée. Il est divisé en trois sections selon les trois étapes de collecte des données réalisées, soit le prétest, le groupe de discussion et les rencontres avec des professionnels en sécurité de l'information. Pour chacune des étapes, le processus de cueillette des données est présenté, suivi par celui d'analyse de ces données.

3.1 Étape A : Prétest – Rencontres individuelles avec des étudiants de la M.Sc.

Ce prétest avait deux objectifs. Il a tout d'abord permis à la chercheuse de s'approprier et de valider le protocole de recherche avant de l'appliquer aux autres étapes de la collecte des données. Il a ainsi contribué à identifier des irritants qui ne pourraient être mis en lumière que lorsque le protocole serait mis en application face à un répondant complètement indépendant de la recherche.

3.1.1 Cueillette des données

Trois étudiants de la M.Sc. en technologies de l'information de HEC Montréal, provenant du réseau de contacts du chercheur, ont été contactés afin de participer à cette étape. Après avoir obtenu le consentement des participants, l'enregistrement audio et la prise de notes ont été

utilisés afin de collecter les données pendant ces rencontres individuelles. Le protocole détaillé utilisé pour cette première étape peut être trouvé à l'annexe 2.

Chaque entrevue a débuté par une présentation, où le sujet, l'objectif de recherche et le vocabulaire du mémoire ont été exposés au participant. Ce dernier a été invité à partager ses impressions quant à l'étude en répondant à une série de questions. Par exemple, il lui a été demandé s'il était familier avec les construits de la culture et du climat de la sécurité de l'information ou encore s'il était capable de les définir. Par la suite, les croyances, les valeurs et les caractéristiques du climat, et leur définition, ont été présentées au participant. Pour susciter la réaction du participant par rapport à celles-ci et pour en évaluer la validité, des questions lui ont été posées. Par exemple, il lui a été demandé si les croyances, les valeurs et les caractéristiques qui lui ont été présentées semblaient liées à la culture ou au climat de la sécurité de l'information.

En lien avec l'objectif initial du mémoire, qui était le développement d'un instrument de mesure, le participant a ensuite dû procéder à un exercice de triage de cartes. Cet exercice avait pour but de s'assurer que l'instrument mesure bien ce qu'il est censé mesurer. Pour ce faire, les items (soit les questions) doivent évaluer adéquatement les dimensions (à savoir les croyances, les valeurs et les caractéristiques du climat) de l'instrument de mesure. Après avoir pris connaissance des dimensions (imprimées sur des enveloppes, voir figure 3.1), le participant a reçu des cartes, sur lesquelles étaient imprimés les items (voir figure 3.2). Ce dernier devait associer les items aux dimensions en fonction du lien entre la définition de la dimension et du sens de l'item. Si l'item présenté sur la carte ne semblait lié à aucune dimension, il était invité à la mettre de côté. Au final, l'exercice incluait 65 items et 16 dimensions. Il faut rappeler qu'à ce stade-ci, l'objectif était de tester le protocole. C'est pourquoi toutes les dimensions et tous les items n'ont pas été présentés aux participants.

Figure 3.1 : Exemple d'enveloppe utilisée pour l'exercice de triage de l'étape A

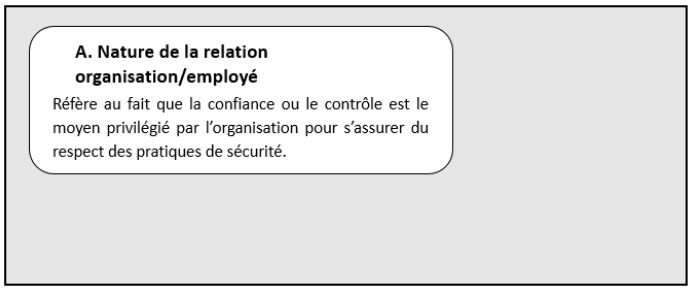


Figure 3.2 : Exemple de carte utilisée pour l'exercice de triage de l'étape A

42. Dans mon organisation, on croit que la sécurité de l'information est l'affaire de tous.

Pendant cet exercice, la technique de protocole « simultané », qui requiert que le participant pense « à haute voix », a été mise en application. Cette technique permet notamment d'examiner le processus décisionnel du participant (Ericsson & Simon, 1980) et a donc contribué à identifier des aspects problématiques par les hésitations ou les questionnements du participant. Suite au triage de cartes, le participant a partagé ses impressions quant à l'exercice effectué en répondant à des questions. Celles-ci ont eu pour effet de collecter davantage de données et de pallier le manque d'information dans les cas où le participant n'a pas été suffisamment expressif lors de la réalisation de l'exercice. On lui a notamment demandé s'il y avait des dimensions ou des items qu'il trouvait redondants. Les rencontres avec ces participants ont duré entre 60 et 90 minutes.

3.1.2 Analyse des données et résultats

Suite à chaque entrevue, les résultats ont fait l'objet d'une analyse approfondie des propos des participants, de leur classement et des difficultés rencontrées. Ainsi, le protocole a été modifié suite à la première entrevue individuelle. Au départ, le temps alloué à chacune des entrevues était de 60 minutes. Il a néanmoins été constaté que le temps imparti était insuffisant puisque le premier participant a mis plus de temps à effectuer l'exercice que prévu. C'est pourquoi 30 minutes supplémentaires ont été planifiées pour les autres rencontres de cette étape.

Mais au-delà de cette simple modification au temps nécessaire pour la conduite d'une entrevue, le prétest s'est avéré un élément critique de la démarche adoptée dans ce mémoire. Ainsi, l'analyse des enregistrements vocaux de chacun des participants a révélé que l'exercice était long. En effet, au cours de l'exercice, tous les participants ont déclaré à plusieurs reprises que l'exercice était éprouvant en raison du nombre élevé de dimensions et d'items à classer. Durant la période de questions qui a suivi l'exercice, ils ont également ajouté qu'il leur était invraisemblable qu'un instrument de mesure comporte autant d'items puisque cela imposerait une lourde charge cognitive sur les participants.

Or, la littérature n'offrait à ce point aucun outil pour distinguer les valeurs, croyances et caractéristiques du climat les plus importantes de celles qui l'étaient moins. Donc, tel qu'il a

été expliqué dans le chapitre 1 du mémoire, il était impossible d'aller de l'avant avec l'objectif premier de développement d'un instrument de mesure. Il valait mieux limiter l'objectif du mémoire à la première étape du processus de développement d'un instrument, soit à la conceptualisation ou, en d'autres mots, à l'identification et à la compréhension des valeurs, croyances et caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés. Donc, au lieu de réaliser le développement d'un instrument de mesure, l'objectif du mémoire devenait de présenter une liste, à la fois complète et parcimonieuse, des croyances, valeurs, et caractéristiques du climat susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés, qui s'avère la première indispensable étape du développement de tout instrument (MacKenzie et al., 2011).

Cette reformulation de l'objectif du mémoire a eu des implications sur le reste de l'approche méthodologique. Ainsi, aux étapes B et C, le focus était désormais d'identifier, de prioriser et de mieux comprendre les croyances, les valeurs et les caractéristiques du climat et leurs impacts sur la mise en œuvre de pratiques sécuritaires par les employés. Dans les étapes suivantes, les participants n'étaient donc pas appelés à associer des items à des dimensions, mais bel et bien à prioriser et à commenter l'importance des croyances, des valeurs et des caractéristiques du climat recensées, par rapport à la mise en œuvre de pratiques sécuritaires par les employés. De ce fait, le matériel utilisé pour les exercices de priorisation a dû être ajusté en fonction du nouvel objectif de l'exercice. Il n'était plus question d'utiliser des cartes (comportant uniquement un item) et des enveloppes (représentant des dimensions). Les participants devaient effectuer l'exercice avec des cartes sur lesquelles figurent le nom d'un élément donné, sa définition ainsi que deux items à titre explicatif. De plus, suite aux observations formulées pendant ce prétest, des clarifications ont été apportées à ces items.

3.2 Étape B : Rencontre avec un groupe de professionnels en sécurité de l'information – groupe de discussion

Cette rencontre avec un groupe de professionnels en sécurité de l'information avait deux objectifs. D'une part, il visait à tester le protocole de recherche, qui a été modifié à l'issue de l'étape A ainsi qu'à vérifier la validité apparente des croyances, des valeurs et des caractéristiques du climat. D'autre part, il a permis au chercheur d'en identifier les irritants et de s'assurer qu'il soit prêt à être appliqué à la prochaine étape de collecte de données. D'ailleurs, la conduite d'un groupe de discussion a été choisie pour cette étape car, selon Delbecq et al. (1986), l'avantage de ce format de rencontre est le concept d'*idea hitchhiking,*

c'est-à-dire le fait qu'une idée puisse en engendrer une autre. Par exemple, une idée partagée par un participant pouvait en stimuler un autre à exprimer une idée qui ne lui serait pas venue à l'esprit s'il avait été seul. Ainsi, les données découlant de ce groupe de discussion offraient une richesse inégalée.

3.2.1 Cueillette des données

Pour cette étape, trois professionnels en sécurité de l'information ont été recrutés par réseau de contacts personnel et selon la méthode de la boule de neige, qui consistait à joindre des experts qui ont été référés par ceux que l'on connaissait déjà. Ils devaient répondre aux critères de sélection suivants:

- L'expert affirme que ses tâches sont liées à la gestion de la sécurité de l'information (établissement des politiques et procédures, sensibilisation et formation, gestion de risque, relation avec les tiers, choix de solutions soutenant la sécurité de l'information, établissement de critères relatifs à la sécurité dans le choix de solutions technologiques, etc.) et que ces tâches représentent au moins le tiers de ses activités professionnelles.
- L'expert réalise ces tâches dans son contexte organisationnel ou est un consultant qui exerce ces tâches dans le cadre de mandats auprès de ses clients.
- Les experts doivent posséder au moins trois années d'expérience dans la réalisation de ces tâches liées à la gestion de la sécurité de l'information.

Ainsi, les trois professionnels recrutés provenaient de trois organisations différentes et étaient expérimentés en sécurité de l'information (puisqu'ils avaient respectivement cinq, 13 et 20 années d'expérience de gestion de la sécurité de l'information à leur actif).

Les pratiques d'excellence de conduite d'un groupe nominal de Delbecq et al. (1986) ont servi d'inspiration pour la conduite de ce groupe de discussion. Le nombre de participants au groupe de discussion était de trois puisque cela constitue un nombre convenable pour assurer une génération d'idées prolifiques et pour atteindre un consensus sans trop de difficulté (Delbecq et al.,1986). Après avoir obtenu le consentement des participants, un enregistrement audio a été réalisé et des notes ont été prises afin de collecter les données.

Le groupe de discussion s'est ouvert sur une présentation du sujet et des objectifs de recherche du mémoire. Elle a été suivie par une discussion autour du lexique du mémoire et autour de l'influence du contexte organisationnel (qui comprend la culture et le climat de la sécurité de l'information) sur la mise en œuvre des pratiques sécuritaires par les employés. Le but de cette discussion était non seulement de briser la glace et de valider le vocabulaire utilisé, mais aussi

de s'assurer que les participants comprenaient bien le modèle de recherche de la figure 2.3 et ce que le modèle tente d'expliquer. Les participants ont été libres d'intervenir pendant la discussion afin de poser des questions ou d'émettre des commentaires.

Par la suite, les participants ont dû réaliser trois exercices de priorisation (soit un exercice de priorisation pour les valeurs, un pour les croyances et un pour les caractéristiques du climat). Ils ont dû classer, par ordre d'importance, les croyances, les valeurs et les caractéristiques du climat qui, selon eux, exerçaient le plus d'influence sur la mise en œuvre de pratiques sécuritaires par les employés, la variable dépendante.

Pour chaque exercice, les participants ont chacun reçu une enveloppe qui contenait des cartes où figuraient, sur chacune d'elles, le nom d'un élément (croyance, valeur ou caractéristique du climat), sa définition, et, à titre illustratif, les deux items qui pourraient potentiellement être utilisés pour le mesurer dans un questionnaire (voir figure 3.3 et l'annexe 5 pour toutes les cartes utilisées à cette étape). Quelques minutes ont été accordées aux participants pour qu'ils puissent lire les cartes, prendre des notes, au besoin, et les prioriser par ordre d'importance par rapport à la variable dépendante. D'ailleurs, les participants pouvaient se référer en tout temps durant les exercices au modèle illustré à la figure 2.3 Pour réaliser les trois exercices, les participants ont reçu la consigne de le faire individuellement, sans échanger de commentaires, afin de leur permettre de se concentrer sur leur propre réflexion. Au final, toutes les croyances, les valeurs et les caractéristiques du climat qui avait été répertoriées dans le chapitre 2 ont été présentées aux participants durant ces exercices.

Figure 3.3 : Exemple de carte utilisée lors d'un exercice de priorisation de l'étape B

RESPONSABILITÉ D'ASSURER LA SÉCURITÉ DE L'INFORMATION

Croyance partagée dans l'organisation qui indique qui a la responsabilité d'assurer la sécurité de l'information.

Par exemple :

- *Dans mon organisation, on croit que la sécurité de l'information est une responsabilité partagée par tous les employés de l'organisation.*
- *Dans mon organisation, on croit que c'est le département informatique (ou l'équivalent) qui a la responsabilité d'assurer la sécurité de l'information.*

Après chacun des exercices de priorisation, les participants ont été invités à partager leur classement, en les plaçant côte-à-côte pour les comparer. À ce stade, la technique *round-robin recording of ideas* de Delbecq et al. (1986) a été utilisée. Elle consistait à faire un tour de table

où les participants doivent chacun présenter le fruit de leur réflexion et à en discuter. Les discussions furent très riches. D'ailleurs, au cours de cette tâche, il est arrivé que certains participants aient modifié leur classement individuel après avoir discuté avec les autres ou bien après avoir admis qu'ils avaient classé la carte en fonction de leur interprétation et non en fonction de la définition proposée sur la carte.

Lorsque cette étape fut complétée, les participants ont été invités à combiner leurs classements individuels pour en faire un classement final collectif. Bien que les instructions étaient les mêmes que celles des exercices de priorisation individuels, les participants avaient le droit de commenter les cartes entre eux. À l'issue de ces exercices, trois classements collectifs ont été réalisés par les participants. Enfin, pour conclure le groupe de discussion, une rétroaction collective sur les classements a permis d'identifier les éléments qui étaient les plus pertinents, redondants ou manquants. Ces exercices collectifs et cette rétroaction avaient notamment pour but de faire appel à la réflexion collective des participants et de bénéficier de la richesse de leur discussion. Les participants ont d'ailleurs fait preuve d'une grande générosité, expliquant leur vision et l'illustrant d'anecdotes tirées de leur expérience professionnelle. Au final, cette rencontre a duré environ trois heures. Le protocole utilisé pour la tenue du groupe de discussion figure à l'annexe 3.

3.2.2 Analyse des données et résultats

À l'issue du groupe de discussion, les données ont été soumises à une analyse. Cette sous-section explique comment cette analyse a été conduite.

Pour préserver leur anonymat, les participants sont identifiés par des chiffres. Ainsi, le groupe de discussion a eu lieu auprès des participants #1, #2 et #3.

Les deux grands objectifs de cette rencontre avec le groupe de discussion ont été atteints. Ainsi, concernant le premier objectif (tester le protocole de collecte de données), le groupe de discussion a permis d'identifier une limite de la méthode employée et de l'améliorer. Durant les exercices de priorisation, il a été remarqué que les participants ne lisaient que le nom des croyances, des valeurs ou des caractéristiques du climat ayant pour résultat que leur interprétation variait énormément. Il devenait donc difficile de comparer et d'analyser leurs classements puisqu'ils se basaient sur des interprétations parfois très différentes. Ce problème a d'ailleurs pu être observé lors des discussions entre les participants pour établir le classement collectif.

Pour ce qui est du deuxième objectif (vérifier la validité apparente des croyances, des valeurs et des caractéristiques du climat), il a également été atteint. En effet, les propos émis par les

participants lors de la discussion ont été examinés afin de déterminer si les croyances, les valeurs et les caractéristiques qui leur ont été présentées étaient adéquates pour cerner la culture et le climat de la sécurité de l'information dans leur intégralité. L'analyse a démontré que les croyances, les valeurs ou les caractéristiques du climat organisationnel répertoriées soulevaient un ensemble de commentaires très pertinents quant à leur capacité à décrire la culture et le climat en lien avec la sécurité de l'information. Il a d'ailleurs été difficile pour les participants de pointer des aspects vraiment incomplets ou erronés.

La seule faiblesse unanimement décriée par l'ensemble des participants est le manque d'importance accordé à « l'imputabilité » parmi les valeurs présentées. Même si cette valeur était implicitement représentée au sein d'autres valeurs, les participants pensaient que le tout devait être plus clairement mis en évidence à cause du rôle important de cette valeur pour expliquer la mise en œuvre de pratiques sécuritaires dans leur organisation respective. Selon eux, plus les employés tendent, au sein de l'organisation, à assumer les conséquences des décisions prises et gestes posés, plus ils se sentiront responsables et seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, s'ils évoluent dans un contexte organisationnel où personne n'est jamais désigné responsable de rien, moins élevées sont les chances qu'ils mettent en œuvre des pratiques sécuritaires.

Ainsi, des changements ont été apportés au protocole pour la prochaine étape de collecte de données. De prime abord, pour éviter que les participants ne lisent que le titre des cartes et qu'ils ne se fient qu'à leur interprétation, il a été décidé d'identifier les cartes par des numéros au lieu de noms, et de les présenter au hasard au participant. À titre d'exemple, la croyance « Responsabilité d'assurer la sécurité de l'information » a été renommée « Croyance #1 ». Comme on a pu le constater à l'étape C, par la suite, cela a forcé le participant à lire l'ensemble du contenu de la carte plutôt que de se limiter au nom de l'élément. Cette expérience avec les professionnels a aussi démontré la pertinence de consacrer plus d'effort à la compréhension conceptuelle des croyances, des valeurs et des caractéristiques du climat que de se hâter à mesurer le construit. De ce fait, les deux items sur les cartes ont été remplacés par les propositions sous-jacentes aux croyances, aux valeurs et aux caractéristiques du climat (qui ont été présentées au chapitre 2) pour en faciliter la compréhension et pour alléger le contenu de la carte (voir les nouvelles cartes à l'annexe 6). Ensuite, la valeur « Imputabilité » a été ajoutée à la liste de valeurs en sécurité de l'information. Pour l'étape de collecte de données suivante, une carte concernant la valeur « Imputabilité » a été ajoutée au matériel de l'exercice de priorisation (voir annexe 6).

3.3 Étape C : Rencontres individuelles avec des professionnels en sécurité de l'information

Les rencontres individuelles avec les professionnels en sécurité de l'information avaient les objectifs suivants : recueillir les commentaires des professionnels en sécurité de l'information dans le but de valider les croyances, les valeurs et les caractéristiques du climat et déterminer, grâce à des exercices de priorisation, afin d'obtenir une liste, à la fois complète et parcimonieuse de celles qui pourraient être les plus susceptibles d'influencer la variable dépendante.

3.3.1 Cueillette des données

Afin d'atteindre ces objectifs, des rencontres individuelles avec 11 professionnels en sécurité de l'information ont été tenues. Bien que les experts invités fussent différents de ceux rencontrés lors de l'étape B, ils devaient répondre aux mêmes critères de sélection. Ils ont également été recrutés par réseau de contacts personnel et par la méthode de la boule de neige. Ainsi, les participants rencontrés provenaient d'organisations de diverses industries et occupaient différents postes (gestionnaire, conseiller ou encore consultant en sécurité de l'information). De plus, l'échantillon se distinguait par sa moyenne élevée de 17 années d'expérience accumulées en sécurité de l'information. Somme toute, la pluralité des profils des participants rencontrés a permis de collecter des données d'une grande richesse.

Pendant chaque rencontre individuelle, un enregistrement audio et une prise de notes ont été utilisés afin de collecter les données après avoir obtenu le consentement du participant. Dans le cas où le participant ait refusé de se faire enregistrer (tels les participants #7 et #14), la prise de notes a été privilégiée afin de capturer l'information provenant de l'entrevue.

Les rencontres individuelles se sont ouvertes sur une présentation du sujet et les objectifs de recherche du mémoire, suivie d'une discussion concernant le lexique du mémoire et l'influence du contexte organisationnel sur la mise en œuvre de pratiques sécuritaires par les employés. Comme pour le groupe de discussion, l'objectif de cette discussion était aussi de s'assurer que le participant comprenne bien le modèle de la figure 2.3. Le participant a pu poser des questions et partager ses réflexions tout au long de la discussion. Par la suite, le professionnel rencontré a dû réaliser les trois exercices de priorisation (un pour les croyances, un pour les valeurs et un pour les caractéristiques du climat) où il a dû classer, par ordre d'importance, les éléments qui, selon lui, exerçaient le plus d'influence sur la variable dépendante, la mise en œuvre des pratiques sécuritaires par les employés. D'ailleurs, le participant pouvait se référer en tout temps durant l'exercice au modèle illustré à la figure 2.3. Pour chaque exercice, des cartes, sur

lesquelles figuraient le type et le numéro d'un élément donné (par exemple, Croyance #1, Valeur #2 ou bien Caractéristique du climat #3, etc.), sa définition et des propositions pouvant l'expliquer (voir figure 3.4, et pour l'intégralité des cartes utilisées durant cette étape, se référer à l'annexe 6), lui ont été distribuées au hasard. Le participant a été invité à commenter les cartes, à partager ses impressions, ses réflexions et son processus décisionnel et à les prioriser par rapport à leur potentielle influence sur la variable dépendante, pendant et suite aux exercices de priorisation.

Figure 3.4 : Exemple de carte utilisée lors d'un exercice de priorisation de l'étape C

CROYANCE #1

Croyance partagée dans l'organisation qui indique qui a la responsabilité d'assurer la sécurité de l'information.

Plus on croit dans l'organisation que la sécurité de l'information est du ressort exclusif du département informatique, moins les employés se sentiront responsables de mettre en œuvre des pratiques sécuritaires. À l'opposé, si on croit que tout le monde dans l'organisation a une responsabilité quant à la sécurité de l'information, plus les employés se sentiront responsables de mettre en œuvre des pratiques sécuritaires.

À la fin de la rencontre, une dernière discussion portant sur les classements réalisés a permis d'obtenir des données additionnelles, puisque le participant a été convié à partager ses impressions finales en tenant compte de ses trois classements. Ces rencontres ont duré entre 60 et 90 minutes. Le déroulement détaillé de l'entrevue est présenté dans le protocole C qui figure à l'annexe 4.

3.3.2 Analyse des données

L'analyse des données collectées au cours des entrevues individuelles se base sur les classements résultant des exercices de priorisation et sur les propos émis par les participants pendant ces rencontres. Ainsi, les sous-sections suivantes expliquent comment ces données ont été exploitées à des fins d'analyse.

3.3.2.1 Analyse des classements

Au cours des entrevues individuelles, dans le cadre de trois exercices de priorisation, les participants ont dû prioriser les croyances, les valeurs et les caractéristiques du climat en fonction de leur potentielle influence sur la mise en œuvre de pratiques sécuritaires. Ainsi, dans

l'optique de déterminer les croyances, les valeurs et les caractéristiques du climat à retenir pour la sélection finale, les critères suivants ont été utilisés :

Score individuel – attribué par chacun des participants

Un score est attribué à chaque élément en fonction de sa position dans le classement de chacun des participants. Par exemple, un élément obtient un point s'il est classé à la première position du classement ou obtient deux points lorsque classé à la deuxième position du classement, et ainsi de suite. De plus, les participants avaient la possibilité d'exclure un élément du classement lorsqu'ils le trouvaient non pertinent ou bien redondant. Ainsi, un élément exclu du classement par un participant est pénalisé en obtenant le score le plus élevé : pour un nombre x d'éléments, l'élément exclu se voit attribuer le score de x+1. Par exemple, une croyance exclue se voit attribuer le score de 8 (sur sept croyances possibles). Donc, plus un élément reçoit un score faible, plus il est perçu comme étant significatif ou important par le participant dans l'explication de la variable dépendante. À l'inverse, plus le score d'un élément est élevé, moins il est considéré important par le participant. Ainsi, les scores individuels minimums et maximums possibles pour chacun des éléments sont les suivants :

- Croyance : un à huit points possibles (sur sept croyances)
- Valeur : un à 11 points possibles (sur dix valeurs)
- Caractéristique du climat : un à 12 points possibles (sur 11 caractéristiques du climat)

Les scores individuels permettent également de comptabiliser le tableau des fréquences pour un élément donné, ce qui permet d'observer combien de fois un élément donné a été classé dans le premier tiers, dans le tiers du milieu ou dans le dernier tiers du classement.

Score total – attribué par l'ensemble des participants

Le score total qu'un élément a reçu au travers des classements de l'ensemble des participants est aussi calculé. Le score total est simplement l'addition des scores individuels attribués à un élément. Il permet d'analyser comment un élément donné se positionne par rapport aux autres éléments du même type.

3.3.2.2 Analyse des propos recueillis

Outre les classements des éléments, le protocole de collecte de données a permis de recueillir les propos des participants pendant et suite aux exercices de priorisation. Ces propos complémentent les classements effectués, car ils permettent de comprendre le raisonnement et les questionnements soulevés chez les participants. D'une part, les propos émis par les

participants ont fait l'objet d'une transcription. Ils ont ensuite été examinés pour en retirer les informations suivantes :

- Le point de vue du participant pour une croyance, une valeur ou une caractéristique du climat donnée (par exemple, s'il la trouvait importante ou non par rapport à la variable dépendante);
- La raison pour laquelle une croyance, une valeur ou une caractéristique du climat donnée est importante ou non;
- Les liens que le participant tisse entre une croyance, une valeur ou une caractéristique du climat donnée et une autre;
- Les anecdotes liées à une croyance, une valeur ou une caractéristique du climat donnée, provenant de l'expérience professionnelle d'un participant.

Ces informations permettent d'orienter la décision de conserver ou de retirer une croyance, une valeur ou une caractéristique du climat donnée du modèle final. Dans le cas où un élément n'a pas été commenté par un participant, la position à laquelle il a été classé a été prise en considération puisqu'elle est révélatrice de l'opinion du participant. Par exemple, un élément qui n'a suscité aucune réaction verbale, mais qui a été placé dans le premier tiers du classement indique néanmoins qu'il s'agit d'un élément important aux yeux du participant. Dans le cas où une entrevue était dépourvue d'enregistrement audio (notamment pour les entrevues des participants #7, #13 et #14), les notes prises au cours de la rencontre ont été analysées. Il va de soi que la prise de notes n'a pu recueillir l'intégralité des propos qui ont été émis lors des entrevues. Néanmoins, les informations qui étaient les plus pertinentes ont été prises en considération et notées pour l'analyse des résultats.

Au total, les scores liés aux classements des croyances, des valeurs et des caractéristiques du climat ainsi que les propos émis par les participants ont été pris en considération de manière conjointe afin de prendre les décisions de conserver ou de retirer chacun des éléments du modèle final. Étant donné que ce travail d'analyse est exhaustif et représente le cœur même des résultats de ce mémoire, les résultats de cette analyse sont présentés dans le chapitre suivant.

3.4 Récapitulatif de l'approche méthodologique

Un récapitulatif de l'approche méthodologique de validation des éléments de la culture et du climat de la sécurité de l'information est présenté dans le tableau ci-dessous. Il reprend les objectifs, les activités et les livrables des étapes méthodologiques suivies.

Tableau 3.1 : Résumé de l'approche méthodologie

Étapes	Objectifs spécifiques	Activités	Participants	Livrable(s)/Résultats
A. Prétest - Rencontres individuelles avec des étudiants de la M.Sc.	• S'approprier et valider le protocole des rencontres individuelles; • Identifier les irritants simples liés au protocole et aux outils de collecte utilisés.	Collecte des données (60 – 90 minutes) • Présentation du mémoire, de ses objectifs de recherche et du vocabulaire utilisé; • Réalisation d'un exercice de triage de cartes selon les associations entre items et dimensions à mesurer; • Rétroaction sur l'exercice. Analyse des données • Analyse des propos recueillis; • Ajustement du protocole et de l'exercice à réaliser.	Trois étudiants de la M.Sc. en technologies de l'information.	• Reformulation de l'objectif de recherche (pour un focus plus précis); • Le protocole ajusté et prêt pour l'étape B.
B. Rencontre avec des professionnels en sécurité de l'information - Groupe de discussion	• Valider le nouveau protocole (modifié suite au prétest). • Valider les croyances, les valeurs et les caractéristiques du climat lors d'une discussion de groupe (validation apparente).	Collecte des données (180 minutes) • Présentation du mémoire, de ses objectifs de recherche et du vocabulaire associé; • Discussion sur l'influence du contexte organisationnel sur la variable dépendante (modèle de la figure 2.3); • Réalisation de trois exercices de priorisation (pour les croyances, les valeurs et les caractéristiques du climat) individuellement; • Réalisation de trois exercices de priorisation (pour les croyances, les valeurs et les caractéristiques du climat) collectivement; • Rétroaction collective sur les exercices de priorisation collectifs. Analyse des données • Analyse des propos recueillis; • Ajustement du protocole et des outils utilisés pour l'étape C.	Trois professionnels en sécurité de l'information.	• Les croyances, les valeurs et les caractéristiques du climat ayant passé une première validation apparente; • L'ajout d'une nouvelle valeur (« Imputabilité ») à la liste d' éléments et à l'exercice de priorisation; • Le protocole ajusté est prêt pour l'étape C.

Tableau 3.1 : Résumé de l'approche méthodologie (suite et fin)

Étapes	Objectifs spécifiques	Activités	Participants	Livrable(s)/Résultats
C. Rencontres individuelles avec des professionnels en sécurité de l'information	• Valider les croyances, les valeurs et les caractéristiques du climat; • Déterminer les éléments organisationnels les plus importants par rapport à la variable dépendante.	<u>Collecte des données (60-90 minutes par rencontre)</u> • Présentation du mémoire, de ses objectifs de recherche et du vocabulaire associé; • Discussion sur l'influence du contexte organisationnel sur la variable dépendante (modèle de la figure 2.3); • Réalisation de trois exercices (priorisation des cartes); • Rétroaction sur les exercices de priorisation. <u>Analyse des données</u> • Analyse des classements (score individuel et score total); • Analyse des propos recueillis.	11 professionnels en sécurité de l'information.	• Une liste de croyances, valeurs et caractéristiques du climat de la sécurité de l'information à la fois complète et parcimonieuse.

Chapitre 4 : Résultats

Ancré dans la littérature, le chapitre 2 a permis de dresser une liste exhaustive des croyances, valeurs et caractéristiques du climat qui peuvent potentiellement influencer la mise en œuvre de pratiques sécuritaires par les employés. Celle-ci a été confrontée à l'expérience de praticiens chevronnés du domaine afin d'en faire une liste qui soit à la fois complète et parcimonieuse. Ce chapitre présente donc les résultats des analyses individuelles et globales qui entourent chacune des croyances, valeurs et caractéristiques du climat. Il expose les résultats des entrevues individuelles et les analyses qui ont été menées, et ce, pour chacune des croyances, valeurs et caractéristiques du climat. Ce chapitre se conclut avec la sélection finale de croyances, valeurs et caractéristiques du climat retenues pour évaluer le contexte organisationnel pouvant influencer la mise en œuvre de pratiques sécuritaires.

Fort des résultats du prétest et du groupe de discussion, 11 professionnels en sécurité de l'information (les participants #4 à #14) ont été rencontrés. Provenant de dix organisations différentes, ils avaient en moyenne 22 années d'expérience sur le marché du travail à leur actif et, plus spécifiquement, 17 années d'expérience en sécurité de l'information. L'objectif de ces entrevues individuelles était de collecter les impressions et les commentaires des professionnels de la sécurité ainsi que les résultats des exercices de priorisation afin de déterminer les croyances, les valeurs et les caractéristiques du climat les plus à même d'influencer la mise en œuvre de pratiques sécuritaires par les employés. Pour ce faire, chacune des croyances, des valeurs et des caractéristiques du climat ainsi que les données brutes (fruits de ces rencontres individuelles) et leur analyse, sont présentées une à une. Pour chacune d'entre elles, une analyse des classements est réalisée. Il est pertinent de rappeler ici comment les points ont été attribués au classement fait par chacun des participants : l'élément le plus important (par exemple, la croyance jugée la plus importante par un participant donné) se voyait attribuer un point, la deuxième plus importante, deux points, et ainsi de suite. Un élément exclu du classement par un répondant se voyait attribuer le maximum de points, soit huit points (dans le cas d'une croyance). Ainsi, les éléments obtenant un faible score global sont parmi les plus importants aux yeux des participants. Une analyse qualitative des propos recueillis est aussi réalisée afin de mieux comprendre les classements et la position des participants. Enchaînons maintenant avec la présentation des résultats obtenus.

4.1 Croyances : résultats et analyses

Au cours des rencontres individuelles avec les professionnels en sécurité de l'information, les croyances répertoriées dans le chapitre 2 ont été présentées dans le cadre d'un exercice de

priorisation. Durant cette activité, les participants ont non seulement dû classer sept croyances par rapport à leur influence sur la mise en œuvre de pratiques sécuritaires par les employés, mais ils ont aussi dû exprimer leur opinion concernant chacune d'elles. Cette sous-section rapporte les résultats des classements et les propos découlant de ces rencontres individuelles, ainsi que les analyses individuelles et globales permettant de dresser la sélection finale de croyances susceptibles d'influencer la variable dépendante.

4.1.1 Croyances : résultats et analyses individuelles

Cette section expose les résultats du premier exercice de priorisation, qui portait sur les sept croyances qui avaient été relevées dans le chapitre 2. Ici, il sera d'abord question d'analyser les résultats à l'aide d'une analyse individuelle, où les classements et les propos émis par les participants sont examinés dans le but de déterminer si la croyance est importante pour expliquer l'influence du contexte organisationnel sur la mise en œuvre de pratiques sécuritaires par les employés. Dans le cas où l'analyse individuelle n'est pas concluante quant à la décision de garder ou d'omettre la croyance de la sélection finale, une analyse globale est conduite. Cette dernière a pour but de comparer cette croyance à d'autres croyances tout en étant présentée à la fin de la section afin de déterminer les croyances à retenir pour la sélection finale.

4.1.1.1 Croyance #1 : Responsabilité d'assurer la sécurité de l'information

CROYANCE #1

Croyance partagée dans l'organisation qui indique qui a la responsabilité d'assurer la sécurité de l'information.

Plus on croit dans l'organisation que la sécurité de l'information est du ressort exclusif du département informatique, moins les employés se sentiront responsables de mettre en œuvre des pratiques sécuritaires. À l'opposé, si on croit que tout le monde dans l'organisation a une responsabilité quant à la sécurité de l'information, plus les employés se sentiront responsables de mettre en œuvre des pratiques sécuritaires.

- **Résultats**

Par l'entremise des classements réalisés par les participants, cette croyance a obtenu entre un et six points de la part des participants. De plus, aucun participant n'a écarté cette croyance de son classement. Des commentaires sur cette croyance ont été colligés pour chacun des participants, sauf pour les participants #7 et #13 (dans ces derniers cas, l'absence de commentaires peut s'expliquer par une prise de notes incomplète ou par le silence des

participants). Les classements, les points attribués et les commentaires émis relatifs à cette croyance figurent dans le tableau 4.1.

Tableau 4.1 : Résultats (classements, points et commentaires) obtenus pour la croyance #1

Participant	Classement de la croyance (sur 7)	Points attribués	Commentaires sur cette croyance
Participant #4	6	6	• « C'est polarisé comme croyance. » • « J'ai vu que quand la responsabilité de la sécurité est juste attribuée aux équipes de sécurité ; ça nuit de manière phénoménale. Ça enlève toute la responsabilité. Ça a l'effet contraire de la responsabilité morale. » *(à propos de la proposition « Département informatique »*) • « Je ne suis pas sûr que ce soit mieux. Ça m'a toujours donné l'impression que ça dilue la responsabilité. Oui [quand c'est l'affaire de tous, c'est l'affaire de personne]. Il y a des personnes-clé qui doivent être responsables. Je pense que tout le monde a une forme de responsabilité, mais ce n'est pas tout le monde égal. Il doit y avoir des pôles de responsabilité et il faut que ça soit respecté. […] Dans mon entreprise, j'ai souvent entendu la sécurité est l'affaire de tous et tous ces éléments-là de façon péjorative. » *(à propos de la proposition « L'affaire de tous »*) • « Il y a plusieurs spins sur la même idée. C'est comme… La croyance #7 et la croyance #1… Je trouve que c'est la même thématique, mais juste phrasée différemment. » *(lien avec la croyance #7)*
Participant #5	4	4	• « Importante, mais cette croyance et la croyance #2 reviennent à la même chose, parce qu'elles concernent la gestion de la sécurité de l'information. » *(lien avec croyance #2)* • Il suggère de les combiner.
Participant #6	4	4	• « Oui, c'est un élément super important qui influence directement. »
Participant #7	3	3	• *(Aucun commentaire)*
Participant #8	2	2	• « Les gens voient tellement la sécurité comme une affaire des TI, une affaire technique [dans son entreprise]. » *(lien avec croyance #2)* • « Ça ressemble à la croyance #2. » *(lien avec la croyance #2)*

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.1 : Résultats (classements, points et commentaires) obtenus pour la croyance #1 (suite)

Participant	Classement de la croyance (sur 7)	Points attribués	Commentaires sur cette croyance
Participant #9	6	6	• « Qui a la responsabilité? La réponse est 'tout le monde'. Je suis totalement en accord avec ça. » • « Non, peut-être dans le milieu policier ou militaire [la sécurité est déléguée entièrement aux TI]. Dans le milieu militaire, on ne demande pas de trop réfléchir, mais de se conformer. Je ne connais pas vraiment, mais c'est ma compréhension. Dans le milieu policier, on demande aux gens d'agir, on leur demande d'être 'intelligents'. Alors, on parle de maturité et les entreprises ont des niveaux de maturité différents. Alors, dans des grandes entreprises de type paragouvernemental ou gouvernemental, on va travailler beaucoup sur la synergie entre l'individu et la technologie. Pour les entreprises qui sont moins matures, par exemple dans le secteur manufacturier, elles sont tellement en retard sur la sécurisation de leur environnement que la priorité est de sécuriser technologiquement. Actuellement, l'eau coule de partout. Alors, ce qu'elles veulent, c'est un plombier qui va arrêter l'eau où elle coule. Une fois qu'elles vont avoir réglé les problèmes de plomberie, là elles vont parler aux résidents de la résidence pour leur dire comment utiliser les bons robinets et comment les fermer correctement. Là, elles sont plus dans une situation de répondre à l'urgence parce que leur maturité n'est pas là. Et je te parle des entreprises manufacturières qui ont fait ce constat-là. Il y en a plusieurs qui ne sont même pas rendues à ce constat-là. Pour eux, il n'y a pas de problème. Alors, là, on est loin… »
Participant #10	3	3	• « Encore c'est une balance de juste mesure. » *(lien avec la croyance #7)* • « Ce qui est important, c'est de faire en sorte que les gens croient qu'on se fie sur eux, qu'on se base sur eux, qu'ils sont importants pour préserver la sécurité de l'organisation. Donc, [il faut] les impliquer comme partenaires. Si, par contre, ça tombe trop sur leurs épaules, ils vont te dire 'attends minute, je ne suis pas payé par faire la job de quelqu'un en sécurité', puis il va y avoir une émeute. Ils vont dire 'ça n'a pas d'allure, blah-blah'. Le rôle du département de sécurité TI est d'agir en guide et de les inspirer à agir de façon sécuritaire […] par des méthodes appropriées. Malheureusement, tu ne peux pas l'appliquer parce que, au-delà de la culture en sécurité, il y a la culture d'entreprise et ça encore ça varie beaucoup. Il faut que ça soit la mobilisation, le partenariat, faut qu'il soit dans un langage que les gens comprennent. Si tu fais ça dans un langage de sécurité TI, tu commences à parler de botnet et des détails techniques, tu les as perdus. Oui, c'est super intéressant, mais ça veut dire quoi pour eux autres ? Il faut trouver le langage. Qu'est-ce qui pourrait leur faire mal à eux ? Comment ça va les toucher personnellement ? Quel est l'impact ? Il faut que ça les touche personnellement. » • « J'ai de la difficulté avec la croyance #1 et la croyance #7 parce que j'ai de la difficulté à donner une importance relative à l'un ou l'autre. Et parce que, pour les deux, ça peut varier. Dans ma tête, je vois toutes sortes de scénarios et ça dépend énormément d'une entreprise à l'autre. » *(lien avec la croyance #7)*

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.1 : Résultats (classements, points et commentaires) obtenus pour la croyance #1 (suite et fin)

Participant	Classement de la croyance (sur 7)	Points attribués	Commentaires sur cette croyance
Participant #11	3	3	• « Je suis d'accord. 100%.» • « C'est certain que si tu crois que c'est seulement la responsabilité des experts en sécurité de faire la sécurité… Ça a beaucoup été ça dans le passé. […] Mettons que je suis en charge d'un programme où je donne un flux d'information à certains clients, très simple sur où je dois déployer ma sécurité pour que la confidentialité, l'intégrité, la disponibilité soient assurées. Il y a tellement de tentacules que le upper manager ne peut pas le savoir sauf s'il est expert en sécurité lui-même… Il ne peut pas savoir où sont justement les priorités. Puis là, tu dis 'Quoi? On a des gens qui travaillent en sécurité. Aie, c'est eux autres qui vont faire ça'. Mais là, on arrive dans les nouveaux programmes où on demande au program owner d'identifier les besoins en sécurité de son programme. » *(à propos de la* p*roposition « Département informatique »*) • « Oui [la complexité amène un désengagement des gens]. C'est la complexité et la peur de l'inconnu. C'est tellement complexe qu'ils m'ont dit 'J'espère que ce n'est pas moi qui est en charge de ça'. » *(à propos de la* p*roposition « L'affaire de tous »*)
Participant #12	2	2	• « Si quelqu'un le lit vite 'qui est responsable d'assurer la sécurité?', ben je ne sais pas… C'est que dans n'importe quel projet, il n'y a qu'une seule personne qui est accountable. Là, si vous dites non, on est tous responsables. Si on l'est tous, ça veut dire que personne l'est vraiment. On ne peut pas être tous accountable. Peut-être juste changer le libellé. C'est le rôle de qui… Parce que pour moi, responsabilité et accountability, je fais le lien, il n'y a qu'une seule personne, ça va être le directeur de la sécurité de l'information, le responsable, le CISO, peu importe… Ça, c'est sa job à lui de s'assurer que tout est coordonné. Mais c'est le rôle de chacun… Je pense que c'est ce que vous voulez dire? »
Participant #13	1	1	• *(Aucun commentaire)*
Participant #14	3	3	• Très proche aussi de la croyance #2. *(lien avec la croyance #2)*
	Score global =	**37 pts**	

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels présentés dans le tableau 4.1 permettent d'arriver aux fréquences présentées dans le tableau 4.2. Ce tableau montre que sept participants ont placé cette croyance dans le premier tiers, deux participants l'ont fait au tiers du milieu et deux autres l'ont classée dans le dernier tiers du classement.

Tableau 4.2 : Tableau des fréquences pour la croyance #1

	Position	Fréquence	Total
Premier tiers	1	1	7
	2	2	
	3	4	
Tiers du milieu	4	2	2
Dernier tiers	5	-	2
	6	2	
	7	-	

- **Analyse des résultats obtenus pour cette croyance**

La majorité des participants (#7, #8, #10, #11, #12, #13 et #14) a placé cette croyance dans le premier tiers du classement, ce qui lui a valu un score global relativement faible de 37 points (pour un score global possible variant entre 11 et 88 points). Les commentaires des participants étaient d'ailleurs le reflet de ce classement car ils étaient pour la plupart positifs. En effet, les participants #5, #6, #9 et #11 ont déclaré que cette croyance avait une influence importante pour la mise en œuvre de pratiques sécuritaires. Pour les participants #7 et #13, l'examen de leur classement respectif s'est avéré utile pour découvrir ce dont ils en pensaient. Ces derniers l'ont tous deux placée dans le premier tiers du classement, ce qui signifie qu'elle leur semble importante.

Les critiques émises à l'encontre de cette croyance se sont principalement adressées à sa deuxième proposition: « Si on croit que tout le monde dans l'organisation a une responsabilité quant à la sécurité de l'information, plus les employés se sentiront responsables de mettre en œuvre des pratiques sécuritaires. ». En effet, les participants #4, #10, #11 et #12 ont plutôt pensé que responsabiliser tous les employés de l'organisation menait ceux-ci à se désengager à cause de la complexité de la sécurité de l'information. Ils ont d'ailleurs estimé que tous les employés pouvaient être responsabilisés, mais qu'ils devaient être guidés par un responsable en sécurité de l'information (CIO, sponsor, etc.).

Plusieurs participants ont également relevé le lien entre cette croyance et d'autres croyances qui leur ont été présentées. Les participants #4 et #10 ont relevé un lien entre cette croyance et

la croyance #7 (« Le maillon faible en sécurité de l'information »). Selon eux, les deux traitaient de la même thématique, c'est-à-dire de la responsabilité de l'humain quant à la sécurité de l'information. Les participants #5, #8 et #14 ont considéré, quant à eux, que cette croyance ressemblait fortement à la croyance #2 (« Vision de l'organisation quant à la nature des défis en termes de la sécurité de l'information ») puisque les deux traitent de la manière dont l'humain gère la sécurité de l'information.

Ainsi, en considérant les classements et les propos des participants, on peut affirmer que cette croyance est importante pour expliquer l'influence du contexte organisationnel sur la variable dépendante. Les commentaires et les critiques émis par les participants pourraient mener à modifier la deuxième proposition de cette croyance, voire de la fusionner avec une autre croyance. Un examen global est nécessaire afin de déterminer si cette croyance doit être modifiée ou être conservée telle quelle. Cet examen sera présenté dans la section 4.1.2.

4.1.1.2 Croyance #2 : Vision de l'organisation quant à la nature des défis en termes de sécurité de l'information

CROYANCE #2

Croyance partagée dans l'organisation qui indique la nature des défis rencontrés en sécurité de l'information.

Plus on croit dans l'organisation que la sécurité de l'information est avant tout un défi d'ordre technique, moins les employés sentiront la nécessité de mettre en œuvre des pratiques sécuritaires parce qu'ils se fieront aux solutions technologiques. À l'opposé, plus on a la conviction dans l'organisation qu'il y a des composantes humaine, technique et managériale à la sécurité de l'information, plus élevées sont les chances que tout le monde jouera le rôle qu'il a à jouer afin de protéger l'information.

- **Résultats**

Par l'entremise des classements réalisés par les participants, cette croyance a obtenu entre un et cinq points de la part des participants. De plus, aucun participant n'a écarté cette croyance de son classement. Des commentaires sur cette croyance ont été colligés pour chacun des participants, sauf pour le participant #13 (dans ce dernier cas, l'absence de commentaires peut s'expliquer par une prise de notes incomplète ou par le silence du participant). Les classements, les points attribués et les commentaires émis relatifs à cette croyance figurent dans le tableau 4.3.

Tableau 4.3 : Résultats (classements, points et commentaires) obtenus pour la croyance #2

Participant	Classement de la croyance (sur 7)	Points attribués	Commentaires sur cette croyance
Participant #4	5	5	• « Je mettrais ça sur un poster, puis je le ferai lire à beaucoup de gens. Ce sont des choses qu'il y a à faire pour augmenter la culture de sécurité. C'est de la responsabilisation au lieu de rendre ça imputable aux machines, c'est comment les êtres humains interagissent. »
Participant #5	4	4	• « Personne n'est conscient que ses actions peuvent mettre en péril l'entreprise. » • « Importante, mais [la croyance #1] et la croyance #2 reviennent à la même chose, parce qu'elles concernent la gestion de la sécurité de l'information. » *(lien avec la croyance #1)*
Participant #6	5	5	• « Je suis assez d'accord. Je ne suis pas sûre que ce soit le premier élément. Je le mettrais très proche. Je suis certaine que ça l'influence, mais pas le premier. »
Participant #7	4	4	• Il trouve qu'il y a un problème de cohérence entre les propositions de la croyance #2 et les propositions de la croyance #7. Son raisonnement l'amène au fait que l'humain est le maillon faible. *(lien avec la croyance #7)*
Participant #8	3	3	• « Les gens voient tellement la sécurité comme une affaire des TI, une affaire technique [ndlr : il faisait le lien avec la culture de la sécurité de l'information dans son entreprise]. » *(lien avec croyance #1)* • « [La croyance #1] ressemble à la croyance #2. » *(lien avec la croyance #1)* • « Ah oui, celle-là est belle. Effectivement, ça, c'est clair. Quand les gens pensent que c'est juste relié à la technologie, ils ne font rien de spécial. Ils vont toujours se fier à la technologie qui va faire le travail pour eux. »
Participant #9	4	4	• « Totalement d'accord. »
Participant #10	2	2	• « Ça c'est important par exemple. C'est très important. En effet, il ne faut pas tout laisser sur les épaules de la technologie. Il faut d'abord mobiliser [les employés] et faire en sorte que les employés prennent conscience des obligations qui leur reviennent, pour ne pas les laisser aller et dire 'le département de sécurité va s'en occuper pour nous'. Non. Ça, c'est un aspect extrêmement important. Il faut travailler fort pour l'avoir, mais une fois acquis, c'est un gain très important pour l'organisation. »
Participant #11	5	5	• « Exactement, c'est tout à fait vrai. » • « Le mariage entre la gouvernance et la sécurité des TI se perd. Donc là, c'est les TI, c'est les gars en TI. […] Mais pourquoi on véhicule ces images-là? C'est parce que c'est encore pittoresquement ce qu'on voit, ce qu'on voudrait pouvoir avoir. La techno, c'est eux autres qui s'en occupent. Mais ce n'est pas comme ça. [Et puis] le fait que beaucoup des higher ups sont peu conscients; ce n'est pas eux qui vont mettre en place dans leur groupe cette conscientisation-là. […] Et c'est ancré dans la croyance que la sécurité is a necessary evil, pas un enabler. Pis c'est la base, c'est un racisme, si tu veux, envers la techno 'Ah, ça là, c'est sûr, c'est leur problème, pas le mien!'. […] Encore le chicken and egg : le gestionnaire va être content de comprendre ce qu'il doit gérer en sécurité, une fois qu'il sait ce qu'il a à gérer en sécurité. Mais ils ne le savent pas. Donc, c'est l'insouciance, l'ignorance…» *(à propos de la proposition « Défi technique»)*

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.3 : Résultats (classements, points et commentaires) obtenus pour la croyance #2 (suite et fin)

Participant	Classement de la croyance (sur 7)	Points attribués	Commentaires sur cette croyance
Participant #12	1	1	• « La croyance # 2, [porte sur la nature de la sécurité de l'information] et la croyance # 7 aussi; il est lié à la nature aussi je trouve… Beaucoup. Entre [les croyances] #2 et #7, je trouve qu'il y a beaucoup de redondance. La nature générale de l'être humain, non… C'est lié à #2, #6 et #7… C'est pas mal lié. […] Ces trois-là, il y a tellement de redondance qu'il y a peut-être moyen de les simplifier. […] Le plus important pour moi, c'est le #2. » *(lien avec la croyance #6 et la croyance #7)*
Participant #13	2	2	• *(Aucun commentaire)*
Participant #14	3	3	• Interprétation très proche de #7. Pourquoi y a-t-il deux croyances? La différence est très mince. Je trouve que #2 est le négatif de #7. *(lien avec la croyance #7)*
Score global = 38 points			

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels du tableau 4.3 permettent d'arriver aux fréquences présentées dans le tableau 4.4. Ce tableau montre que cinq participants ont placé cette croyance dans le premier tiers, trois participants l'ont fait au tiers du milieu et trois autres l'ont classée dans le dernier tiers du classement.

Tableau 4.4 : Tableau des fréquences pour la croyance #2

	Position	Fréquence	Total
Premier tiers	1	1	5
	2	2	
	3	2	
Tiers du milieu	4	3	3
Dernier tiers	5	3	3
	6	-	
	7	-	

- **Analyse des résultats obtenus pour cette croyance**

Cette croyance a été placée dans le premier tiers du classement par la majorité des participants (#8, #10, #12, #13 et #14), ce qui lui a conséquemment valu un score global assez bas, soit 38 points (pour un score global possible variant entre 11 et 88 points). L'importance de cette croyance se reflète également dans les commentaires des participants puisque la majorité d'entre eux (#4, #5, #6, #8, #9, #10 et #11) remarque qu'elle est importante pour influencer la variable dépendante. En ce qui concerne le participant #13, son classement montre qu'il l'a placée en deuxième position de son classement. On peut ainsi en déduire qu'elle lui semblait importante.

Comme mentionné pour la croyance précédente, les participants #5 et #8 estimaient que cette croyance #2 ressemblait fortement à la croyance #1 (« Responsabilité d'assurer la sécurité de l'information ») parce qu'elles concernent la manière dont la sécurité de l'information est gérée par l'humain. En effet, la perception de la sécurité de l'information pourrait teinter la mise en œuvre de pratiques sécuritaires des employés. Ainsi, si la sécurité de l'information est un défi technique, alors l'employé serait moins porté à mettre en œuvre des pratiques sécuritaires. De plus, les participants évoquent la redondance entre cette croyance et les croyances #6 (« Nature générale de l'être humain ») (participant #12) et #7 (« Le maillon faible en sécurité de l'information ») (participants #7, #12 et #14) car elles concernent l'aspect humain en sécurité de l'information. Bien que ces croyances leur semblaient redondantes, il faut tenir compte de leurs nuances. En effet, la croyance #1 a trait à la nature de la sécurité de l'information tandis que la croyance #2 concerne les responsables de la sécurité de l'information. Pour ce qui est

de la croyance #6, elle se rapporte à la nature humaine et à ce qui les motive à mettre en œuvre des pratiques sécuritaires alors que la croyance #7 concerne le rôle que joue les employés en sécurité de l'information.

À la lumière des classements et des commentaires des participants, il est possible d'affirmer que cette croyance est importante pour expliquer l'influence du contexte organisationnel sur la variable dépendante. En effet, la majorité des participants ont placé cette croyance dans le premier tiers du classement. Les propos des participants évoquent aussi l'importance de cette croyance. De plus, les participants ont soulevé le fait que cette croyance avait plusieurs liens avec d'autres croyances. Il semblerait qu'au final, ces croyances ne sont pas ostensiblement différentes. Ces propos tendent donc vers la possibilité de fusionner cette croyance avec une autre. Bien que cette croyance soit importante, il ne reste qu'un examen global doit être conduit pour déterminer si une fusion est nécessaire. Cet examen de l'ensemble des croyances figurera à la section 4.1.2.

4.1.1.3 Croyance #3 : Importance générale qu'a la sécurité de l'information dans l'organisation

CROYANCE #3

Croyance partagée dans l'organisation qui réfère à l'importance générale que l'on accorde à la sécurité de l'information.

Plus on croit dans l'organisation que la sécurité de l'information est importante, plus les employés sentiront la nécessité de mettre en œuvre des pratiques sécuritaires. À l'opposé, si on croit dans l'organisation que la sécurité de l'information n'est pas importante, moins élevées sont les chances que les employés mettent en œuvre des pratiques sécuritaires.

- **Résultats**

Par l'entremise des classements réalisés par les participants, cette croyance a obtenu entre un et huit points de la part des participants. Seul un participant (le participant #10) a écarté cette croyance de son classement parce qu'elle ne lui semblait pas être comparable aux autres croyances. Des commentaires sur cette croyance ont été colligés pour chacun des participants, sauf pour les participants #13 et #14 (dans ces derniers cas, l'absence de commentaires peut s'expliquer par une prise de notes incomplète ou par le silence des participants). Les classements, les points attribués et les commentaires émis relatifs à cette croyance figurent dans le tableau 4.5.

Tableau 4.5 : Résultats (classements, points et commentaires) obtenus pour la croyance #3

Participant	Classement de la croyance (sur 7)	Points attribués	Commentaires sur cette croyance
Participant #4	2	2	• « Oui, il faut [avoir] une croyance partagée que la sécurité est importante. Mais [la question est] comment on le véhicule aux gens. Si on a le buy-in de la haute direction et c'est véhiculé de cette façon-là, oui, je pense que ça peut aider beaucoup la culture de sécurité dans l'organisation. »
Participant #5	1	1	• « C'est important. L'organisation doit prêcher par l'exemple en sécurité de l'information. »
Participant #6	2	2	• « Oui, définitivement. Je dirais que c'est la base. »
Participant #7	2	2	• « C'est très proche de la responsabilité morale. » *(lien avec la croyance #5*)
Participant #8	1	1	• « Oui, effectivement. Quand tout vient d'en haut, de la haute direction… C'est l'importance que les gens donnent à la sécurité. Ça part de là. Moi, je pense que ça part de l'opinion de la haute direction sur l'importance de la sécurité et le reste va découler. »
Participant #9	1	1	• « Totalement et absolument d'accord avec ça. Effectivement... Rien d'autre à dire. » • « Il faut que la haute direction manifeste clairement que la sécurité est importante. Si ce n'est pas le cas, les employés vont se dire 'pourquoi moi je me compliquerais la vie si le patron croit que ce n'est pas important?'. »
Participant #10	Exclue	8	• « Ça, c'est le pilier sur lequel tu bâtis. C'est sûr que je travaille dans ce domaine et si tu me demandes si [cette croyance] est importante, je vais dire 'ben oui, c'est très important'. Tout le monde te dit ça. Maintenant, dans quelle mesure est-ce important pour l'organisation? C'est un centre de coût, c'est quelque chose qui vaut de l'argent, ce n'est pas quelque chose qui va faire de l'argent. C'est un coût pour la business; ça ne t'apporte pas de revenu. Donc, si j'étais un haut dirigeant de l'entreprise, je sentirais le besoin de le réduire au minimum. […] Donc, l'importance accordée à la sécurité de l'information est en lien avec un risque. C'est pour cela que la notion de risque que je mentionnais tantôt est très importante pour moi. À haut niveau, tu regardes pourquoi tu mets de l'argent pour des efforts TI et en sécurité TI, tu mets de l'argent comme pour une police d'assurance pour être raisonnablement sûr que des choses mauvaises ne vont pas arriver. »
Participant #11	2	2	• « Si c'est bien, c'est tout à fait possible. Tout à fait. » • « On le voit ici [ndlr : dans son organisation]. La nature de l'entreprise est de faire de la sécurité. Ça se fait ici, 25 personnes… C'est cohésif dans tout ça. Mais j'ai travaillé dans plusieurs entreprises, où le botté d'envoi par les higher-ups était que c'est important. 'Aïe, c'est l'information privilégiée des gens. C'est leur dossier médical. On peut pas niaiser.' Mais malgré ça, il y en avait encore quelques-uns qui [n'avaient pas compris le message]. »
Participant #12	4	4	• « C'est le walk the talk [énoncé par] la compagnie. »
Participant #13	6	6	• *(Aucun commentaire)*
Participant #14	2	2	• *(Aucun commentaire)*
Score global = 31 points			

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels présentés dans le tableau 4.5 permettent d'arriver aux fréquences présentées dans le tableau 4.6. Ce tableau montre que huit participants ont placé cette croyance dans le premier tiers, un participant l'a fait au tiers du milieu, un l'a classée dans le dernier tiers du classement, et un autre l'a exclue du sien.

Tableau 4.6 : Tableau des fréquences pour la croyance #3

	Position	Fréquence	Total
Premier tiers	1	3	8
	2	5	
	3	-	
Tiers du milieu	4	1	1
Dernier tiers	5	-	1
	6	1	
	7	-	
Exclusion	-	1	1

- **Analyse des résultats obtenus pour cette croyance**

La majorité des participants (#4, #5, #6, #7, #8, #9, #11 et #14) a placé cette croyance dans le premier tiers du classement. Elle a conséquemment obtenu un faible score de 31 points (pour un score global possible variant entre 11 et 88 points). Cela se reflète également dans les propos des participants puisque sept d'entre eux (#4, #5, #6, #8, #9, #10 et #11) déclarent qu'elle est importante pour influencer la variable dépendante. Par ailleurs, si l'on se fie au classement des participants #13 et #14, on observe que cette croyance serait importante pour le premier participant, tandis qu'elle serait d'importance moindre pour le deuxième participant.

D'autre part, seul le participant #7 a spécifié que cette croyance était similaire à la croyance #5 (« Responsabilité morale en sécurité de l'information »). Si l'on se fie au classement réalisé par le participant #7, on pourrait croire que cette similitude provient de l'importance de ces deux croyances par rapport à la variable dépendante. En effet, les croyances #5 et #3 occupent respectivement la première et la deuxième place de son classement.

Les commentaires qui ont justifié l'exclusion de cette croyance par le participant #10 démontraient clairement qu'il a utilisé un angle d'interprétation différent pour classer cette croyance. Selon lui, cette croyance est relative au risque associé à la protection des actifs informationnels de l'organisation. En d'autres termes, plus le risque associé à la protection des actifs informationnels est élevé, plus l'organisation va considérer la sécurité de l'information comme étant importante en y investissant des fonds. Étant donné que cet angle d'interprétation s'éloigne de l'objectif premier poursuivi par l'exercice de priorisation, l'exclusion de cette

croyance par ce participant ne semblait pas remettre en question l'importance relative accordée à cette croyance par les autres participants.

Étant donné que cette croyance ait été majoritairement placée dans le premier tiers des classements et que la plupart des participants s'accordent à dire qu'elle a une influence sur la variable dépendante, cette croyance est à retenir pour la sélection finale.

4.1.1.4 Croyance #4 : Auto-efficacité organisationnelle face aux menaces

CROYANCE #4

Croyance partagée dans l'organisation qui réfère à la capacité de l'organisation à se défendre contre les menaces à la sécurité de l'information.

Plus on croit dans l'organisation qu'il est fondamentalement impossible d'assurer vraiment la protection de l'information, moins les employés seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si on est convaincus dans l'organisation qu'il est possible de prendre des actions préventives et de protéger l'information, plus élevées sont les chances que les employés mettront en œuvre des pratiques sécuritaires.

- **Résultats**

Par l'entremise des classements réalisés par les participants, cette croyance a obtenu entre trois et sept points de la part des participants. De plus, aucun participant n'a écarté cette croyance de son classement. Des commentaires sur cette croyance ont été colligés pour chacun des participants, sauf pour les participants #12 (dans ce cas-ci, l'absence de commentaires est due au silence de ce dernier) et #14 (dans ce dernier cas, l'absence de commentaires peut s'expliquer par une prise de notes incomplète ou par le silence du participant). Les classements, les points attribués et les commentaires émis relatifs à cette croyance figurent dans le tableau 4.7.

Tableau 4.7 : Résultats (classements, points et commentaires) obtenus pour la croyance #4

Participant	Classement de la croyance (sur 7)	Points attribués	Commentaires sur cette croyance
Participant #4	7	7	• « Il faut qu'on puisse croire qu'on est capable d'aborder [les problèmes en sécurité de l'information] et qu'on a le pouvoir de réaliser ou de protéger. Je pense que c'est très important. » • « Je n'aime pas le terme en français d'habiliter les gens; j'aime mieux le terme en anglais d'empowerment et c'est exactement ça. » *(à propos de la proposition « Impossibilité »)* • « On véhicule beaucoup l'idée que c'est une bataille perdue d'avance, puis le motivateur en moi haït ça. [On voit cette attitude de défaitisme partout.] Partout! Et c'est impossible d'aller chercher le buy-in des gens si les gens ont déjà un message négatif ou de défaitisme. » *(à propos de la proposition « Possibilité »)*
Participant #5	7	7	• Il n'est pas certain quant à la pertinence de cette croyance. Il faut ajouter la dimension temporelle. • Cette croyance peut bouger dans le temps.
Participant #6	6	6	• « Ce n'est pas que c'est moins important, c'est simplement qu'elle a moins d'influence, je pense, sur la culture. Ça, c'est un peu un élément qui ne va pas teinter l'ensemble de la culture organisationnelle, mais qui va plutôt influencer les stratégies qui vont être prises par l'équipe de la sécurité. Je ne crois pas qu'elle influence directement l'ensemble de la culture. Pour nous, comme responsables de la sécurité, c'est définitivement un élément qu'on considère, mais que c'est une croyance qui est partagée dans l'organisation? Là, je suis moins sûre à dire comment ça influence directement le comportement des employés par rapport à la sécurité. »
Participant #7	6	6	• Très faible impact parce qu'on peut rentrer [les malveillants peuvent s'infiltrer] partout… Chez NASA, CIA, FBI, malgré une auto-efficacité très élevée.
Participant #8	4	4	• « Oui, je suis d'accord, ça fait du sens. C'est sûr que quand ça vient d'en haut, de la haute direction, la haute direction met elle-même en œuvre ce qu'elle vient de dire. Oui, je pense que ça fait en sorte que les employés vont suivre et vont comprendre. Mais ce n'est pas juste de le dire, il faut le faire comprendre. Dans plusieurs cas, c'est 'oui, mais pourquoi je ferais ça ? Ça me rajoute du travail…'. Mais oui, effectivement, je suis d'accord avec cette croyance. »
Participant #9	3	3	• « Oui [pour la proposition « Impossibilité »] … Totalement d'accord [avec la proposition « Possibilité »] ».
Participant #10	5	5	• « Je suis tout à fait d'accord avec ça, mais ça a plutôt rapport à la psychologie qu'à la sécurité des TI. C'est parce que ça revient fondamentalement à la question de confiance en soi. C'est la confiance en soi de l'organisation. C'est ça ce que ça veut dire. Oui, on le rencontre souvent dans le domaine des TI, mais c'est très subjectif. Personnellement, j'aime mieux me pencher sur les trucs objectifs et tirer une conclusion à la fin. Et ça, je ne suis même pas sûr si j'attaquerais cette question au niveau organisationnel. C'est sûr que, dans le discours d'un vice-président, [on aura] 'il faut qu'on soit original, on va réussir… Oui...'. Mais c'est très subjectif par exemple. »

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.7 : Résultats (classements, points et commentaires) obtenus pour la croyance #4 (suite et fin)

Participant	Classement de la croyance (sur 7)	Points attribués	Commentaires sur cette croyance
Participant #11	6	6	• « Hum… Croyance partagée dans l'organisation qui réfère à la capacité de l'organisation de se défendre contre les menaces? Si justement historiquement, tu t'es fait planter, tu t'es fait planter, tu t'es fait planter, [alors] la croyance… Nos gars et nos filles en sécurité ne savent pas ce qu'ils font... »
Participant #12	6	6	• *(Aucun commentaire)*
Participant #13	4	4	• « Oui, c'est important. »
Participant #14	6	6	• *(Aucun commentaire)*
Score global = 60 points			

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels présentés dans le tableau 4.7 permettent d'arriver aux fréquences présentées dans le tableau 4.8. Ce tableau montre qu'un participant a placé cette croyance dans le premier tiers, deux participants l'ont fait au tiers du milieu, et huit l'ont classée dans le dernier tiers du classement.

Tableau 4.8 : Tableau des fréquences pour la croyance #4

	Position	Fréquence	Total
Premier tiers	1	-	1
	2	-	
	3	1	
Tiers du milieu	4	2	2
Dernier tiers	5	1	8
	6	5	
	7	2	

- **Analyse des résultats obtenus pour cette croyance**

Cette croyance a été placée dans le milieu ou le dernier tiers du classement par la plupart des participants (#4, #5, #6, #7, #8, #10, #11, #12, #13 et #14), ce qui lui a valu, par conséquent, un score global assez élevé de 60 points (pour un score global possible variant entre 11 et 88 points). Ces participants indiquaient d'ailleurs leur accord avec les deux propositions de cette croyance, mais que son importance pour influencer la variable dépendante était faible. Par exemple, le participant #6 a déclaré que cette croyance influençait plutôt les stratégies en sécurité de l'information que les employés. Le participant #7, quant à lui, a mentionné que l'auto-efficacité organisationnelle n'a aucune influence, puisqu'elles se croient efficaces ou non, les organisations sont toujours à la merci d'incidents de sécurité de l'information. Seul le participant #9 a classé cette croyance dans le premier tiers du classement.

Les classements et les propos des participants laissent supposer que cette croyance est d'importance moindre pour influencer la variable dépendante. Néanmoins, un examen global est nécessaire pour déterminer si cette croyance doit être retenue pour la sélection finale. Cet examen global des croyances sera présenté à la section 4.1.2.

4.1.1.5 Croyance #5 : Responsabilité morale de protéger l'information

CROYANCE #5

Croyance partagée dans l'organisation quant à la responsabilité morale que l'entreprise a de protéger les informations.

Plus on croit que l'organisation a la responsabilité morale de protéger l'information, plus les employés seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si on ne croit pas que l'organisation a cette responsabilité morale, moins élevées sont les chances que les employés mettent en œuvre des pratiques sécuritaires.

- **Résultats**

Par l'entremise des classements réalisés par les participants, cette croyance a obtenu entre un et six points de la part des participants. De plus, aucun participant n'a écarté cette croyance de son classement. Des commentaires sur cette croyance ont été colligés pour chacun des participants, sauf pour les participants #13 et #14 (dans ces derniers cas, l'absence de commentaires peut s'expliquer par une prise de notes incomplète ou par le silence des participants). Les classements, les points attribués et les commentaires émis relatifs à cette croyance figurent dans le tableau 4.9.

Tableau 4.9 : Résultats (classements, points et commentaires) obtenus pour la croyance #5

Participant	Classement de la croyance (sur 7)	Points attribués	Commentaires sur cette croyance
Participant #4	1	1	• « Je pense qu'elle a un impact sur l'intelligence parce qu'elle introduit l'imputabilité sur la responsabilité des gens envers la sécurité de l'information. Pour moi, on sort de la conformité et on va vers l'intelligence parce que cette responsabilité morale vient chercher les valeurs des gens à vouloir protéger les actifs informationnels. »
Participant #5	6	6	• « Ça peut aider. »
Participant #6	1	1	• « Oui. Je suis totalement d'accord. Ça va beaucoup rejoindre le premier élément [dans son classement], l'importance générale. C'est comme un sous-élément. » *(lien avec croyance #3)*
Participant #7	1	1	• La responsabilité morale de l'individu est encore plus importante que celle organisationnelle.
Participant #8	6	6	• « Effectivement, mais ça revient un peu à la conformité quand on dit responsabilité morale. Moi, je vois responsabilité morale dans le sens que, légalement, tu dois protéger l'information. Je le vois dans ce sens-là. C'est juste moral de protéger… Par acquit de conscience, je dois la protéger, mais j'ai rarement vu une entreprise qui, par acquit de conscience, protégeait son information. Généralement, c'est parce qu'il y a une loi en arrière, ou il y a quelque chose qui l'oblige. Donc, la responsabilité morale, je dirais que c'est quasiment plus chaque employé qui se donne la responsabilité morale. » • « Oui. Il y a des gens qui vont se dire 'Non, moi, dans mon éthique de travail, je ne peux pas croire qu'on fait ça ou je ne peux pas laisser passer ça'. J'ai des gens qui viennent me voir avec des problématiques comme ça. Regarde, ce matin, je vois des données d'employés; il me semble que ça ne fait pas de sens. Je le vois plus au niveau individuel qu'au niveau organisationnel. Moi, personnellement, je n'ai jamais vu une organisation se dire 'c'est dans nos valeurs éthiques de protéger l'information'. Bien souvent si ce n'est pas quelqu'un pour leur faire peur… C'est comme ça. Moi, je le vois de même. »
Participant #9	2	2	• « Oui, je suis d'accord avec ça. » • « C'est un autre niveau. La moralité ne vient pas en premier. La moralité vient plutôt après l'importance [de la sécurité de l'information] dans l'organisation. » *(lien avec la croyance #3)*
Participant #10	6	6	• « Là, on combine la morale avec la business. Oui, c'est intéressant, mais s'il n'y a pas d'obligation de conformité, de loi ou de règlement, ou encore politique interne, on ne peut pas être contre la vertu, on veut protéger les choses. Mais si ça coûte 2 millions, on va se limiter aux affaires qu'on est obligé de faire. Donc, il n'y a personne qui est contre la morale et les bonnes façons d'agir, mais quand on leur demande d'ouvrir la bourse et sortir un peu d'argent, ben ça va aller à l'année prochaine, etc. » • « Cette croyance est trop philosophique et elle l'est encore plus que [la croyance # 6]. Et je ne sais pas dans quelle mesure elle est importante. Je la mettrais en dernier. » *(lien avec la croyance #6)*

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.9 : Résultats (classements, points et commentaires) obtenus pour la croyance #5 (suite et fin)

Participant	Classement de la croyance (sur 7)	Points attribués	Commentaires sur cette croyance
Participant #11	1	1	• « Ce n'est pas juste le moral, c'est la loi [COBIT, ISO, etc.]. Si l'entreprise n'a pas bien compris ses besoins en sécurité, que ce soit moralement ou pas dans ses besoins d'affaires, là… Garbage in, garbage out. »
Participant #12	5	5	• « La responsabilité morale de l'entreprise à protéger ses informations, ça demande une maturité des quatre phases de développement… Ça demande une maturité qu'un employé n'a pas nécessairement, mais qu'un VP va avoir. Donc, si on pose l'hypothèse qu'on s'adresse à des employés, qu'on questionne des employés, le volet de la responsabilité morale, il est nice, mais… À la fin [du classement], peut-être. »
Participant #13	5	5	• *(Aucun commentaire)*
Participant #14	5	5	• *(Aucun commentaire)*
Score global = 39 points			

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels présentés dans le tableau 4.9 permettent d'arriver aux fréquences présentées dans le tableau 4.10. Ce tableau montre que cinq participants ont placé cette croyance dans le premier tiers, aucun participant ne l'a fait au tiers du milieu, et six l'ont classée dans le dernier tiers du classement.

Tableau 4.10 : Tableau des fréquences pour la croyance #5

	Position	Fréquence	Total
Premier tiers	1	4	5
	2	1	
	3	-	
Tiers du milieu	4	-	-
Dernier tiers	5	3	6
	6	3	
	7	-	

- **Analyse des résultats obtenus pour cette croyance**

Le classement de cette croyance est mitigé. Cinq des participants (#4, #6, #7, #9 et #11) l'ont mise dans le premier tiers tandis que six autres (#5, #8, #10, #12, #13 et #14) l'ont classée dans le dernier tiers du classement. Cela lui attribue un score global assez bas de 39 points (pour un score global possible variant entre 11 et 88 points). Le bilan est tout aussi mitigé pour les commentaires des participants étant donné que certains (#4, #5, #6, #9 et #11) s'entendent sur le fait que cette croyance soit susceptible d'influencer la variable dépendante, tandis que d'autres (#8, #10 et #12) questionnent ouvertement cette influence. D'autre part, les classements des participants #13 et #14 ont révélé que cette croyance leur semblait importante, puisqu'ils l'ont classée dans le premier tiers.

Pour les participants #7 et #8, la responsabilité morale relève davantage du niveau individuel que du niveau organisationnel. Cette croyance a également été critiquée par les participants #10, #11 et #12 car ils croyaient que cette croyance était secondaire et qu'elle n'était que le produit de la maturité ou de la conformité à la sécurité de l'information. D'après les propos des participants #10 et #12, ce sont donc la maturité et la conformité qui exerceraient davantage un impact sur la mise en œuvre de pratiques sécuritaires. Ces éléments de réponse remettaient donc en question l'influence de cette croyance sur la variable dépendante.

Les participants #6 et #9 ont soulevé le lien entre cette croyance et la croyance #3 (« Importance générale qu'a la sécurité de l'information »). Pour eux, cette croyance découle de la croyance #3 car si la sécurité de l'information est importante au sein de l'organisation, alors les employés seraient davantage enclins à protéger l'information. Le participant #10, quant à lui, a dit que

cette croyance était trop philosophique (plus que la croyance #6, « Nature générale de l'être humain »). On pourrait donc penser que, pour ce participant, ces deux croyances sont plus facilement observables en théorie qu'en pratique.

Compte tenu du classement mitigé de cette croyance et des commentaires de certains participants (stipulant que cette croyance influence indirectement la variable dépendante), elle doit faire l'objet d'un examen global. Cet examen sera présenté à la section 4.1.2.

4.1.1.6 Croyance #6 : Nature générale de l'être humain

CROYANCE #6

Croyance partagée dans l'organisation quant à la nature générale de l'être humain et, plus spécifiquement, en ce qui a trait aux raisons qui motivent ses actions.

Plus on croit dans l'organisation que les gens agissent dans le meilleur intérêt de l'organisation et qu'on peut leur faire confiance, plus ils seront responsables et motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si on croit que les gens sont fondamentalement mauvais et qu'on les déresponsabilise en les contrôlant comme des enfants, moins les gens mettront en œuvre des pratiques sécuritaires.

- **Résultats**

Par l'entremise des classements réalisés par les participants, cette croyance a obtenu entre un et sept points de la part des participants. De plus, aucun participant n'a écarté cette croyance de son classement. Des commentaires sur cette croyance ont été colligés pour chacun des participants, sauf pour le participant #14 (dans ce dernier cas, l'absence de commentaire peut s'expliquer par une prise de notes incomplète ou par le silence du participant). Les classements, les points attribués et les commentaires émis relatifs à cette croyance figurent dans le tableau 4.11.

Tableau 4.11 : Résultats (classements, points et commentaires) obtenus pour la croyance #6

Participant	Classement de la croyance (sur 7)	Points attribués	Commentaires sur cette croyance
Participant #4	4	4	• « Je pense que la nature générale de l'être humain, c'est de faire confiance. Et faire confiance, c'est un terrain miné avec la sécurité de l'information parce qu'il y a trop de domaines où on veut abuser pour attaquer justement une organisation. Donc, faire confiance à la nature générale des gens, c'est un risque. Je ne vois pas nécessairement comment il peut aider à faire augmenter la culture. Il faut faire attention. Il faut avoir une petite dose raisonnable de méfiance. » • « On apprend avec l'expérience que même si les gens veulent être responsables, ils n'ont pas les bons réflexes. Donc, on peut faire confiance aux gens, mais ils ne sont pas nécessairement bien outillés aujourd'hui pour pouvoir faire la bonne action. On a souvent des cas de phishing où on veut manipuler les gens, on les appelle. […] Puis, ça n'enlève rien à la bonne volonté ou à l'honnêteté des gens qui travaillent [dans notre organisation]. Ce sont des gens qui sont habiles pour les exploiter. […] Se soucier des gens fait partie de la génétique de notre organisation. On veut faire confiance à nos gens, mais il faut les outiller, il faut qu'ils apprennent. »
Participant #5	2	2	• « Ça touche à la question de l'engagement organisationnel qui va responsabiliser les employés. »
Participant #6	7	7	• « Cela, je ne sais pas parce que je ne sais pas ce qui influence réellement la culture de l'organisation. Je ne sais pas si on peut réellement faire un lien avec cet élément-là. C'est comme si on dit que si on ne fait pas confiance aux gens, ils ne mettront pas en œuvre des pratiques de sécurité. Par contre, si on a confiance en eux, ils vont le faire. Donc, c'est comme dire dans le fond que la culture de sécurité dépend de la confiance qu'on a en nos employés. Ça, je ne suis pas certaine d'être d'accord. Je doute. » • « J'ai l'impression, sans l'avoir essayé, que la bonne direction est de leur faire confiance et de les responsabiliser. J'ai l'impression que l'autre façon de faire qui est plus traditionnelle, l'expérience a démontré que ça ne marche pas si bien que ça. Dans d'autres entreprises qui font ça, c'est comme 'Non, tout le monde a accès, on vous fait confiance. On va vous surveiller un petit peu, mais on vous fait confiance'. Puis, eux autres, c'était comme une nouvelle façon de faire; je ne sais pas s'ils réussissent bien ou pas, mais ça m'amène à réfléchir et en tout cas… C'est plus positif pour un employé et c'est plus motivant. Est-ce que ça marche ? Je ne le sais pas. Mais jusqu'à maintenant, on a beaucoup fait, on a beaucoup contrôlé et là, on s'en va vers l'autre façon de faire de plus en plus. » *(lien avec la croyance #7)*
Participant #7	5	5	• On peut faire confiance si on sait que les gens ont les compétences [par exemple, dans le département TI]. Si information security literacy n'est pas fort, la confiance doit être limitée.

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.11 : Résultats (classements, points et commentaires) obtenus pour la croyance #6 (suite)

Participant	Classement de la croyance (sur 7)	Points attribués	Commentaires sur cette croyance
Participant #8	7	7	• « Petit bémol pour cette croyance… » • « Il ne faut pas aller trop loin dans la confiance malheureusement. Il y a des menaces internes de plus en plus présentes. Il faut trouver un équilibre, je pense. Il ne faut pas les contrôler comme des enfants. Je pense qu'il faut leur donner les outils et les procédures et leur faire comprendre que 'je te fais confiance, mais je suis toujours là pour te surveiller'. Si on met la limite de vitesse à 100, on s'entend que tout le monde va rouler à 140-150. L'autre extrême, si je me méfie de tout le monde, personne ne va travailler ici. Il faut être capable de travailler ensemble. » *(à propos de la proposition « Confiance »)*
Participant #9	7	7	• « J'ai un peu de difficulté avec ça. » • « L'être humain est un animal fondamentalement méchant. On ne peut pas présumer que parce qu'on fait confiance aux gens, que les gens vont faire les choses correctement. On veut qu'ils agissent dans le meilleur intérêt de l'organisation, mais ça revient toujours à eux essentiellement. Et s'il y a une contradiction entre l'organisation et eux, la tendance va être, s'il n'y a pas d'encadrement, que les individus voient à leurs intérêts au détriment de ceux de l'organisation. *(à propos de la proposition « Confiance »)* • Malheureusement, l'expérience me démontre qu'il faut mettre des encadrements pour la raison que je t'ai dite, c'est-à-dire que l'être humain va penser à lui en premier. L'autre chose est que, même s'ils sont responsables, ils ne connaissent peut-être pas les pratiques sécuritaires. Alors, il faut leur mettre des encadrements. […] Oui, il faut faire confiance à ses employés, mais il ne faut pas avoir une confiance aveugle. Alors, la règle du moindre effort, la règle de la simplicité, la règle de 'ça n'arrivera pas à moi, je n'ai pas d'information hautement sensible', etc... Non! On ne traite pas l'employé comme un enfant, mais on le met dans un environnement encadré et on s'assure de certains niveaux de conformité. Mais il faut qu'on lui explique. Si je ne fais qu'imposer les façons de faire, sans qu'il ne comprenne pourquoi, je ne lui change pas les croyances. *(à propos de la proposition « Confiance »)* • « À cela, il faut mettre une nuance dans l'affirmation que j'ai faite. La nature humaine est comme ça : les gens vont penser à eux avant de penser à l'organisation et je pense que c'est humain. Il ne s'agit pas de déresponsabiliser et de contrôler comme des enfants. Il faut les sensibiliser, il faut les informer adéquatement. C'est que je crois qu'une personne qui est bien informée va avoir une meilleure croyance de la sécurité qu'elle doit mettre en place et de là, ses pulsions primaires de penser à lui avant... Si on l'informe bien, si on le sensibilise bien, si on l'encadre bien, il va comprendre pourquoi et il va avoir une meilleure tendance à penser au bien-être de l'organisation parce qu'il va comprendre l'objectif ultime qui est de protéger l'organisation et qui va indirectement le protéger. » *(à propos de la proposition « Contrôle »)*

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.11 : Résultats (classements, points et commentaires) obtenus pour la croyance #6 (suite)

Participant	Classement de la croyance (sur 7)	Points attribués	Commentaires sur cette croyance
Participant #10	1	1	• « Ça, c'est philosophique, la nature de l'être humain. […] Oui, c'est très vrai. Par contre, ça dépend beaucoup des expériences personnelles et du genre d'individus avec lesquels tu as à composer dans l'organisation. On a une tendance de par la nature humaine de voir le monde avec nos yeux et ceux des gens qui nous entourent de très près. Alors ceux qui sont proches de nous ont une tendance forte à nous ressembler. Donc, on est dans notre petite bulle, dans notre petit monde. C'est une question de croyances. J'ai certaines croyances parce que, dans ma petite bulle, ça se passe de même. Mais j'ai l'impression que […] la nature humaine peut être différente en fonction du contexte des individus. [Il n'y a pas nécessairement de différence entre une grande organisation et une PME]. […] Si l'entreprise a grandi, c'est parce qu'il y a certains principes qui lui ont permis de grandir. Entre autres, le fait de grandir veut dire qu'il y a eu certains gens qui se sont impliqués, qui ont contribué, etc. Et tu vois, une petite compagnie, une start-up en sécurité, ils font ça parce qu'ils mangent de ça du matin au soir. Ce n'est pas nécessairement la taille, ça peut être plutôt l'industrie [ndlr : dans laquelle œuvre l'organisation]. Par industrie, ça peut varier beaucoup, plus que par taille de l'organisation, à mon avis. » • « Dans certains endroits, tu as raison de contrôler les employés pour des affaires… » *(à propos de la proposition « Contrôle »)* • « La question de la nature humaine est très complexe parce que la nature humaine varie beaucoup. Mais si je reviens à mon petit monde connu, le genre de clients avec lequel je travaille d'habitude, oui, c'est très important. C'est très important parce que je travaille avec des gens intelligents, des gens qui sont très motivés, qui connaissent leur place et ils aiment être considérés comme des partenaires plutôt que de petits enfants que je vais contrôler. Ça peut même être insultant. » *(à propos de la proposition « Confiance »)*
Participant #11	7	7	• « Encore dans l'exercice du gouvernement, une des croyances de base des personnes qui établissaient la structure, c'est que there is good will for the implementation of security in government. Donc il y a de la bienveillance envers la sécurité. Mais c'est le contraire. C'est la première affaire qui saute. Regarde, ils veulent faire de la sécurité, on veut juste mettre des objectifs, ça va marcher. Au contraire, on va se planter comme il faut! On ne peut pas faire confiance aux gens. Les gens, s'ils sont bien guidés, tu peux leur faire confiance à tour de bras. Mais si les higher-ups ne donnent pas à la masse le coup d'envoi, l'importance qu'ils ont, les ressources pour que ça puisse se faire, eux autres sont laissés devant… Il y a un gouffre tellement énorme à combler dans leurs façons de faire, pis sans qu'ils aient les outils pour, ben là, regarde… » *(à propos de la proposition « Confiance »)* • « Je suis absolument convaincu [que l'on peut faire confiance] si l'être humain est bien encadré. » *(à propos de la proposition « Confiance »)*

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.11 : Résultats (classements, points et commentaires) obtenus pour la croyance #6 (suite et fin)

Participant	Classement de la croyance (sur 7)	Points attribués	Commentaires sur cette croyance
Participant #12	7	7	• « La croyance #2 c'est sur ce qu'est la nature [ndlr : la nature de la sécurité de l'information] et la croyance #7 aussi; il est lié à la nature aussi je trouve… Beaucoup. Entre la croyance #2 et la croyance #7, je trouve qu'il y a beaucoup de redondance. La nature générale de l'être humain, non… C'est lié [aux croyances] #2, #6 et #7… C'est pas mal lié. […] Ces trois-là, il y a tellement de redondance qu'il y a peut-être moyen de les simplifier. […] Le plus important pour moi, c'est la #2. » *(lien avec la croyance #2et la croyance #7)* • « Écoute [les croyances] #6 et #7... Je relis les définitions… Pourtant, j'ai été dans des entreprises publiques, pas gouvernementales, mais publiques, des grosses… J'ai de la misère à arrimer ça à la réalité en 2016. Je ne dis pas que ça n'arrive pas, mais il y a quand même un accroissement de la maturité depuis une vingtaine d'années. Il y a 20 ans, tu pouvais dire que tes employés, c'était des épais, qu'ils sont habituellement irresponsables. Si quelqu'un osait dire 'Mais pourquoi tu les as engagés à ce moment-là?' Je fais un parallèle avec le télétravail. Il y a 20 ans, le télétravail, ça n'était pas accepté. Pourtant, la même règle s'appliquait. Tu leur fais confiance pour qu'ils travaillent chez vous et pour leur donner accès à de l'information sensible, mais tu ne leur fais pas confiance pour travailler de la maison? Il y a peut-être un problème. On a dépassé ça. Donc, je ne pense pas c'est applicable. […] On pense que les gens sont foncièrement mauvais? Je ne le pense pas. Je ne suis pas d'accord. » *(lien avec la croyance #7; à propos de la proposition « Contrôle »)*
Participant #13	3	3	• « Tout à fait d'accord [ndlr : par rapport aux propositions de la croyance] et c'est relativement important [par rapport à l'impact sur la variable dépendante]. »
Participant #14	7	7	• *(Aucun commentaire)*
Score global = 57 points			

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels présentés dans le tableau 4.11 permettent d'arriver aux fréquences présentées dans le tableau 4.12. Ce tableau montre que trois participants ont placé cette croyance dans le premier tiers, un participant l'a fait au tiers du milieu, et sept l'ont classée dans le dernier tiers du classement.

Tableau 4.12 : Tableau des fréquences pour la croyance #6

	Position	Fréquence	Total
Premier tiers	1	1	3
	2	1	
	3	1	
Tiers du milieu	4	1	1
Dernier tiers	5	1	7
	6	-	
	7	6	

- **Analyse des résultats obtenus pour cette croyance**

Cette croyance a majoritairement été placée dans le tiers du milieu et dans le dernier tiers du classement par les participants (#4, #6, #7, #8, #9, #11, #12 et #14), ce qui lui a valu un score global relativement élevé de 57 points (pour un score global possible variant entre 11 et 88 points). Cela transparaissait aussi dans les propos des participants puisque seuls trois d'entre eux (#7, #10 et #13) évoquaient son influence sur la mise en œuvre de pratiques sécuritaires.

Les participants ont critiqué cette croyance pour diverses raisons. Les participants #4 et #6 questionnaient l'influence sur la variable dépendante de cette croyance. Les participants #8, #9 et #12 avaient de la difficulté à croire que cette croyance reflétait la réalité. Ils n'étaient d'accord avec aucune des propositions de la croyance : « Plus on croit dans l'organisation que les gens agissent dans le meilleur intérêt de l'organisation et qu'on peut leur faire confiance, plus ils seront responsables et motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si on croit que les gens sont fondamentalement mauvais et qu'on les déresponsabilise en les contrôlant comme des enfants, moins les gens mettront en œuvre des pratiques sécuritaires. » Pour ces participants, il était nécessaire d'atteindre un juste équilibre entre la confiance et le contrôle pour que l'influence sur la mise en œuvre de pratiques sécuritaires soit significative.

Enfin, les participants #6 et #12 ont fait le lien entre cette croyance et la croyance #7 (Le maillon faible en sécurité de l'information »). Ces participants ont tous deux souligné qu'il était plus efficace de faire confiance aux employés que de les contrôler. En effet, pour le

participant #6, les employés ne sont pas foncièrement mauvais. Le participant #12, quant à lui, a déclaré qu'être contrôlant envers eux n'était plus ancré dans la réalité organisationnelle (notamment avec le télétravail qui gagne en popularité dans les organisations). Tel que mentionné dans l'analyse individuelle de la croyance #2, le participant #12 a évoqué la redondance entre les croyances #2 (« Vision de l'organisation quant à la sécurité de l'information »), #6 et #7 (« Le maillon faible en sécurité de l'information ») parce qu'elles ont trait à l'aspect humain en sécurité de l'information. Or, comme mentionné précédemment, ces croyances concernent des thèmes différents. Selon ce participant, la croyance #2 est la plus importante.

En raison du constat mitigé découlant de l'analyse individuelle de cette croyance, celle-ci doit faire l'objet d'un examen global. Cet examen est présenté à la section 4.1.2.

4.1.1.7 Croyance #7 : Le maillon faible en sécurité de l'information

CROYANCE #7

Croyance partagée dans l'organisation quant au rôle que joue l'être humain dans la sécurité de l'information.

Plus on croit dans l'organisation que les gens représentent le maillon faible en sécurité de l'information, moins les employés seront motivés à mettre en œuvre des pratiques sécuritaires parce que l'entreprise mettra en place des outils menant à une déresponsabilisation. À l'opposé, si on croit que les gens sont des maillons importants de la sécurité de l'information, plus élevées sont les chances que l'organisation leur fera confiance, les responsabilisera et que les employés agiront dans le meilleur intérêt de l'organisation en mettant en œuvre des pratiques sécuritaires.

- **Résultats**

Par l'entremise des classements réalisés par les participants, cette croyance a obtenu entre un et huit points de la part des participants. Un participant (le participant #7) a exclu cette croyance de son classement parce qu'il désapprouvait l'une des propositions de cette croyance, ce qui explique l'attribution de 8 points. Tous les participants ont d'autant plus émis des commentaires par rapport à cette croyance. Les classements, les points attribués et les commentaires émis relatifs à cette croyance figurent dans le tableau 4.13.

Tableau 4.13 : Résultats (classements, points et commentaires) obtenus pour la croyance #7

Participant	Classement de la croyance (sur 7)	Points attribués	Commentaires sur cette croyance
Participant #4	3	3	• « L'être humain est une faiblesse pour la sécurité de l'information que les gens utilisent à leur détriment. Puis, ça n'enlève rien à la bonne volonté ou à l'honnêteté des gens qui travaillent [dans notre organisation]. Ce sont des gens qui sont habiles pour les exploiter. […] L'être humain n'a pas été bâti, sociologiquement parlant, pour œuvrer dans un monde connecté comme ça, où nos sensors ne réagissent pas aux bons aspects de gestion de risque. Il faut faire attention. On n'est pas outillé encore pour avoir les bons réflexes. » *(à propos de la proposition « Maillon faible » ; lien avec la croyance #6)* • « Maillon faible ou maillon important, j'aime beaucoup le terme. Ça change le spin de défaitisme à quelque chose qui habilite les gens. Oui, on est un maillon important. Je pense que c'est quelque chose de super important et c'est quelque chose que j'ai très peu entendu comme croyance. J'ai rarement entendu cette croyance. » • « Il y a plusieurs spins sur la même idée. C'est comme… [les croyances] #7 et #1… Je trouve que c'est la même thématique, mais juste phrasée différemment. » *(lien avec la croyance #1)*
Participant #5	2	2	• « Il faut amener les gens à comprendre l'utilité de la sécurité. Il faut leur faire savoir que ça affecte leur vie personnelle. » • « Les entreprises gagnent à éduquer leurs employés. »
Participant #6	3	3	• « Hum, intéressant ça. Oui, je suis d'accord. Quand on lit [la définition], c'est super important comme élément. » • « Je suis étonnée. Je ne suis pas certaine d'être d'accord avec l'énoncé dans le sens que je ne crois pas que ça représente ce qui est systématiquement fait. Je pense que, quand on considère que [les employés] sont le maillon faible, on va plutôt renforcer la sensibilisation et tenter de les responsabiliser. Un humain étant ce qu'il est, on a d'autres moyens pour palier, on ne peut pas juste se fier à l'humain. Ça ne va pas faire en sorte qu'on ne va pas travailler sur sa sensibilisation et sa responsabilisation. C'est là que j'ai un petit bémol. À part ça, c'est important comme croyance. » *(à propos de la proposition « Maillon faible »)*
Participant #7	Exclue	8	• Selon lui, si les gens sont conscients qu'ils sont le maillon faible, ils seront davantage motivés à adopter des comportements sécuritaires parce qu'ils savent que, s'il y a un incident, ça serait à cause d'eux. Les outils de surveillance n'amènent pas à la déresponsabilisation. Ça pousse les gens à avoir de meilleurs comportements parce qu'ils savent que le cas contraire a des conséquences. Avec cette interprétation, la croyance #7 est très importante. *(à propos de la proposition « Maillon faible »)* • Il a notamment exclu cette croyance de son classement car il trouvait que la première proposition ne reflétait pas la réalité. *(à propos de la proposition « Maillon faible »)*

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.13 : Résultats (classements, points et commentaires) obtenus pour la croyance #7 (suite)

Participant	Classement de la croyance (sur 7)	Points attribués	Commentaires sur cette croyance
Participant #8	5	5	• « Oui, mais ça dépend. » • « C'est sûr que les gens sont le maillon le plus facile à exploiter, ingénierie sociale et toutes ces choses-là. Est-ce que c'est le maillon faible? En fait, pour moi, parce que les gens sont exploitables, ils deviennent le maillon important dans le sens que c'est important pour moi de les éduquer, de les former, de les sensibiliser, parce que, s'ils n'agissent pas de la bonne façon, j'aurais beau mettre 50 millions en technologie, il y en a un qui va donner son mot de passe à un moment donné. C'est sûr et certain. Quand je vois ça 'maillon faible', ça dépend de comment on le présente. » *(à propos de la proposition « Maillon faible »)*
Participant #9	5	5	• « Plusieurs choses là-dedans. » • « En général, l'employé est le maillon faible de la sécurité de l'information. On a beau mettre toutes les technologies, les pratiques, les directives, etc. en place, si l'employé ne les utilise pas, les bris de sécurité vont être inévitables. Mais, lorsque je lis la définition, je comprends que si l'entreprise considère l'employé comme étant non fiable, moins l'employé sera motivé à mettre en pratique des mesures de sécurité. Pour moi, ce sont deux choses en parallèle. Il faut tenir compte que l'être humain est le maillon faible, mais il faut mettre en place des pratiques qui vont favoriser son intérêt et sa motivation à respecter l'encadrement en sécurité. C'est là la nuance. » *(à propos de la proposition « Maillon faible »)*
Participant #10	3	3	• « C'est discutable. Ça dépend beaucoup du contexte organisationnel. Le rôle de l'humain… L'humain n'est pas plus faible que la technologie. Il se peut que ça soit vrai; il se peut aussi que ça ne soit pas du tout le cas. C'est très variable. Ça dépend beaucoup d'une organisation à l'autre. » • « Il ne faut surtout pas les déresponsabiliser. Il ne faut pas dire 'de toute façon, vous comptez pour rien dans la sécurité. On va mettre un bon outil qui va vous remplacer'. Il ne faut pas lancer ce message. Par contre, oui, tu leur fais confiance, mais tu vas aussi avoir des outils qui vont valider le comportement. Il faut qu'ils se sentent surveillés. Il faut qu'ils sachent que quelqu'un regarde les journaux. Il faut faire confiance, oui, parce que si tu serres la vis trop, ils vont être très créatifs et ils vont trouver des façons de faire ce qu'ils veulent faire puis éviter les pratiques de sécurité mises en place, mais il ne faut pas laisser croire que l'humain est moins important que la technologie. »

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.13 : Résultats (classements, points et commentaires) obtenus pour la croyance #7

Participant	Classement de la croyance (sur 7)	Points attribués	Commentaires sur cette croyance
Participant #11	4	4	• « L'approche maintenant est plus de se protéger. C'est que tu assumes, tu sais qu'ils sont en dedans. The bad guy is inside. Avant, ce qu'on disait 'Je me protège contre l'externe'. » • « L'inconnu… C'est tout à fait relié au fait que nos technologies sont d'emblée brisées, elles sont d'emblée tout à fait vulnérables. Donc, le commun des mortels qui utilise les technologies, il sait que c'est déjà tout plein de trous, que même l'antivirus ne sera pas suffisant. Donc, d'un côté, ils se sentent un petit peu débordés d'être identifiés comme étant le maillon faible. Ils ont la responsabilité de la sécurité, mais ils n'ont pas d'idée ce qu'ils font. S'il n'y a pas un bon awareness program pour les administrateurs, pour les software developers, pour les secrétaires, pour le commun des mortels… Donc 'Ah, comment ça, c'est tout le temps de ma faute? Si c'est de ma faute, aide-moi! Je ne sais pas qu'est-ce que je fais.' La preuve est que bien des gens qui trouvent une clé USB dans le garage ou quelque part […] vont l'apporter au bureau parce qu'on a de la sécurité au bureau! […]» *(à propos de la proposition « Maillon faible »)*
Participant #12	3	3	• « [La croyance] #2, c'est quoi la nature [ndlr : la nature de la sécurité de l'information] et [la croyance] #7 aussi; elle est liée à la nature aussi je trouve… Beaucoup. Entre [la croyance] #2 et [la croyance] #7, je trouve qu'il y a beaucoup de redondance. La nature générale de l'être humain, non… C'est lié [aux croyances] #2, #6 et #7… C'est pas mal lié. […] Ces trois-là, il y a tellement de redondance qu'il y a peut-être moyen de les simplifier. […] Le plus important pour moi, c'est la #2. » *(lien avec la croyance #2 et la croyance #6)* • « Écoute [les croyances] #6 et #7... Je relis les définitions… J'ai de la misère à arrimer ça à la réalité en 2016. Je ne dis pas que ça n'arrive pas, mais il y a quand même un accroissement de la maturité depuis une vingtaine d'années. Il y a 20 ans, tu pouvais dire que tes employés, c'était des épais, qu'ils sont habituellement irresponsables. Si quelqu'un osait dire 'Mais pourquoi tu les as engagés à ce moment-là?' Je fais un parallèle avec le télétravail. Il y a 20 ans, le télétravail, ça n'était pas accepté. Pourtant, la même règle s'appliquait. Tu leur fais confiance pour qu'ils travaillent chez vous et pour leur donner accès à de l'information sensible, mais tu ne leur fais pas confiance pour travailler de la maison? Il y a peut-être un problème. […] Fait que je ne pense pas c'est applicable. Les gens sont foncièrement mauvais? Je ne suis pas d'accord. » *(lien avec la croyance #6)* • « Je pense que [la croyance] #7… J'aime bien l'énoncé, mais je lis le détail et je ne l'aime pas. Je n'aime pas parce que je ne suis pas d'accord. Je suis le premier à dire que les employés, l'être humain, c'est le maillon faible, mais je n'ai pas l'impression que ça déresponsabilise. Au contraire. » *(à propos de la proposition « Maillon faible »)*
Participant #13	7	7	• Il est en désaccord avec la première portion de la proposition car, selon lui, les employés demeureront toujours le maillon faible. • Selon lui, que l'on fasse confiance ou non, il y a des mesures technologiques à mettre en place pour protéger l'information.

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.13 : Résultats (classements, points et commentaires) obtenus pour la croyance #7 (suite et fin)

Participant	Classement de la croyance (sur 7)	Points attribués	Commentaires sur cette croyance
Participant #14	1	1	• Il n'est pas d'accord avec les propositions. • Si les gens savent qu'ils sont le maillon faible, ils seront plus responsables, ils feront plus attention à leurs comportements et aux risques. *(à propos de la proposition « Maillon faible »)*
Score global = 44 points			

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels présentés dans le tableau 4.13 permettent d'arriver aux fréquences présentées dans le tableau 4.4. Ce tableau montre que six participants ont placé cette croyance dans le premier tiers, un participant l'a fait au tiers du milieu, trois l'ont classée dans le dernier tiers du classement, et un autre l'a exclue du sien.

Tableau 4.14 : Tableau des fréquences pour la croyance #7

	Position	Fréquence	Total
Premier tiers	1	1	6
	2	1	
	3	4	
Tiers du milieu	4	1	1
Dernier tiers	5	2	3
	6	-	
	7	1	
Exclusion	-	1	1

- **Analyse des résultats obtenus pour cette croyance**

Cette croyance a été classée dans le premier tiers du classement par la majorité des participants (#4, #5, #6, #10, #12 et #14), ce qui lui a donné un score global de 44 points (pour un score global possible variant entre 11 et 88 points). Deux participants (#4 et #6) ont exprimé initialement leur accord quant à l'influence positive de cette croyance sur la mise en œuvre de pratiques sécuritaires par les employés, mais ont ensuite fait quelques suggestions afin de clarifier les propositions liées à cette croyance.

La plupart des critiques (#4, #6, #7, #8, #9, #10, #12, #13 et #14) ont été formulées à l'égard de la première proposition de cette croyance : « Plus on croit dans l'organisation que les gens représentent le maillon faible en sécurité de l'information, moins les employés seront motivés à mettre en œuvre des pratiques sécuritaires parce que l'entreprise mettra en place des outils menant à une déresponsabilisation ». D'une part, les participants #4, #7, #12 et #14 ont estimé que le fait d'être un maillon faible en sécurité de l'information ou non n'avait aucune incidence sur la variable dépendante. Pour ces participants, l'être humain agira toujours pour le bien-être de son organisation. D'autre part, les participants #6, #8, #9, #12 et #13 étaient en désaccord avec cette proposition car, selon eux, l'organisation mettrait plutôt en place des outils menant à une responsabilisation (telles que la sensibilisation à la sécurité de l'information ou bien la formation) dans le cas où les employés y étaient perçus comme étant le maillon faible en sécurité de l'information.

Le participant #4 a mentionné que cette croyance et la croyance #1 (« Responsabilité d'assurer la sécurité de l'information » étaient redondantes car elles traitaient de la même thématique (à savoir, à qui était assignée la responsabilité d'assurer la sécurité de l'information). Il a également fait le lien entre cette croyance et la croyance #6 (« Nature générale de l'être humain). Enfin, tel qu'il a été dit précédemment, le participant #12 a remarqué que les croyances #2, (« Vision de l'organisation quant à la nature des défis en termes de sécurité de l'information »), #6 (« Nature générale de l'être humain) et #7 étaient redondantes car elles concernaient l'aspect humain de la sécurité de l'information. À son avis, la croyance #2 était la plus importante. Les propos de ces participants indiquaient la possibilité de fusionner cette croyance avec une autre, puisque la parcimonie est l'un des objectifs de ce mémoire. Comme il a été mentionné précédemment, ces croyances semblaient redondantes car elles traitent de l'aspect humain de la sécurité de l'information. Il semblerait toutefois que ces participants n'aient pas noté les nuances existant entre ces croyances.

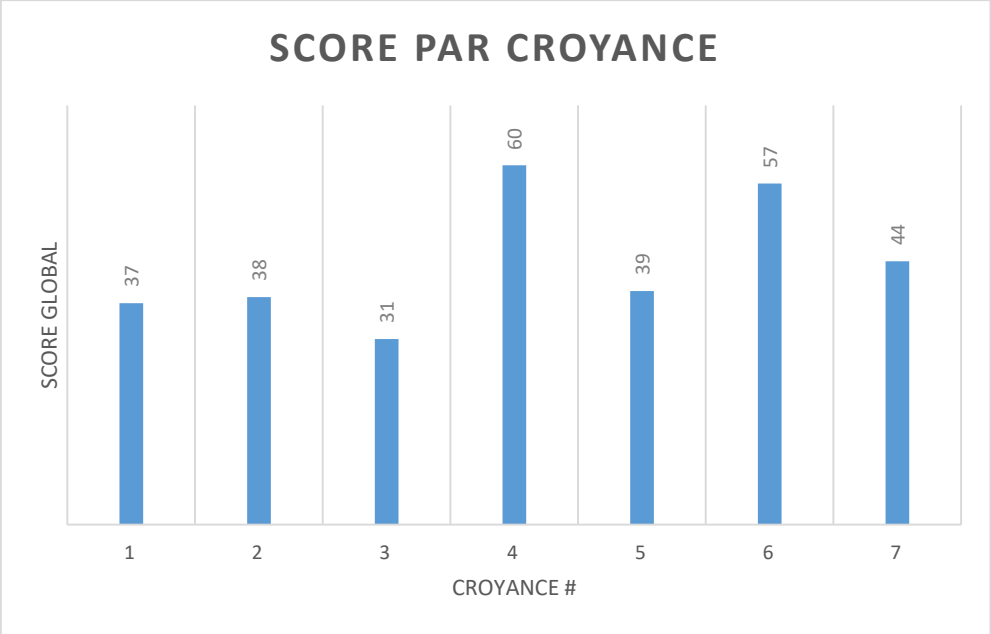
D'ailleurs, le participant #7 a exclu cette croyance en raison de son désaccord avec la première proposition : « Plus on croit dans l'organisation que les gens représentent le maillon faible en sécurité de l'information, moins les employés seront motivés à mettre en œuvre des pratiques sécuritaires parce que l'entreprise mettra en place des outils menant à une déresponsabilisation. ». Selon lui, si les gens croient qu'ils sont le maillon faible, alors ils vont être davantage motivés à agir de façon sécuritaire. Il a toutefois déclaré que cette croyance a une influence importante quant à la variable dépendante si l'on se borne à l'esprit général qui s'en dégage.

L'exclusion de cette croyance basée sur le contenu de la première proposition et les critiques aussi formulées à l'égard de cette même proposition ont conduit à l'examen d'une possible nouvelle formulation qui refléterait l'ensemble des commentaires reçus. Pourtant, toute formulation ancrée dans l'expérience des participants menait à la conclusion que, dans un sens ou dans l'autre (maillon faible ou fort), la croyance n'avait au total que peu d'influence sur la variable dépendante. En effet, que l'on croit que les employés représentent le maillon faible en sécurité de l'information ou non, l'impact sur la mise en œuvre de pratiques sécuritaires est le même. Selon l'analyse de cette croyance, les employés seront toujours motivés à mettre en œuvre des pratiques sécuritaires. À cela s'ajoute le fait que cette croyance soit redondante avec d'autres croyances, qui semblent exercer plus d'influence sur la variable dépendante que celle-ci. C'est pourquoi cette croyance n'est pas retenue pour la sélection finale.

4.1.2 Croyances : Analyse globale et décisions

L'analyse individuelle de chacune des croyances a permis de prendre une décision d'inclusion ou de rejet dans le cas de plusieurs croyances, mais certains résultats plus mitigés (telles les croyances #1, #2, #4, #5, et #6) requièrent une analyse comparative élargie afin de voir si les résultats globaux pourraient alimenter la réflexion. Pour ce faire, les analyses individuelles de la sous-section précédente (qui comprend les résultats et les commentaires des participants à l'égard de chaque croyance) ainsi que le score global attribué à chacune des croyances (voir la figure 4.1) sont utilisés. Il faut rappeler que plus le score global est faible dans la figure 4.1, plus la croyance est susceptible d'influencer la variable dépendante selon les participants.

Figure 4.1 : Score obtenu pour chacune des croyances suite à l'ensemble des classements



Il est important de rappeler que les analyses individuelles ont permis d'emblée d'inclure la croyance #3 (« Importance générale qu'a la sécurité de l'information ») et d'écarter la croyance #7 (« Le maillon faible en sécurité de l'information ») de la liste finale des croyances. Les conclusions des autres analyses individuelles montraient que les croyances #1, #2, #4, #5, et #6 devaient faire l'objet d'un examen global.

L'analyse des croyances #1 (« Responsabilité d'assurer la sécurité de l'information ») et #2 (« Vision de l'organisation quant à la nature des défis en termes de sécurité de l'information ») a permis de reconnaître qu'elles étaient d'importantes influences sur la variable dépendante. La figure 4.1 vient appuyer ce constat puisque ces deux croyances se sont vues attribuer le deuxième et le troisième score global le plus faible parmi toutes les croyances. La forte ressemblance entre la croyance #1 et la croyance #2, qui a été relevée par certains participants,

a motivé la conduite d'un examen global. L'analyse des propos de ces derniers indique la possibilité de les fusionner, car elles semblaient mutuellement redondantes. En effet, ces croyances concernaient la manière dont les employés géraient la sécurité de l'information. Plus précisément, ces croyances portaient sur la perception de la sécurité de l'information des employés, et comment celle-ci influençait leur mise en œuvre de pratiques sécuritaires. Puisque ce mémoire vise à la fois la complétude et la parcimonie, il s'avère donc judicieux de fusionner ces croyances.

Afin d'englober l'esprit qui se dégage des croyances à fusionner, la nouvelle croyance portera le nom suivant : « Vision de l'organisation quant à la nature des défis et la gestion de la sécurité de l'information ». L'idée que le département informatique soit exclusivement en charge de la gestion de la sécurité de l'information (provenant de la première proposition de la croyance #1) sera par contre intégrée à la première proposition de la nouvelle croyance #A. La définition de la nouvelle croyance sera ajustée en conséquence. Les croyances initiales ainsi que la nouvelle croyance découlant de leur fusion sont présentées dans le tableau 4.15.

Tableau 4.15 : Fusion des croyances #1 et #2

Croyances initiales	Croyance #A fusionnée
Croyance #1 : Responsabilité d'assurer la sécurité de l'information **Croyance partagée dans l'organisation qui indique qui a la responsabilité d'assurer la sécurité de l'information.** *Plus on croit dans l'organisation que la sécurité de l'information est du ressort exclusif du département informatique, moins les employés se sentiront responsables de mettre en œuvre des pratiques sécuritaires. À l'opposé, si on croit que tout le monde dans l'organisation a une responsabilité quant à la sécurité de l'information, plus les employés se sentiront responsables de mettre en œuvre des pratiques sécuritaires.*	**Croyance A : Vision de l'organisation quant à la nature des défis et à la gestion de la sécurité de l'information** **Croyance partagée dans l'organisation qui indique la nature des défis rencontrés en sécurité de l'information et de la manière <u>dont ils sont gérés</u>.** *Si l'on croit que la sécurité de l'information est un défi d'ordre technique, <u>plus élevées sont les chances que la responsabilité de la protection de l'information soit exclusivement assignée au département informatique</u>. À l'opposé, si l'on est convaincu que la sécurité de l'information a des composantes humaine, technique et managériale, plus élevées sont les chances que tous les employés joueront un rôle dans la protection de l'information.*
Croyance #2 : Vision de l'organisation quant à la nature des défis en termes de sécurité de l'information **Croyance partagée dans l'organisation qui indique la nature des défis rencontrés en sécurité de l'information.** *Plus on croit dans l'organisation que la sécurité de l'information est avant tout un défi d'ordre technique, moins les employés sentiront la nécessité de mettre en œuvre des pratiques sécuritaires parce qu'ils se fieront aux solutions technologiques. À l'opposé, plus on a la conviction dans l'organisation qu'il y a des composantes humaine, technique et managériale à la sécurité de l'information, plus élevées sont les chances que tout le monde jouera le rôle qu'il a à jouer afin de protéger l'information.*	

Légende : le texte souligné indique ce qui a été modifié dans le texte de nouvelle croyance.

L'analyse individuelle de la croyance #4 (« Auto-efficacité organisationnelle face aux menaces ») a révélé qu'elle était d'importance moindre pour influencer la variable dépendante et qu'elle devait faire l'objet d'une analyse globale. Bien que certains participants l'aient considérée importante, il n'en demeure pas moins que son impact sur la variable dépendante leur semblait relativement faible. Cette croyance pourrait être une source d'influence plus importante sur les pratiques d'affaires (par exemple, les stratégies en sécurité de l'information, comme l'a mentionné le participant #6) que sur les comportements quotidiens des employés. À ce constat s'ajoute le fait que son score global de 60 points est le plus élevé parmi toutes les croyances (voir figure 4.1). Dans un but de parcimonie, il s'avère donc pertinent de ne pas conserver cette croyance pour la sélection finale de croyances.

L'analyse individuelle de la croyance #5 (« Responsabilité morale ») a révélé la nécessité de conduire un examen global. En effet, es commentaires des participants se sont avérés être mitigés. Les participants pour lesquels la responsabilité morale était une influence importante pour la variable dépendante opéraient dans des organisations où la manipulation de données personnelles sensibles de clients (par exemple, la date de naissance, le numéro d'assurance sociale, le dossier médical, etc.) était au cœur de leurs activités. Pour les autres participants, pour qui la manipulation de ce type de données est moins critique dans leur organisation, la responsabilité morale en sécurité de l'information n'est pas innée. Selon eux, elle découle plutôt du respect de la conformité et des lois. Elle n'exerce donc pas d'influence directe sur la mise en œuvre de pratiques sécuritaires par les employés. De ce fait, on constate donc que la responsabilité morale en sécurité de l'information n'est pas universelle. D'autre part, en se basant sur la figure 4.1, on observe que la croyance #5 détient un score global de 39 points, qui est le quatrième le plus élevé parmi toutes les croyances. Ainsi, cette croyance ne figurera pas dans la sélection finale, puisque l'on vise la parcimonie.

L'analyse individuelle de la croyance #6 (« Nature générale de l'être humain ») s'est aussi soldée par le besoin de conduire un examen global. En effet, les participants ont questionné les propositions de cette croyance car elles ne leur semblaient pas fidèles à la pratique. Sur la base de leur expérience, ils estimaient que faire trop confiance ou trop contrôler ses employés n'avait qu'une faible incidence sur la variable dépendante. Pour ce faire, il semble nécessaire d'atteindre un équilibre entre ces deux manières de faire. De plus, la figure 4.1 montre que cette croyance détient le deuxième score global le plus élevé (57 points). Dans un souci de parcimonie et en tenant compte aussi de l'écart de points considérable par rapport aux autres croyances, elle n'est donc pas conservée pour la sélection finale.

En conclusion, à l'issue des analyses des données individuelles et globales, les décisions suivantes ont été prises :

- Une croyance a été retenue et sera incluse telle quelle dans la sélection finale :
    - Croyance #3 : Importance générale qu'a la sécurité de l'information dans l'organisation
- Deux croyances ont été fusionnées et la croyance qui en résulte sera incluse dans la sélection finale :
    - Croyance #1 : Responsabilité quant à la sécurité de l'information (non retenue pour la sélection finale)
    - Croyance #2 : Vision de l'organisation quant à la nature des défis en termes de sécurité de l'information (non retenue pour la sélection finale)
    - Leur esprit est fusionné dans la nouvelle croyance #A : Vision de l'organisation quant à la nature des défis et la gestion de la sécurité de l'information
- Quatre croyances ne sont pas retenues pour la sélection finale :
    - Croyance #4 : Auto-efficacité organisationnelle face aux menaces
    - Croyance #5 : Responsabilité morale de protéger l'information
    - Croyance #6 : Nature générale de l'être humain
    - Croyance #7 : Le maillon faible en sécurité de l'information

4.2 Valeurs : résultats et analyses

Cette section fait l'état des résultats du deuxième exercice de priorisation, qui portait sur les dix valeurs susceptibles d'influencer la variable dépendante. Telle la section précédente, il sera premièrement question d'analyser les résultats à l'aide d'une analyse individuelle, où les classements et les propos des participants sont examinés dans l'optique de déterminer si la valeur est importante pour expliquer l'influence du contexte organisationnel sur la variable dépendante. Dans le cas où l'analyse individuelle n'a pas permis de prendre une décision quant à une valeur, une analyse globale sera conduite. Cette analyse globale consiste à comparer cette valeur à d'autres valeurs et sera exposée à la fin de cette section. Ces résultats sont également analysés afin de déterminer les valeurs qui figureront dans la sélection finale.

4.2.1 Valeurs : résultats et analyses individuelles

Cette sous-section présente les résultats recueillis lors des entrevues individuelles avec les professionnels en sécurité de l'information. Pour chaque valeur, la carte sur laquelle elle est inscrite, les classements et les commentaires des participants ainsi qu'une analyse des résultats seront exposés.

4.2.1.1 Valeur #1 : Bases générales sur lesquelles les décisions sont prises dans l'organisation

VALEUR #1

Valeur partagée dans l'organisation quant aux bases sur lesquelles les décisions doivent être prises au sein de l'organisation.

Plus l'organisation privilégie les bases quantitatives pour asseoir ses décisions (analyses quantitatives, métriques, benchmarking, etc.), plus élevées sont les chances qu'elle évaluera les aspects liés à la sécurité de l'information d'une manière globale et complète menant à la mise en place d'outils stimulant davantage les employés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si on tend à privilégier des décisions basées sur l'intuition et les émotions (« gut feelings »), plus élevées sont les chances que l'on négligera de conduire une évaluation rigoureuse des aspects liés à la sécurité de l'information, menant ainsi à l'absence d'outils favorisant la mise en œuvre de pratiques sécuritaires.

- **Résultats**

Par l'entremise des classements réalisés par les participants, cette valeur a obtenu entre un et dix points de la part des participants. De plus, aucun participant n'a écarté cette valeur de son

classement. Des commentaires sur cette valeur ont été colligés pour chacun des participants, sauf pour le participant #7 (dans ce dernier cas, l'absence de commentaires peut s'expliquer par une prise de notes incomplète ou par le silence du participant). Les classements, les points attribués et les commentaires émis relatifs à cette valeur figurent dans le tableau 4.16.

Tableau 4.16 : Résultats (classements, points et commentaires) obtenus pour la valeur #1

Participant	Classement de la valeur (sur 10)	Points attribués	Commentaires sur cette valeur
Participant #4	8	8	• « Mes lectures me portent de plus en plus à croire qu'on n'est pas bons pour faire de l'analyse de risques qualitative pour mesurer le risque par l'être humain sans avoir des chiffres concrets. Ça crée un biais sur comment on voit les situations. Donc, apporter des métriques concrètes là-dessus, ça peut être un énorme bénéfice. Si ça marche pour le domaine des finances, ça devrait marcher pour le monde de la sécurité. » *(à propos de la proposition « Quantitatif »)*
Participant #5	10	10	• « On peut travailler à avoir une belle culture de sécurité sachant que c'est un peu loin de la réalité, l'approche quantitative. Donc, on réussit quand même sans avoir cet élément-là. Je pense que ça peut peut-être avoir de l'influence. Mais moi, je n'ai jamais considéré cet élément-là comme un élément qui va influencer la culture. C'est plus les autres éléments qu'on a vus avant. » • « Ça, j'hésite un peu. En sécurité, prendre une approche qui est purement quantitative, c'est un vœu pieux. [Dans notre domaine, c'est] utopique parce qu'on n'a pas assez de données. Quand on arrive à une situation où on n'a pas assez de données, on ne peut plus se baser sur une analyse quantitative. Exemple, les compagnies d'assurance ont beaucoup de données et peuvent utiliser des données, donc une approche quantitative. Mais quand… Je ne sais pas… Une star qui veut faire assurer son petit doigt; il n'y a pas assez de données là-dessus. Donc, là, qu'est-ce qu'ils font? Ils créent un comité et ils se rencontrent et ensuite, ils jasent… Ils jasent… Donc, en fonction de certains faits d'actualité, l'expérience de chacun, les discussions, finalement, il y a un consensus. Donc c'est par consensus, consensus basé sur des opinions, des perceptions, etc. Donc, même les compagnies d'assurance, qui veulent assurer des petits doigts sont obligées de mettre un peu de côté l'analyse quantitative. Puis, en sécurité, il nous manque souvent de l'information. » *(à propos de la proposition « Quantitatif »)*

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.16 : Résultats (classements, points et commentaires) obtenus pour la valeur #1 (suite)

Participant	Classement de la valeur (sur 10)	Points attribués	Commentaires sur cette valeur
Participant #6	9	9	• « Je pense qu'effectivement, c'est un bon élément qui est important. » • « Le seul élément dont je ne suis pas certaine, c'est le dernier bout de l'énoncé qui dit qu'il y a un lien direct entre le fait d'utiliser une démarche quantitative, qui va également se répercuter sur la sécurité de l'information, qui va être analysée de manière quantitative et tout ça va faire en sorte qu'on va avoir des outils ou non… Je ne suis pas certaine que c'est exact. Je dis pas qu'on ne fait pas ça ici et là, mais je me dis qu'une entreprise peut faire une analyse qui est complètement subjective et se baser sur un gut feeling, mais quand même avoir le réflexe de mettre en place des outils. C'est comme le lien entre la manière que tu l'analyses et la qualité de tes outils. Je me dis peut-être qu'on ne va juste pas déployer les outils qui vont être efficaces parce qu'on n'a pas bien mesuré ce sur quoi on devait travailler. Donc, peut-être l'efficacité des outils sera moins bonne, mais ça ne fait pas en sorte que tu n'en auras pas d'outil. Je me dis qu'on peut juste prendre des mauvaises décisions d'affaires et investir dans les mauvais outils. […] C'est juste qu'ici on dit 'menant ainsi à l'absence d'outils'. Si on dit 'favorisant la mise en œuvre de pratiques sécuritaires'… C'est plus le volet pertinence. C'est peut-être un petit détail dans la manière que c'est formulé, mais il y a définitivement un lien, c'est certain. » *(à propos de la proposition « Quantitatif »)* • « Ça doit certainement avoir un impact, mais j'ai l'impression que ça a moins d'impact que l'éthique, que l'engagement de l'employé, qui pour moi sont comme vraiment directement en lien avec [la variable dépendante]. » *(lien avec la valeur #3 et #7)*
Participant #7	9	9	• *(Aucun commentaire)*
Participant #8	9	9	• « C'est vrai. Ce n'est pas évident à trouver [des données] pour des bases quantitatives. En sécurité, c'est vrai effectivement [par exemple] quand on se compare aux autres, quand on évalue la performance de nos processus pour mieux aligner nos décisions, dépendamment du niveau de maturité de l'entreprise, évidemment. J'ai vu des entreprises qui étaient très peu matures et les données quantitatives étaient dures à mesurer quand tu n'avais même pas de processus en place. Donc, dans ce cas, tu n'as pas le choix d'aller un peu avec ton gut feeling. Mais, oui, tout à fait [d'accord]. C'est un peu plus difficile à trouver. »

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.16 : Résultats (classements, points et commentaires) obtenus pour la valeur #1 (suite)

Participant	Classement de la valeur (sur 10)	Points attribués	Commentaires sur cette valeur
Participant #9	3	3	• « Alors, je le mettrais en deuxième lieu, celle-là… Pourquoi? Parce que, pour prendre des décisions sur l'importance de développer les connaissances, il faut que tu te réfères à un benchmark, tout ça, les meilleures pratiques, ce qui se fait ailleurs, etc. Donc, si tu as une approche structurée, tu vas pouvoir former et informer tes employés correctement. » • [ndlr : La chercheure lui demande les métriques qu'il utilise] « Il y a les Gartner de ce monde, il y a plein de sites de statistiques sur les bonnes pratiques, etc. Une organisation pourrait faire aussi un audit de sécurité sur ses propres pratiques et là, voir les faiblesses, les places où il y a matière à amélioration. En fonction de ces résultats-là, elle pourrait dire 'Ah, mais c'est bien, on va former le personnel technique à gérer mieux les coupe-feu. On va former le personnel RH à faire des enquêtes de sécurité sur les employés qu'ils embauchent préalablement, etc.'. Alors, c'est un peu ça. »
Participant #10	4	4	• « Hum… Également important et je le mettrais même en deuxième. [ndlr : après valeur #3 et avant valeur #2] Pourquoi? Dans le cadre de mon expérience et puis par le prisme des interactions avec mes clients… On a tendance, autant moi que mes clients, à être très cartésiens. Donc, si je ne comprends pas pourquoi tu me demandes de faire quelque chose, je suis moins porté à le faire que si tu me donnes des arguments. Je réponds très bien aux arguments… Au raisonnement, tout court. Donc, si tu me dis 'Écoute, il faut que tu fasses telle ou telle affaire en sécurité parce que voici ce que les chiffres nous disent', ok, je vais cliquer là-dessus et je vais l'appliquer. Et ça, je suis capable de l'absorber même si ça n'a pas été planifié. Si tu me donnes des arguments, je suis plus susceptible de faire ce que [tu me demandes] et [même chose pour] mes clients. » • [ndlr : La chercheure lui demande les métriques qu'il utilise] « Dépendamment du domaine. Tu regardes par application, par ligne d'affaires, par comportement des usagers… Par exemple, il y a 25 000 courriels de phishing qui sont rentrés dans l'organisation le mois passé. Est-ce le temps de dépenser un petit peu pour faire une campagne de sensibilisation pour les employés pour leur dire qu'il ne faut pas cliquer sur ça? Oui, s'il y en a eu 25 000 et qu'il y a eu des clics qui ont été faits là-dessus… C'est la manière que j'utilise pour justifier auprès de mes clients des décisions d'investissement et de dépenser leur argent dans un domaine plutôt que dans l'autre. »
Participant #11	6	6	• « L'analyse de risque basée sur l'intuition, ça fonctionne tout le temps, ça! C'est clair! Toutes les méthodologies d'analyse de risque sont terre à terre, mais c'est ardu, c'est méthodique. Si ce n'est pas méthodique, c'est rien que des émotions. C'est rien que des impressions… Tu espères que ce ne sera pas complètement subjectif… » *(à propos de la proposition « Qualitatif »)*

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.16 : Résultats (classements, points et commentaires) obtenus pour la valeur #1 (suite et fin)

Participant	Classement de la valeur (sur 10)	Points attribués	Commentaires sur cette valeur
Participant #12	2	2	• « [Pour cette valeur], je pense que le morceau le plus important, ce n'est pas l'analyse quantitative, les métriques. Le morceau le plus important de la décision, c'est la gouvernance [de la haute direction]. Et s'ils ont pris ça par gut feeling, ce n'est pas important. Ce n'est pas génial, mais ce n'est pas important. Parce que l'important, c'est qu'il y a de la gouvernance, il y a une direction. Le CISO, sa job, c'est d'établir les règles de gouvernance… Oui, qui peuvent être bâties sur plein d'affaires, mais une fois que tu as mis en place la gouvernance, le reste des décisions peuvent s'appuyer sur ce que tu veux. Mais je me mets à la place d'un C.A., je ne pense pas qu'il va faire du benchmarking, mais il va quand même établir la gouvernance. Puis ça fait que cette valeur #1 peut être mesurée à peu près à tous les niveaux… Le directeur du groupe, le VP, le CIO, le board. » • « La gouvernance, je le vois comme un élément qui est pas des métriques, pas du benchmarking. […] La gouvernance de l'entreprise en matière de sécurité de l'information plus des bases quantitatives pour asseoir des décisions, c'est extrêmement important. » • « Deuxième [valeur la plus importante pour moi], c'est 'les bases sur lesquelles les décisions doivent être prises au sein de l'organisation'. Oui, il y a le volet quantitatif, mais il y a aussi le volet gouvernance. Je l'ai étendue votre définition, fait qu'il y a des bases quantitatives, mais des fois, c'est des bases de valeurs. C'est quoi les valeurs d'entreprise et c'est quoi la gouvernance d'entreprise? Les bases quantitatives reflètent aussi pour moi l'engagement… C'est un reflet de l'engagement de l'entreprise… »
Participant #13	1	1	• Il pense que c'est vrai, mais il y a très peu d'approches quantitatives en sécurité. Par contre, ce qu'on peut faire, c'est du qualitatif bien expliqué, bien structuré qui peut être utilisé comme des métriques.
Participant #14	6	6	• Il ne pense pas que les bases analytiques encouragent un comportement sécuritaire. Selon son expérience, ce n'est pas toujours nécessaire de faire une analyse complète. En réalité, une bonne décision pour un comportement sécuritaire est un mélange d'analytique et d'intuition.
	Score global =	**67 pts**	

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels présentés dans le tableau 4.16 permettent d'arriver aux fréquences présentées dans le tableau 4.17. Ce tableau montre que quatre participants ont placé cette valeur dans le premier tiers, deux participants l'ont fait au tiers du milieu et cinq autres l'ont classée dans le dernier tiers du classement.

Tableau 4.17 : Tableau des fréquences pour la valeur #1

	Position	Fréquence	Total
Premier tiers	1	1	4
	2	1	
	3	1	
	4	1	
Tiers du milieu	5	-	2
	6	2	
Dernier tiers	7	-	5
	8	1	
	9	3	
	10	1	

- **Analyse des résultats obtenus pour cette valeur**

Cette valeur a été placée dans le tiers du milieu et dans le dernier tiers du classement par la plupart des participants (#4, #5, #6, #7, #8, #11, #14). Ce classement s'est d'ailleurs soldé par un score global relativement élevé de 67 points (pour un score global possible variant entre 11 et 121 points). Même si la plupart des commentaires reçus étaient positifs (#4, #5, #6, #8, #9, #10, #11, #12, #13) quant à l'influence de cette valeur sur la variable dépendante, ceux-ci remettaient également en cause les propositions liées à cette valeur. Il s'avère donc pertinent d'examiner les propos des participants afin de comprendre pourquoi cette valeur a obtenu un bilan aussi mitigé. Seul le participant #14 a critiqué ouvertement l'importance de cette valeur. En ce qui concerne le participant, son classement était révélateur de ce qu'il pensait de cette valeur. En effet, elle lui semblait d'importance moindre étant donné qu'il l'a placée dans le dernier tiers de son classement.

D'une part, les participants #4, #5, #8, et #13 ont dénoncé le fait qu'il était ardu d'identifier des bases quantitatives pertinentes en sécurité de l'information, afin de conduire leurs analyses. Les participants #4 et #5 ont d'ailleurs souligné que cela était une faiblesse de leur domaine. Le participant #8 a également ajouté que cette faiblesse touchait particulièrement les organisations dont les processus d'affaires en sécurité de l'information étaient peu matures. On

pourrait donc croire que cette faiblesse serait liée au niveau de maturité de leurs processus d'affaires en sécurité de l'information.

Bien que le participant #13 ait relevé cette faiblesse dans les analyses en sécurité de l'information, il a néanmoins trouvé un moyen de pallier ce problème, à l'instar des participants #11 et #14. En effet, faute de bases quantitatives solides, les participants #11, #13 et #14 combinent donc des bases quantitatives et des bases qualitatives pour conduire leurs analyses en sécurité de l'information.

Seul le participant #10 semblait convaincu de la possibilité de conduire une analyse en sécurité de l'information qui s'appuie sur des bases quantitatives. Cela peut s'expliquer par le domaine dans lequel il exerce sa profession car il a déclaré que ses clients et lui avaient « tendance à être très cartésiens ». Par ailleurs, lorsqu'il a été demandé aux participants quels étaient les métriques utilisées dans leur analyse en sécurité de l'information, le participant #10 était le seul à donner une réponse concrète, à savoir le taux de clics sur les liens malveillants des courriels de hameçonnage. Néanmoins, ce type de données pourrait seulement être collecté par des organisations dont les processus d'affaires en sécurité de l'information sont matures, si l'on se fie aux dires du participant #8.

Seul le participant #6 a relevé des liens entre cette valeur et d'autres valeurs. En effet, il a déclaré que cette valeur influencerait la variable dépendante mais qu'elle est d'importance moindre par rapport aux valeurs #3 (« Prédispositions éthiques de l'organisation ») ou #7 (« Force du réseau au sein de l'organisation »). Ce commentaire pourrait être expliqué par le fait que l'éthique et la collaboration auraient une influence directe sur la variable dépendante, contrairement à une prise de décision par la haute direction qui exercerait une influence indirecte sur la variable dépendante. Par exemple, la haute direction peut décider d'investir dans un nouveau programme de sensibilisation que les employés devront suivre et qui pourrait, ainsi, les inciter à agir de manière plus sécuritaire.

Ainsi, en prenant en compte les classements et les propos des participants, il est possible d'affirmer que cette valeur est d'importance moindre pour influencer la variable dépendante. D'une part, son impact serait moindre par rapport à certaines des autres valeurs présentées aux participants. D'autre part, la pratique liée à cette valeur (à savoir l'analyse qualitative ou quantitative) est difficilement applicable en sécurité de l'information car, à ce stade, la plupart des organisations ne sont pas outillées pour obtenir des données concrètes qui pourraient contribuer à une prise de décisions basées sur des fondements quantitatifs solides. Par conséquent, cette valeur n'est pas retenue pour la sélection finale.

4.2.1.2 Valeur #2 : Horizon temporel habituel de la planification dans l'organisation

VALEUR #2

Valeur partagée dans l'organisation qui reflète les habitudes de planification de l'organisation.

Plus l'organisation a l'habitude de planifier à long terme, plus élevées sont les chances qu'elle le fera aussi en sécurité de l'information, ce qui l'amènera à faire les investissements requis afin de favoriser la mise en œuvre de pratiques sécuritaires. À l'opposé, si le focus de l'organisation est surtout à court terme, moins élevées sont les chances que la sécurité de l'information fera l'objet des investissements nécessaires à la mise en œuvre de pratiques sécuritaires.

- **Résultats**

Par l'entremise des classements réalisés par les participants, cette valeur a obtenu entre un et neuf points de la part des participants. De plus, aucun participant n'a écarté cette valeur de son classement. La majorité des participants a d'autant plus émis des commentaires par rapport à cette valeur. Des commentaires sur cette valeur ont été colligés pour chacun des participants, sauf pour les participants #7 (dans ce cas-ci, l'absence de commentaires peut s'expliquer par une prise de notes incomplète ou par le silence de ce dernier) et #9 (dans ce dernier cas, l'absence de commentaires peut s'expliquer par le silence du participant). Les classements, les points attribués et les commentaires émis relatifs à cette valeur figurent dans le tableau 4.18.

Tableau 4.18 : Résultats (classements, points et commentaires) obtenus pour la valeur #2

Participant	Classement de la valeur (sur 10)	Points attribués	Commentaires sur cette valeur
Participant #4	4	4	• « Oui, la planification à long terme. Je ne pourrais pas être gestionnaire aujourd'hui et ne pas valoriser la planification à long terme. Ceci étant dit, quand on est dans un domaine où il y a beaucoup de perturbateurs, ça devient un défi, vite, de garder le cap à long terme, s'assurer qu'on va à la bonne place. Mais je pense que c'est un élément essentiel pour l'atteindre. Savoir quel est notre objectif et s'assurer qu'on travaille d'une manière continue sur une longue période de temps, je pense que c'est essentiel. […] Oui, absolument… Et ça fait beaucoup moins réactif… Mais encore, là, il ne faut pas tomber dans le piège qu'il arrive un incident et qu'on veut tout réévaluer la planification à long terme à cause d'un incident. »
Participant #5	9	9	• « Celle-là, je le vois moins parce qu'une organisation peut avoir une volonté de planifier à long terme en fonction de son core business, mais sans nécessairement avoir un lien avec la sécurité. Je vois [la sécurité] plus comme étant une propriété de quelque chose et non pas un poste budget à atteindre. À part si tu veux avoir des objets très spécifiques… Par exemple, un cadre de gouvernance et autres. Mais la sécurité, c'est quelque chose de tous les jours. Donc, même si tu as une stratégie [d'affaires] quinquennale, et que tu es habitué à présenter toujours une vision pour les cinq prochaines années, oui, c'est quelque chose de bien pour la business, mais je vois moins de lien avec la sécurité. Il faut avoir une approche stratégique en sécurité, ça, c'est clair. Mais est-ce que ça a un lien avec le fait que tu ne cliqueras pas sur un courriel ou que tu vas raisonner avant de poser une action…? Ça va avoir un lien plus au niveau de la conformité, donc prévoir les coups lorsque telle situation va arriver, qu'on soit prêt. […] Mais est-ce que ça, ça va influencer l'ensemble des employés? Pour les employés, je pense que c'est plus [important] de leur dire 'La sécurité, c'est important'. »
Participant #6	1	1	• « Oui, effectivement, la planification, à savoir si c'est planifié à long terme, ou pas, ça va influencer sur la mise en œuvre des pratiques sécuritaires. Oui, on peut être en mode pompier et on va ajouter des trucs pour boucher des trous, mais on ne travaillera pas sur les comportements puis sur les pratiques des employés.Là, ça dépend c'est quoi le long terme dans le sens que planifier sur quatre-cinq ans, c'est plus tellement [important]. Ça change tellement que le long terme est rendu peut-être un peu plus court qu'il y a quelques années. Trois ans, maximum. » *(à propos de la proposition « Planification sur le long terme »)*
Participant #7	6	6	• *(Aucun commentaire)*
Participant #8	6	6	• « Oui, effective ment. Parce qu'on ne voit pas toujours à long terme, on va aller chercher le gain rapide. On va aller chercher l'argent rapide, mais on ne mettra pas d'argent en sécurité. La sécurité, ce n'est pas une fin en soi; la sécurité, c'est un processus continu. »

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.18 : Résultats (classements, points et commentaires) obtenus pour la valeur #2 (suite et fin)

Participant	Classement de la valeur (sur 10)	Points attribués	Commentaires sur cette valeur
Participant #9	2	2	• *(Aucun commentaire)*
Participant #10	5	5	• « Également très important, mais je le mettrais en deuxième. » [ndlr : après la valeur #3]
Participant #11	8	8	• « C'est stratégique et tactique. Tactique, tu réponds au court terme. Puis tu as besoin de répondre au court terme : 'Aie, notre serveur est down!'. Regarde, fais quelque chose! On a des processus d'affaires, l'équipe de reprise des activités, l'équipe de surveillance, jusqu'à éventuellement un business continuity plan, c'est tout un continuum ça. Tout à fait. » • « Si tu planifies juste le tactique, tu réponds aux feux. Si les employés, l'ensemble des gens voient qu'on est toujours en train de se faire tasser et de se faire bouger par ce qui se passe dans l'industrie, on voit qu'on n'est pas super résilient et qu'on n'est pas en avant et que ce n'est pas nous autres qui lead le programme. C'est exactement l'inverse de ce qui se passe ici [ndlr : il parle de son organisation]. Donc, c'est sûr qu'en termes de planification, si tu montres que tu te plantes et que tu te fais tasser, les valeurs en souffrent… »
Participant #12	1	1	• « La valeur la plus importante, pour moi, c'est la valeur #2… Les habitudes de planification. Si c'est ad hoc… La sécurité, ça ne peut pas être ad hoc. » • « Pour la valeur #2… Pour moi, le quantitatif pour asseoir des décisions, c'est quantitatif plus en fonction de la gouvernance ou la politique en place. »
Participant #13	2	2	• « C'est tellement vrai. »
Participant #14	6	6	• Cette valeur affecte surtout l'intelligence parce que l'éducation et « devenir intelligent » prennent du temps.
Score global = 50 pts			

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels présentés dans le tableau 4.18 permettent d'arriver aux fréquences présentées dans le tableau 4.19. Ce tableau montre que cinq participants ont placé cette valeur dans le premier tiers, quatre participants l'ont fait au tiers du milieu et deux autres l'ont classée dans le dernier tiers du classement.

Tableau 4.19 : Tableau des fréquences pour la valeur #2

	Position	Fréquence	Total
Premier tiers	1	2	5
	2	2	
	3	-	
	4	1	
Tiers du milieu	5	1	4
	6	3	
Dernier tiers	7	-	2
	8	1	
	9	1	
	10	-	

- **Analyse des résultats obtenus pour cette valeur**

La majorité des participants a placé cette valeur dans le premier tiers (#4, #6, #9, #12 et #13) et dans le tiers du milieu (#7, #8, #10 et #14) du classement, ce qui lui a valu un score global relativement faible de 50 points (pour un score global variant de 11 à 121 points). Les commentaires des participants étaient à l'image de ce classement car ils étaient pour la plupart positifs (#4, #6, #8, #10, #12, #13 et #14) et soulignaient l'importante influence que cette valeur exerce sur la variable dépendante. Pour ce qui est des participants #7 et #9, leur classement montre qu'ils l'ont respectivement classée dans le premier tiers et dans le tiers du milieu de leur classement.

La première proposition liée à cette valeur (« Plus l'organisation a l'habitude de planifier à long terme, plus élevées sont les chances qu'elle le fera aussi en sécurité de l'information, ce qui l'amènera à faire les investissements requis afin de favoriser la mise en œuvre de pratiques sécuritaires ») a soulevé de multiples réactions. Selon les participants #4, #6, #8 et #14, la planification à long terme serait essentielle pour influencer la mise en œuvre de pratiques sécuritaires par les employés étant donné que la sécurité de l'information est un processus continu (participant #8) et requiert du temps pour influencer les employés à mettre en œuvre des pratiques sécuritaires (participant #14). Par contre, les participants #4 et #6 ont mentionné qu'en sécurité de l'information, la planification à court terme était également importante afin de répondre aux évènements perturbateurs (par exemple, une brèche de données ou une cyber-

attaque). Ainsi, ce serait l'alliage d'une planification à long terme et d'une planification à court terme qui influencerait la variable dépendante de manière significative.

Les participants #5 et #11 ont placé cette valeur dans le dernier tiers du classement. Néanmoins, le classement et les propos émis par ces participants semblaient sans conséquence sur le résultat final de cette analyse. Premièrement, le participant #5 semblait confondre la responsabilité de réaliser une pratique avec les effets d'une valeur sur l'organisation ou sur la variable dépendante. Il avait mentionné que la planification relevait plutôt du core business que de la sécurité de l'information. Deuxièmement, le participant #11 s'est principalement prononcé sur la planification à court terme. Il a notamment mentionné l'inefficacité de conduire une planification à court terme en sécurité de l'information et semble avoir classé cette valeur en fonction de l'inefficacité de la planification à court terme, et non par rapport à l'influence de cette valeur sur la variable dépendante.

En somme, l'analyse des classements et des commentaires des participants a mis en exergue l'importance de cette valeur pour influencer la variable dépendante. Ainsi, elle est retenue pour la sélection finale.

4.2.1.3 Valeur #3 : Prédispositions éthiques dans l'organisation

VALEUR #3

Valeur partagée dans l'organisation quant à la place de l'éthique dans l'organisation.

Plus l'organisation adopte une position éthique dans la conduite générale de ses affaires, plus élevées sont les chances qu'elle le fera aussi pour protéger les informations, menant ainsi à la mise en œuvre de pratiques sécuritaires. À l'opposé, si l'éthique n'est pas une valeur importante dans l'organisation, cela affectera négativement la mise en œuvre de pratiques peu sécuritaires.

Résultats

Par l'entremise des classements réalisés par les participants, cette valeur a obtenu entre un et dix points de la part des participants. De plus, aucun participant n'a écarté cette valeur de son classement. Des commentaires sur cette valeur ont été colligés pour chacun des participants, sauf pour le participant #7 (dans ce dernier cas, l'absence de commentaires peut s'expliquer par une prise de notes incomplète ou par le silence du participant). Les classements, les points attribués et les commentaires émis relatifs à cette valeur figurent dans le tableau 4.20.

Tableau 4.20 : Résultats (classements, points et commentaires) obtenus pour la valeur #3

Participant	Classement de la valeur (sur 10)	Points attribués	Commentaires sur cette valeur
Participant #4	3	3	• « Absolument. Oui. Je pense que l'éthique est essentielle, oui. »
Participant #5	3	3	• « Oui, je trouve qu'il y a une importance au niveau de l'éthique. […] Dans [notre contexte], il y a plusieurs volets liés à l'éthique […]. Ça, ça montre une certaine importance. […] Donc, ça montre une certaine prise de conscience et une volonté au-delà de simplement d'être conforme aux lois. Pour les organismes privés, on peut quand même avoir des valeurs éthiques. Puis ça permet de dire 'On vient en fait se positionner un petit peu plus loin que seulement la loi'. Parce qu'on sait que l'éthique vient remplir des éléments au-delà de la loi, qui ne sont pas clairement adressés. Donc, là, nous, on va rendre ça encore plus clair. Donc, c'est sûr que ça montre une volonté supérieure au cadre législatif des ententes contractuelles qu'on pourrait avoir. »
Participant #6	1	1	• « Je pense que c'est l'un des premiers. » • « L'éthique, c'est vraiment quelque chose qui est comme en filigrane de l'ensemble du reste, de tous les gestes. C'est vraiment comme un pilier qui va vraiment influencer beaucoup les comportements et les décisions. C'est toujours un élément qui est présent. Il est comme dans à peu près tout ce qu'on fait. L'élément éthique va être un élément présent qui va nous influencer directement. Pour moi, c'est vraiment la valeur. Définitivement, en termes de sécurité, c'est un pilier. »
Participant #7	4	4	• *(Aucun commentaire)*
Participant #8	7	7	• « Tout à fait. Absolument. Si l'éthique est importante dans l'entreprise, effectivement, ça va aider pour mettre en place les pratiques sécuritaires… »
Participant #9	1	1	• « Tout à l'heure, on parlait de la haute direction qui supporte les principes de sécurité à mettre en place… Pour moi, l'éthique, c'est la même chose. Si l'organisation a l'éthique d'entreprise comme étant extrêmement importante, c'est sûr que ça va rehausser les agissements du personnel. […] Alors je vois [cette valeur] comme étant très importante. »
Participant #10	1	1	• « Absolument, oui. »
Participant #11	4	4	• « C'est très visible quand la valeur de l'éthique n'est pas là; quand elle n'est pas identifiée clairement, il a de bonnes chances que l'entreprise agisse éthiquement quand même. De la même façon que [la croyance 3] l'importance de la sécurité, un manquement à l'éthique serait tellement porté à causer un impact sur la réputation que c'est impensable. Je pense que si tu es capable de cerner l'éthique plus précisément pour la job de chacun, tu as probablement plus de maturité dans l'identification de tes processus d'affaires. Donc, j'ai l'impression que ça a rapport avec le niveau de la maturité organisationnelle. »

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.20 : Résultats (classements, points et commentaires) obtenus pour la valeur #3 (suite et fin)

Participant	Classement de la valeur (sur 10)	Points attribués	Commentaires sur cette valeur
Participant #12	7	7	• « La septième valeur en ordre d'importance, c'est la valeur #3. L'éthique, c'est super beau, c'est comme sauver le monde et la paix dans le monde. C'est vraiment génial. […] Les gens qui ont la maturité de mettre l'éthique, planifient déjà, prennent déjà des décisions sur des bases rationnelles; ils sont déjà sensibles à former leurs employés; il y a déjà des politiques qui sont relativement respectées. Donc, pour moi, l'éthique, c'est la somme du reste, mais ce n'est pas en focussant sur l'éthique qu'on va régler les problèmes. »
Participant #13	9	9	• Ce participant aimerait recevoir la définition que l'on donne à ce qu'est l'éthique parce que, selon lui, tout le monde n'a pas la même définition de l'éthique. Pour lui, l'éthique est très variable comme notion (par rapport à une situation, un contexte politique ou économique).
Participant #14	10	10	• Le participant croit que l'impact de l'éthique sur le comportement sécuritaire des employés est très faible. Selon lui, les employés ne font pas de lien entre l'éthique et les comportements sécuritaires.
	Score global =	**50 pts**	

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels présentés dans leur tableau 4.20 permettent d'arriver aux fréquences présentées dans le tableau 4.21. Ce tableau montre que sept participants ont placé cette valeur dans le premier tiers et quatre autres l'ont classée dans le dernier tiers du classement.

Tableau 4.21 : Tableau des fréquences pour la valeur #3

	Position	Fréquence	Total
Premier tiers	1	3	7
	2	-	
	3	2	
	4	2	
Tiers du milieu	5	-	-
	6	-	
Dernier tiers	7	2	4
	8	-	
	9	1	
	10	1	

- **Analyse des résultats obtenus pour cette valeur**

La majorité des participants (#4, #5, #6, #7, #9, #10 et #11) a placé cette valeur dans le premier tiers du classement, ce qui lui a valu un score global relativement faible de 50 points (pour un score global variant de 11 à 121 points). Les propos de ces participants ainsi que du participant #8 (qui l'a placée dans le dernier tiers) indiquaient que cette valeur influençait la variable dépendante. , Pour ce qui est du participant #7, le fait qu'il l'ait placée dans le premier tiers de son classement est signe qu'elle lui semblait être une source d'influence.

Afin de découvrir la raison pour laquelle les participants #8, #12, #13 et #14 ont placé cette valeur dans le dernier tiers du classement, il est utile d'analyser leurs propos. Premièrement, le participant #8 a émis des propos contradictoires au rang qu'il a donné à cette valeur dans son classement. Bien qu'il l'ait placée en septième position, il a pourtant affirmé qu'elle était importante. Il semblerait donc que, malgré l'importance qu'il lui accorde, les autres valeurs qui lui ont été exposées lui semblaient davantage importantes. En ce qui concernait le participant #12, il n'a pas questionné l'importance de cette valeur, mais en a plutôt commenté les impacts sur d'autres valeurs. De ce fait, ses propos et son classement laissaient entendre qu'elle était fondamentale, mais qu'elle serait moins influente que les autres valeurs qui lui ont été présentées. Pour ce qui du classement effectué par le participant #13, il semble être expliqué par le fait qu'il ait remis en cause la définition de cette valeur. En effet, même avec la définition proposée, il semblait avoir de la difficulté à se faire une idée précise de ce qu'est l'éthique.

Cela a semblé affecter son jugement et, par conséquent, son classement. Enfin, le participant #14 est le seul à avoir déclaré que cette valeur n'avait aucune influence sur la variable dépendante. Les informations collectées ne permettaient pas de mieux en comprendre la raison.

Au total, l'analyse des classements et des propos des participants laisse supposer que cette valeur serait susceptible d'exercer une influence sur la variable dépendante. Même si elle semble d'importance moindre comparée à certaines des autres valeurs présentées aux participants, elle n'a pas fait l'objet de critiques permettant de la rejeter. De ce fait, elle est retenue pour la sélection finale.

4.2.1.4 Valeur #4 : Attitude des employés envers la conformité

VALEUR #4

Valeur partagée dans l'organisation quant au respect des règles et des politiques définies au sein de l'organisation.

Plus il existe dans l'organisation une prédisposition à respecter les règles et les politiques définies, plus élevées sont les chances que les employés respecteront aussi les pratiques de sécurité de l'information définies. À l'opposé, s'il existe un mépris généralisé envers les règles et les politiques organisationnelles, les chances sont que la même chose se produira pour la mise en œuvre des pratiques de sécurité de l'information définies par l'entreprise.

- **Résultats**

Par l'entremise des classements réalisés par les participants, cette valeur a obtenu entre deux et sept points Des commentaires sur cette valeur ont été colligés pour chacun des participants, sauf pour le participant #7 (dans ce dernier cas, l'absence de commentaires peut s'expliquer par une prise de notes incomplète ou par le silence du participant). Les classements, les points attribués et les commentaires émis relatifs à cette valeur figurent dans le tableau 4.22.

Tableau 4.22 : Résultats (classements, points et commentaires) obtenus pour la valeur #4

Participant	Classement de la valeur (sur 10)	Points attribués	Commentaires sur cette valeur
Participant #4	2	2	• « Oui, absolument. »
Participant #5	7	7	• « Moi, je dirais que oui. Oui, ça a une influence. Parce que tu peux mettre beaucoup de règles, c'est bien beau, tu vas respecter les règles, mais est-ce que ça va te donner un meilleur jugement? Je ne suis pas sûr parce que, tantôt, tu me parlais du jugement et de gouvernance. Donc, au niveau gouvernance, ça va aider à respecter les obligations. C'est clair que ça va aider la conformité. »
Participant #6	6	6	• « Ça aussi [c'est important]. »
Participant #7	3	3	• *(Aucun commentaire)*
Participant #8	4	4	• « Effectivement, ça part de là. On ne peut pas dire aux gens de respecter les politiques qui n'existent pas. On avait ça comme problème. Il y avait peu de politiques. On avait une politique de la sécurité qui, je pense, datait de 2007 et n'avait jamais été révisée. Il a fallu remettre ça à jour l'année dernière. »
Participant #9	4	4	• « Absolument [d'accord quant à l'importance de cette valeur sur la variable dépendante]. » • « Si on a des références et on développe des politiques et que les gens respectent ces politiques sans savoir trop pourquoi, au moins, je m'assure un certain niveau de sécurité en fonction de ces politiques-là. Mais si j'ai des politiques et, en plus, les gens savent pourquoi, ça va juste s'améliorer. Et si les gens respectent les politiques et savent pourquoi et travaillent ensemble, ça va être parfait. » *(à propos de la proposition « Respect des règles »)* • « Et à l'inverse, si les gens travaillent ensemble et ne savent pas pourquoi et ne respectent pas les politiques, ça marchera pas. Ils peuvent travailler ensemble à ne pas respecter les politiques… Il faut qu'ils soient informés. » *(à propos de la proposition « Mépris des règles »)*
Participant #10	3	3	• « Oui… Fort important. Très important. »
Participant #11	5	5	• « S'il n'y a pas [cette valeur] et l'imputabilité, [à quoi servent] les huit autres [valeurs]? » *(lien avec la valeur #10)*
Participant #12	5	5	• « Même si les règles sont simples ou complexes […], si elles ne sont pas respectées, ça devient un élément de mesure facile, d'une part, et un élément qui est plus important que les autres qui est beaucoup plus lié, aux valeurs soft d'une entreprise. Celui-là, il se mesure et ça peut être une activité en soi : comprendre les politiques qui ne sont pas respectées. Si les politiques ne sont pas respectées, c'est qu'il a une raison. Je pose l'hypothèse que, par défaut, les employés sont généralement bien intentionnés dans leur entreprise; peut-être pas super motivés, mais au moins, bien intentionnés… La majorité l'est. »
Participant #13	6	6	• Pour qu'il y ait mépris généralisé, il faut que ça vienne d'en haut, de la haute direction. S'il y a des comportements qui se font et qui sont tolérés par l'organisation, ça va se gangréner au reste de l'organisation.
Participant #14	4	4	• Cette valeur influence surtout la composante 'conformité'. Je ne vois pas l'impact sur l'intelligence; en tout cas, pas aussi fort que sur la conformité.
	Score global =	**49 pts**	

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels présentés dans le tableau 4.22 permettent d'arriver aux fréquences présentées dans le tableau 4.23. Ce tableau montre que six participants ont placé cette valeur dans le premier tiers, quatre participants l'ont fait au tiers du milieu et un autre l'a classée dans le dernier tiers du classement.

Tableau 4.23 : Tableau des fréquences pour la valeur #4

	Position	Fréquence	Total
Premier tiers	1	-	6
	2	1	
	3	2	
	4	3	
Tiers du milieu	5	2	4
	6	2	
Dernier tiers	7	1	1
	8	-	
	9	-	
	10	-	

- **Analyse des résultats obtenus pour cette valeur**

La majorité des participants a placé cette valeur dans le premier tiers du classement (#4, #7, #8, #9, #10 et #14) et dans le tiers du milieu (#6, #11, #12 et #13) du classement, ce qui lui a valu un score global relativement faible de 49 points (pour un score global variant de 11 à 121 points). Les commentaires émis par les participants sont à l'image de ces classements étant donné qu'ils étaient principalement positifs (#4, #5, #6, #8, #9, #10, #11, #12, #13, #14) et appuyaient l'importance de cette valeur comme source d'influence sur la variable dépendante. En ce qui concerne le participant #7, le fait qu'il ait placé cette valeur dans le premier tiers de son classement indique qu'elle lui semblait importante.

Bien que le participant #5 a affirmé que cette valeur pourrait influencer la variable dépendante, il était le seul à l'avoir placée dans le dernier tiers du classement. De concert avec le participant #14, il a stipulé que cette valeur n'exercerait pas d'influence sur la composante « Intelligence » de la variable dépendante. Selon lui, le simple fait de respecter des règles ne développerait pas le jugement des employés. Bien que son commentaire soit plausible, l'étude, à ce stade-ci de développement de connaissances, il ne cherche pas à déterminer quelle composante de la variable dépendante est influencée par cette valeur. De plus, si l'on se fie aux propos des autres participants, cette valeur semble essentielle et constitue un premier pas vers la mise en œuvre de pratiques sécuritaires par les employés.

Le participant #11 a d'ailleurs déclaré qu'à l'instar de la valeur #10 (« Imputabilité »), cette valeur est importante. Sans elles, les huit autres valeurs qui lui ont été présentées lui sembleraient inutiles. Ce commentaire démontre donc le rôle central que jouerait cette valeur pour influencer la variable dépendante.

Étant donné que cette valeur ait principalement été placée dans le premier tiers et dans le tiers du milieu lors du classement et que son influence vis-à-vis de la variable dépendante n'a pas été remise en cause, elle est donc retenue pour la sélection finale.

4.2.1.5 Valeur #5 : Importance accordée au développement des ressources humaines

VALEUR #5

Valeur partagée dans l'organisation qui réfère à l'importance qu'a le développement des connaissances et des habiletés des employés dans l'organisation.

Plus il existe dans l'organisation une valorisation du développement des ressources humaines, plus élevées sont les chances que le même sentiment sera instauré par rapport à la sécurité de l'information et que les employés recevront tout le soutien nécessaire à la mise en œuvre de pratiques sécuritaires. À l'opposé, si le développement n'est pas valorisé, moins les employés mettront en œuvre des pratiques sécuritaires parce qu'ils seront livrés à eux-mêmes, sans soutien, ni formation.

- **Résultats**

Par l'entremise des classements réalisés par les participants, cette valeur a obtenu entre un et dix points de la part des participants. De plus, aucun participant n'a écarté cette valeur de son classement. Des commentaires sur cette valeur ont été colligés pour chacun des participants, sauf pour le participant #14 (dans ce dernier cas, l'absence de commentaires peut s'expliquer par une prise de notes incomplète ou par le silence du participant).Les classements, les points attribués et les commentaires émis relatifs à cette valeur figurent dans le tableau 4.24.

Tableau 4.24 : Résultats (classements, points et commentaires) obtenus pour la valeur #5

Participant	Classement de la valeur (sur 10)	Points attribués	Commentaires sur cette valeur
Participant #4	7	7	• « Très important, l'amélioration continue. On voit beaucoup de jeunes qui n'ont pas appris les principes de sécurité de l'information quand ils sortent de l'université… On pense [notamment] aux programmeurs. Si on n'utilise pas l'amélioration continue et l'éducation continue, l'esprit reste connecté à une époque et on n'a pas assez d'informations pour adresser les nouveaux problèmes. »
Participant #5	5	5	• « Je suis d'accord avec ça. Oui, effectivement. C'est d'ailleurs des obligations de la loi pour les organismes publics, d'avoir de la formation en sécurité et autres. Il y a la loi sur la gouvernance et la gestion des ressources informationnelles. De cette loi découle la politique de sécurité de l'information, la directive de sécurité de l'information gouvernementale [pour les organisations publiques et parapubliques]. [Tous les établissements de notre secteur] doivent respecter cette directive de sécurité ou politique de sécurité. Puis, il y a un point qui dit 'Les employés doivent être sensibilisés et formés sur une base annuelle en sécurité de l'information'. Donc, c'est clairement un élément important. »
Participant #6	5	5	• « Tout à fait. Oui. »
Participant #7	8	8	• Il pense qu'elle n'a pas un impact important parce que, même si c'est une valeur importante dans l'organisation de manière générale, ça n'a pas vraiment d'impact sur la sécurité de l'information. Pour la sécurité de l'information, il faut aller avec des moyens ciblés en fonction du problème que l'on veut corriger.
Participant #8	8	8	• « On est là pour les aider. Souvent, les gens ne se rendent pas compte que c'est des petits gestes très niaiseux. Ils pensent justement que ça prend des experts pour appliquer des mesures de sécurité. Bien souvent, les petits gestes, si on ne leur montre pas, si on n'est pas là [pour leur expliquer] quand ils viennent nous voir, ça ne marchera pas. Effectivement, [je suis d'accord]. »
Participant #9	6	6	• « Est-ce que je peux le considérer comme bonne pratique et moins bonne pratique? Parce que, si c'est une valeur au sein de l'organisation, le développement des connaissances est un requis, c'est sûr que ça va améliorer [la mise en œuvre de pratiques sécuritaires]. Si les valeurs de l'organisation ne sont pas adéquates, c'est sûr que ça n'améliorera pas [la mise en œuvre de pratiques sécuritaires]. Si les valeurs de l'organisation font qu'ils ont une réponse [en cas de problème] pour trouver un coupable, ça n'améliorera pas. C'est dans ce sens. C'est comme ça que je le classe pour l'instant. » *(lien avec la valeur #8)* • « J'ai mis la valeur #5 avant la valeur #7, parce que je préfère avoir des gens bien informés qui ne collaborent pas que des gens qui collaborent, mais qui ne savent pas de quoi ils parlent. » *(lien avec la valeur #7)*

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.24 : Résultats (classements, points et commentaires) obtenus pour la valeur #5 (suite et fin)

Participant	Classement de la valeur (sur 10)	Points attribués	Commentaires sur cette valeur
Participant #10	6	6	• « Oui, c'est vrai. Où je mettrais ça? La formation… S'ils ne savent pas ce qu'est la bonne façon de faire, on ne peut pas leur exiger d'agir de la bonne façon, n'est-ce pas? Donc, c'est quand même important. Je le mettrais tout de suite après la [valeur sur la] planification. Parce qu'on doit planifier le road map des compétences et comment on veut développer nos employés. » *(lien avec la valeur #2)*
Participant #11	1	1	• « Oui. [Cette valeur, ça concerne plus] comment je me sens reconnu dans l'entreprise : valeurs partagées dans l'organisation qui ont de l'importance pour le développement des connaissances. Est-ce que je me sens reconnu comme étant une valeur que mon boss veut faire évoluer? »
Participant #12	3	3	• « Pour moi, le développement des connaissances [valeur #5] est un prérequis à la responsabilité [valeur #10], mais [est] intimement relié. 'Je te forme à devenir responsable et je m'attends donc que tu deviennes responsable'. Ce n'est pas 'Je te forme à être responsable et huit autres priorités et, après ça, j'espère que tu es responsable'. Donc, [ces valeurs] vont être une à côté de l'autre, mais #5 en premier et #10 par la suite. » *(lien avec la valeur #10)* • « Peu importe à quel point on met de l'effort, si les employés ne savent même pas ce qu'est la sécurité de l'information et ne peuvent même pas comprendre l'importance que ça a, donc s'ils ne sont pas formés par rapport au danger que ça représente, au risque et aux méthodes pour le gérer, ne serait-ce qu'un peu, [les autres valeurs] ne servent à rien. Si je regarde des valeurs qui viennent en dernier, un exemple… la valeur #7. La force du réseau intra-organisationnelle, ben un troupeau de moutons non formés, ça peut être pire. Donc, oui, ils ont une belle valeur interne, mais ils demeurent des poules pas de tête, ils n'ont aucune idée de ce qu'ils font. Ils n'ont aucune idée où ils s'en vont. » *(lien avec la valeur #7)* • « Même s'il y a de la pression externe, la formation et la connaissance sont plus importantes. Parce que, même s'il y a de la pression externe et les gens n'ont aucune idée quoi faire. Donc, la pression externe ne devient, pas inutile, mais elle est reléguée au second plan. » *(lien avec la valeur #9)*
Participant #13	10	10	• « Elle ne sera pas dans le top [du classement], c'est clair. » • Il est très déçu du rôle des RH dans la sécurité de l'information (dans les organisations où il a travaillé). C'est le leadership du gestionnaire ou la culture d'en haut qui va encourager le développement des employés. La fonction des RH est encore trop traditionnelle et se limite aux formulaires.
Participant #14	5	5	• *(Aucun commentaire)*
Score global = 64 pts			

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels présentés dans le tableau 4.24 permettent d'arriver aux fréquences présentées dans le tableau 4.25. Ce tableau montre que deux participants ont placé cette valeur dans le premier tiers, cinq participants l'ont fait au tiers du milieu et quatre autres l'ont classée dans le dernier tiers du classement.

Tableau 4.25 : Tableau des fréquences pour la valeur #5

	Position	Fréquence	Total
Premier tiers	1	1	2
	2	-	
	3	1	
	4	-	
Tiers du milieu	5	3	5
	6	2	
Dernier tiers	7	1	4
	8	2	
	9	-	
	10	1	

- **Analyse des résultats obtenus pour cette valeur**

La majorité des participants a placé cette valeur dans le tiers du milieu (#5, #6, #9, #10 et #14) et dans le dernier tiers (#4, #7, #8 et #13) du classement, ce qui lui a valu un score global relativement élevé de 64 points (pour un score global variant de 11 à 121 points). Curieusement, les propos de la plupart des participants l'ayant classée dans le tiers du milieu et dans le dernier tiers mettaient en avant l'importance de cette valeur par rapport à la variable dépendante.

Pour la plupart des participants, former et éduquer les employés de l'organisation quant à la sécurité de l'information est un requis. En effet, il est essentiel qu'ils prennent connaissance des gestes sécuritaires afin de se prémunir contre les menaces en sécurité de l'information. Malgré l'importance de l'influence de cette valeur sur la variable dépendante soulignée par les participants, plusieurs d'entre eux ont relevé le lien existant entre cette valeur et d'autres valeurs et ce sont ces liens qui semblent justifier le classement le plus faible de cette valeur. Par exemple, le participant #9 pensait que cette valeur était plus importante que la valeur #7 (« Force du réseau au sein de l'organisation »). Selon lui, il vaut mieux avoir des employés informés qui opèrent en silo que des employés non informés qui collaborent. Dans ce derniers cas, cela pourrait s'avérer nocif car ils pourraient mutuellement s'induire en erreur et, dans le pire des cas, causer des incidents de sécurité. Ce participant a également ajouté que cette valeur pourrait mener l'organisation à mettre en place des bonnes pratiques visant à outiller les employés dans leur mise en œuvre de pratiques sécuritaires, contrairement à la valeur #8

(« Réaction habituelle de l'organisation face aux problèmes »). Pour ce qui est du participant #10, il a déclaré qu'éduquer ses employés est important, mais il est avant tout essentiel de planifier les stratégies en sécurité de l'organisation (valeur #2 – « Horizon temporel habituel de la planification dans l'organisation »). Quant au participant #12, il a mentionné que cette valeur était un prérequis aux valeurs #7 (« Force du réseau au sein de l'organisation », #9 (« Réponse habituelle de l'organisation face aux pressions externes ») et #10 (« Imputabilité »). Effectivement, les employés doivent être éduqués, sans quoi la collaboration, le respect des pressions externes et l'imputabilité auront une influence minime sur la variable dépendante.

Seuls les participants #7 et #13 ont vraiment contesté l'importance de cette valeur. D'une part, le participant #7 a déclaré que cette valeur n'influencerait que très peu la variable dépendante. Selon lui, cette influence moindre est causée par les programmes de formation en sécurité de l'information qui sont encore trop larges, et qui ne permettent pas d'outiller les employés à corriger des problèmes spécifiques de sécurité. Par contre, cette critique semblait être sans conséquence car ses commentaires laissaient entendre que le participant n'a pas classé cette valeur par rapport à son influence sur la variable dépendante, mais plutôt en fonction de l'impact des programmes de formation actuels sur la variable dépendante. Pour le participant #13, cette valeur avait une influence moindre car, selon lui, le département des ressources humaines se limitait généralement à de la gestion administrative et n'encourageait pas le développement des employés, dans les organisations dans lesquelles il a opéré. Cette prise de position n'a pas affecté l'analyse car elle se basait essentiellement sur le rôle déficitaire que joue le département des ressources humaines dans le développement des employés et avait peu à voir avec le lien entre la valeur et la variable dépendante.

Cette analyse a mis en exergue l'importance de cette valeur en fonction de la variable dépendante. Les propos viennent contredire le classement, qui tendait vers le dernier tiers et qui pourrait être expliqué par la prévalence des autres valeurs par rapport à la variable dépendante. Il n'en demeure pas moins que cette valeur semble importante pour influencer les employés à mettre en œuvre des pratiques sécuritaires. Ainsi, cette valeur est retenue pour la sélection finale.

4.2.1.6 Valeur #6 : Attitude générale des employés face au changement

VALEUR #6

Valeur partagée dans l'organisation quant à la façon de réagir au changement organisationnel.

Plus on valorise l'ouverture au changement dans l'organisation, plus il sera facile de changer les pratiques organisationnelles afin que les employés mettent en œuvre des pratiques de plus en plus sécuritaires. À l'opposé, si on tend à résister au changement, les chances sont plus élevées que les changements engendrés par la mise en œuvre de pratiques de plus en plus sécuritaires seront difficiles à accepter.

- **Résultats**

Par l'entremise des classements réalisés par les participants, cette valeur a obtenu entre trois et dix points de la part des participants. De plus, aucun participant n'a écarté cette valeur de son classement. Des commentaires sur cette valeur ont été colligés pour chacun des participants, sauf pour le participant #14 (dans ce dernier cas, l'absence de commentaires peut s'expliquer par une prise de notes incomplète ou par le silence du participant). Les classements, les points attribués et les commentaires émis relatifs à cette valeur figurent dans le tableau 4.26.

Tableau 4.26 : Résultats (classements, points et commentaires) obtenus pour la valeur #6

Participant	Classement de la valeur (sur 10)	Points attribués	Commentaires sur cette valeur
Participant #4	9	9	• « La courbe du changement pour beaucoup de gens, ça ne peut pas juste nuire à la sécurité, ça peut nuire à plusieurs sphères de l'organisation. En plus, [la sécurité de l'information], c'est un domaine qui est tout le temps en train de changer. On découvre tout le temps des nouvelles façons [de faire]. Donc, il faut rester à l'affût et il faut rester ouvert d'esprit sur les façons de faire. »
Participant #5	6	6	• « Oui, effectivement. Je suis absolument d'accord. »
Participant #6	4	4	• « Ah ben oui, définitivement. La deuxième… Le volet gestion du changement, réactions face au changement… Oui, [je suis d'accord]. »
Participant #7	5	5	• Selon lui, elle est importante, mais il ne faut pas trop changer dans une courte période. Même si on est ouvert aux changements, il faut laisser une période pour vivre le changement (que le changement soit approprié par les employés); par exemple, lorsqu'un incident arrive, voir que les gens ou les systèmes réagissent comme prévu).
Participant #8	3	3	• « Oui, s'il y a quelque chose qui vas toucher les gens dans leur quotidien, c'est bien la sécurité. »
Participant #9	8	8	• « [Cette valeur] va aller après le partage. » *(lien avec la valeur #7)*
Participant #10	10	10	• « Oui, c'est tout à fait vrai, mais dans quelle mesure? Ma logique, ce que je suis en train de me dire dans ma tête, c'est que le changement, le bon changement, découle d'une habilité de planification. Donc, tu vas faire un changement parce que tu sais où tu veux t'en aller. C'est forcément dépendant de la valeur qui porte sur la planification de l'organisation. On peut faire des changements ad hoc et sans réfléchir, puis les gens vont être enthousiastes. Mais ça va marcher quelques fois et quand ils vont voir que les changements successifs que tu fais n'ont pas donné les résultats escomptés, ils vont être moins portés à accepter le changement à l'avenir. » *(lien avec la valeur #2)*
Participant #11	10	10	• « L'être humain a par définition une aversion au changement. Mais quand le changement peut être absorbé à travers de ta planification stratégique, tu es capable de voir l'impact de ce qui va arriver et de le planifier et même de le transférer au plus tactique. Tu ne te sens pas déstabilisé… Tu ne le sens pas. Tu peux déployer un ensemble de mesures et il faut qu'il y ait une synergie entre les mesures. C'est tout ensemble. » *(lien avec la valeur #2)*
Participant #12	6	6	• « La sécurité, c'est une course à l'armement tout le temps… Il y a toujours des changements. Les techniques se raffinent tout le temps et vont toujours se raffiner. Heureusement, le tout évolue en même temps : autant les menaces, que les vecteurs d'attaque, que la formation et les outils. Donc, les techniques changent; l'organisation s'adapte. Le problème est qu'on l'avait rapidement délégué aux technologies. Je pense que les gens commencent à réaliser que non. Dans certains cas, il faut changer la façon de faire au niveau de l'organisation. »
Participant #13	8	8	• Selon lui, elle est importante si on s'en tient juste à la portion changement de l'organisation plutôt que l'innovation/l'initiative culturelle. Pour lui, une organisation qui prend en compte la sécurité dans ses nouvelles idées, c'est l'idéal.
Participant #14	8	8	• *(Aucun commentaire)*
Score global =		**77 pts**	

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels présentés dans le tableau 4.26 permettent d'arriver aux fréquences présentées dans le tableau 4.27. Ce tableau montre que deux participants ont placé cette valeur dans le premier tiers, trois participants l'ont fait au tiers du milieu et six autres l'ont classée dans le dernier tiers du classement.

Tableau 4.27 : Tableau des fréquences pour la valeur #6

	Position	Fréquence	Total
Premier tiers	1	-	2
	2	-	
	3	1	
	4	1	
Tiers du milieu	5	1	3
	6	2	
Dernier tiers	7	-	6
	8	3	
	9	1	
	10	2	

- **Analyse des résultats obtenus pour cette valeur**

La majorité des participants a placé cette valeur dans le dernier tiers du classement (#4, #9, #10, #11, #13 et #14), ce qui lui a valu un score global relativement élevé de 77 points (pour un score global variant de 11 à 121 points). Cependant, en accord avec leur classement (#5, #6, #8, #12) ou contrairement à leur classement (#4, #10 et #13), les commentaires de plusieurs participants soutenaient fermement l'influence importante de cette valeur sur la variable dépendante. Pour ce qui est du participant #14, son classement montre qu'elle est lui est d'importance moindre puisqu'il l'a classée dans le dernier tiers de son classement.

Tel qu'il a été mentionné dans le paragraphe précédent, plusieurs participants ont stipulé que cette valeur aurait une influence considérable sur la variable dépendante (#4, #5, #6, #7, #8, #10, #11, #12 et #13). En effet, étant donné que la sécurité de l'information est un domaine qui évolue constamment et rapidement, il s'avère donc vital que l'organisation soit ouverte au changement en vue de se protéger des menaces en sécurité de l'information. Cela se matérialise par l'adoption de nouvelles méthodes de faire ou encore par des changements apportés à la politique de sécurité de l'organisation, qui, au final, ont une certaine influence sur la mise en œuvre de pratiques sécuritaires par les employés.

Bien que les participants #7, #10, #11 et #13 aient constaté l'importance de cette valeur, ils ont néanmoins nuancé leurs propos. Les participants #10 et #11 ont établi un lien entre cette valeur

et la valeur #2 (« Horizon temporel de la planification dans l'organisation »). D'après eux, un changement adéquat doit découler d'une planification stratégique permettant de déployer un ensemble de mesures qui soient efficaces et qui pourraient encourager la mise en œuvre de pratique sécuritaires par les employés. D'ailleurs, le participant #7 donne l'exemple d'une bonne planification du changement. Pour lui, apporter trop de changements dans le court terme pourraient s'avérer nuisible car les employés ne comprendraient pas la raison d'être du changement ou bien ils n'auraient pas le temps de s'approprier le changement. En outre, selon lui, un excès de changements sur un court horizon ne semblerait pas avoir une influence sur la variable dépendante. En ce qui concerne le participant #13, il a stipulé que le changement en sécurité de l'information devait être considéré dans les prises de décisions de l'organisation. Cette idée rappelle le lien avec la valeur #2 (« Horizon temporel habituel de la planification dans l'organisation »), mentionnée précédemment, puisque cette dernière valeur concernait la prise de décision par la haute direction. En somme, les propos de ces participants permettent de constater que cette valeur a une influence sur la variable dépendante, mais que le changement doit être planifié par la haute direction afin d'exercer une influence significative sur les employés. Toutefois, ces propos ne remettaient pas en cause l'importance de cette valeur par rapport à la variable dépendante.

Par ailleurs, le participant #9 a mentionné que la valeur #7 (« Force du réseau au sein de l'organisation ») était plus importante que cette valeur. Il n'a pas remis en cause l'importance de cette valeur, mais selon lui, elle semblerait être d'importance moindre que la valeur #7.

Malgré un classement qui tend vers le dernier tiers, les propos des participants ont démontré que cette valeur était importante, surtout en sécurité de l'information, qui est un domaine qui évolue de manière perpétuelle. Bien que le classement indique donc que cette valeur est d'importance moindre par rapport aux autres valeurs qui ont aussi été présentées aux participants, cette valeur semble être une source susceptible d'influence et est ainsi conservée pour la sélection finale.

4.2.1.7 Valeur #7 : Force du réseau au sein de l'organisation

VALEUR #7

Valeur partagée dans l'organisation quant à la façon dont les gens travaillent ensemble (force du réseau intra-organisationnel).

Plus un réseau fort existe entre les membres de l'organisation, plus élevées sont les chances que les employés s'appuieront, se conseilleront et discuteront les problématiques liées à la sécurité de l'information, le tout favorisant la mise en œuvre de pratiques sécuritaires. À l'opposé, si les employés évoluent dans un environnement « en silo », l'individu sera livré à lui-même, ce qui aura pour effet de nuire à la mise en œuvre de pratiques sécuritaires.

- **Résultats**

Par l'entremise des classements réalisés par les participants, cette valeur a obtenu entre un et dix points de la part des participants. De plus, aucun participant n'a écarté cette valeur de son classement. Des commentaires sur cette valeur ont été colligés pour chacun des participants, sauf pour les participants #7 et #13 (dans ces derniers cas, l'absence de commentaires peut s'expliquer par une prise de notes incomplète ou par le silence des participants). Les classements, les points attribués et les commentaires émis relatifs à cette valeur figurent dans le tableau 4.28.

Tableau 4.28 : Résultats (classements, points et commentaires) obtenus pour la valeur #7

Participant	Classement de la valeur (sur 10)	Points attribués	Commentaires sur cette valeur
Participant #4	1	1	• « Oui, je pense que ça, c'est important, aussi. » • « Les silos, ça nuit beaucoup à la sécurité [parce que] je pense que ça complexifie le problème. Ça le personnalise au lieu de le globaliser et d'avoir un objectif commun. En fait, avoir des sous-équipes qui travaillent sur des problèmes en parallèle, ça n'aide pas à avoir une cohérence et une réaction. Il y a un terme en sécurité; on dit que la complexité nuit à la sécurité. Il faut rendre ça un problème simple à résoudre. Si on le fait en silo, ça devient un problème complexe automatiquement parce qu'à ce moment-là, on permet à différents silos de résoudre le même problème de façon différente et tu n'as pas de cohérence d'organisation sur comment on l'aborde. » *(à propos de la proposition « Silo »)*
Participant #5	8	8	• « Oui, ça a une influence [sur la mise en œuvre de pratiques sécuritaires]. C'est clair. Mais il faut quand même avoir un certain niveau de maturité pour être rendu à ce que ça ait un effet positif dans le sens que, au départ, il y a des prises de conscience. Au départ, il y a la formation. Puis ensuite, si on veut continuer à progresser, là, il faut se parler. Parce que, si on reste en silos, effectivement, on va frapper un mur très rapidement et il y a beaucoup de choses qu'on ne verra pas. Donc, de façon globale, la sécurité n'évoluera pas. Donc, oui, ça a une influence. »
Participant #6	7	7	• « Oui… Oui… assez d'accord. »
Participant #7	7	7	• (*Aucun commentaire)*
Participant #8	10	10	• « Je sais pas ça, j'ai jamais vu d'endroits où la sécurité de l'information était un sujet de discussion quotidien entre les gens. Dans le sens que plus un réseau fort existe entre les membres de l'organisation, plus élevées sont les chances que les employés s'appuieront, discuteront des problématiques. Je pense que la sécurité de l'information n'est pas un sujet [de discussion]. Je n'ai pas vu d'endroits où c'était un sujet vraiment d'importance, où les gens échangeaient sur 'Aie oui…'. Je ne suis donc pas convaincu [de l'importance de cette valeur]. »
Participant #9	7	7	• « Oui. La collaboration entre les différents départements est hyper importante. Ça revient un peu à tout à l'heure… La sécurité, ce n'est pas une question de TI. C'est une collaboration de tout le monde. » *(lien avec la croyance #1)* • « Pourquoi j'ai mis la valeur #5 avant la valeur #7? Parce que je préfère avoir des gens bien informés qui ne collaborent pas que des gens qui collaborent, mais ne savent pas de quoi ils parlent. » *(lien avec la valeur #5)*
Participant #10	9	9	• « Oui… Ça, c'est comme transversal… Un petit peu à la base. Ça touche la sécurité. »

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.28 : Résultats (classements, points et commentaires) obtenus pour la valeur #7 (suite et fin)

Participant	Classement de la valeur (sur 10)	Points attribués	Commentaires sur cette valeur
Participant #11	1	1	• « Il n'y a pas de job au monde où tu ne travailles pas en équipe. Ça n'existe pas. […] [Pour la sécurité] oui, ça va prendre un investissement pour l'apprendre et changer nos façons de faire, mais une fois que c'est mis en place, ça va aider. Il faut que le higher-up reconnaisse qu'il y a un salut dans cette approche-là. »
Participant #12	10	10	• « La valeur #7, pour moi, vient en dernier. La force du réseau intra-organisationnel, ben un troupeau… de moutons non formés, ça peut être pire. Donc, oui, ils ont une belle valeur interne, mais ils demeurent des poules pas de tête. Ils n'ont aucune idée de ce qu'ils font. Ils n'ont aucune idée où ils s'en vont. » *(lien avec la valeur #5)* • « [La valeur] la moins importante pour moi, c'est le réseau intra-organisationnel, parce que c'est peut-être la plus dangereuse. Je ne pense pas qu'ils vont s'appuyer pour se conseiller et discuter des problèmes de sécurité. À part pour les gens mordus de sécurité, ce n'est pas un sujet le fun. […] C'est plate pour du monde, la sécurité, puis je doute beaucoup qu'ils en parlent entre eux. Ils vont parler d'un hack qu'ils ont lu, mais je ne pense pas qu'ils vont en parler entre eux [d'un incident à l'interne]. S'ils le font, ça va être lié à la réaction face à l'incident. Ou s'ils se font bien former, la première chose, c'est 'en cas de doute, appelez-nous' ou la politique dit 'Si vous voyez quelque chose de suspect, vous appelez…' Et l'autre chose, s'il parle à quelqu'un, je veux que ce soit un expert parce que la pire chose qui pourrait arriver est 'the blind leading the blind' ou un paquet de moutons. Un mouton demande à l'autre mouton, le deuxième mouton demande au troisième mouton, qui lui demande au premier mouton et finalement on tombe dans une boucle où tout le monde 'Ah finalement, ça doit être correct! Il y a un consensus'. »
Participant #13	5	5	• *(Aucun commentaire)*
Participant #14	9	9	• Le participant pense qu'elle a une importance moyenne.
	Score global =	**74 pts**	

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels présentés dans le tableau 4.28 permettent d'arriver aux fréquences présentées dans le tableau 4.29. Ce tableau montre que deux participants ont placé cette valeur dans le premier tiers, un participant l'a fait au tiers du milieu et huit autres l'ont classée dans le dernier tiers du classement.

Tableau 4.29 : Tableau des fréquences pour la valeur #7

	Position	Fréquence	Total
Premier tiers	1	2	2
	2	-	
	3	-	
	4	-	
Tiers du milieu	5	1	1
	6	-	
Dernier tiers	7	3	8
	8	1	
	9	2	
	10	2	

- **Analyse des résultats obtenus pour cette valeur**

La majorité des participants a placé cette valeur dans le dernier tiers du classement (#5, #6, #7, #8, #9, #10, #12 et #14), ce qui lui a valu un score global relativement élevé de 74 points (pour un score global variant de 11 à 121 points). Face à une telle majorité, il est nécessaire de se pencher sur les classements et les propos des participants qui ont placé cette valeur dans le premier tiers du classement.

En effet, seulement deux participants (#4 et #11) ont placé cette valeur dans le premier tiers du classement. Ils ont expliqué leur geste par le fait que la sécurité de l'information est une responsabilité commune. D'après eux, il s'avère important de bâtir un réseau fort entre les employés pour qu'ils collaborent, ce qui, comme les propositions le laissent entendre, favoriserait la mise en œuvre de pratiques sécuritaires. Le point de vue de ces participants était plausible car la sécurité de l'information est de plus en plus perçue comme étant « l'affaire de tous », comme le soulignait le participant #9, qui a soulevé le lien entre cette valeur et la croyance #1 (« Responsabilité d'assurer la sécurité de l'information »). Il semblerait qu'en théorie, cette valeur influencerait la variable dépendante. Néanmoins, les propos des autres participants semblaient plutôt soutenir le contraire.

De prime abord, les participants #8 et #12 doutaient que cette valeur soit représentative de la pratique. En effet, ils ont rarement été témoins d'employés qui discutaient de sécurité de

l'information entre eux. En faisant un lien entre cette valeur et la valeur #5 (« Importance accordée au développement des RH »), les participants #9 et #12 ont expliqué qu'il était souhaitable que les employés soient très éduqués en matière de sécurité de l'information afin d'encourager ce type de discussion ou un fort réseau au sein de l'organisation, mais que cela pouvait être nocif dans le cas contraire. En effet, le participant #12 a ajouté que, sans la formation, les employés pourraient mutuellement s'induire en erreur s'ils collaborent sur la base de connaissances limitées. À la lumière des propos des participants, on pourrait affirmer que l'importance présentement accordée à la sécurité de l'information et les formations actuellement offertes au sein des organisations ne permettent pas de bâtir un fort réseau qui puisse contribuer à mettre en œuvre des pratiques sécuritaires par les employés. En fait, il est peu probable que tous les employés d'une organisation soient assez outillés pour former ce réseau. On pourrait penser que seule l'équipe en sécurité de l'information serait en mesure de le faire car ils sont éduqués en la matière. D'autre part, on pourrait affirmer que les organisations, à l'heure actuelle, ne sont pas encore matures quant à la formation et à la sensibilisation à la sécurité de l'information. C'est pourquoi, pour la plupart des participants, cette valeur ne semblait pas adéquate à leur réalité organisationnelle.

L'analyse des classements et des propos des participants a révélé que cette valeur n'exercerait qu'une influence très limitée sur la mise en œuvre de pratiques sécuritaires par les employés, mais aussi qu'elle n'existerait pas dans la plupart des organisations en raison de l'éducation limitée des employés en termes de sécurité de l'information. De ce fait, elle n'est pas retenue pour la sélection finale.

4.2.1.8 Valeur #8 : Réaction habituelle de l'organisation face aux problèmes

VALEUR #8

Valeur partagée dans l'organisation quant à la réaction première de l'organisation face à un problème ou à un incident.

Plus la réaction instinctive de l'organisation face à un problème ou à un incident est de pointer un coupable, moins les employés seront motivés à partager les problèmes/incidents/difficultés entre eux et plus élevées sont les chances que les employés mettront en œuvre des pratiques non sécuritaires. À l'opposé, si la réaction est plutôt d'encourager les employés à partager leurs problèmes/incidents/difficultés, plus les chances sont élevées que ce sera aussi la même chose dans le cas de la sécurité de l'information, menant ainsi à la mise en œuvre de pratiques plus sécuritaires.

- **Résultats**

Par l'entremise des classements réalisés par les participants, cette valeur a obtenu entre un et 11 points de la part des participants. Le participant #7 a écarté cette valeur de son classement. Des commentaires sur cette valeur ont été colligés pour chacun des participants, sauf pour le participant #14 (dans ce dernier cas, l'absence de commentaires peut s'expliquer par une prise de notes incomplète ou par le silence du participant). Les classements, les points attribués et les commentaires émis relatifs à cette valeur figurent dans le tableau 4.30.

Tableau 4.30 : Résultats (classements, points et commentaires) obtenus pour la valeur #8

Participant	Classement de la valeur (sur 10)	Points attribués	Commentaires sur cette valeur
Participant #4	5	5	• « Ça, ça peut nuire de manière phénoménale. La culture de la culpabilisation… Si c'est en place, ça peut carrément détruire la capacité de détection sur un incident et d'assurer qu'on trouve la cause du problème et qu'on la ressoude. Oui. » *(à propos de la proposition « Pointer un coupable »)*
Participant #5	1	1	• « Oui, ça, je suis absolument d'accord. En fait, si on n'adopte pas une approche constructive, si on cherche à trouver un fautif, ça va nuire parce que chercher un fautif va faire en sorte que les gens ne voudront pas signaler, ne voudront pas parler. Donc, c'est contre-productif. Ça, c'est à contre-courant. Donc, oui, c'est un élément très important pour moi. »
Participant #6	7	7	• « Oui, ça aussi… Ça aussi, c'est important. Oui, ça a vraiment un impact. »
Participant #7	Exclue	11	• Il n'est pas d'accord avec la proposition de partager les incidents sans aucune imputabilité surtout si l'incident est majeur. *(lien avec la valeur #10)*
Participant #8	2	2	• « Effectivement, [je suis] très d'accord. Si ta première réaction est de trouver à qui est la faute et de le lyncher, c'est sûr et certain que personne ne viendra te voir pour te dire qu'il y a des problématiques. Je suis entièrement d'accord. On était un peu ici [ndlr : dans son organisation] il y a deux ans. »
Participant #9	10	10	• « Je suis d'accord avec les deux affirmations, pour les valeurs #8 et # 9… J'ai de la difficulté à mettre une préséance… C'est difficile de mettre une par rapport à l'autre. » *(lien avec la valeur #9)*

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.30 : Résultats (classements, points et commentaires) obtenus pour la valeur #8 (suite)

Participant	Classement de la valeur (sur 10)	Points attribués	Commentaires sur cette valeur
Participant #10	8	8	• « Je ne suis pas sûr de ça. Oui… » • « Cette problématique est complexe. C'est sûr qu'il faut avoir une imputabilité [parce qu'] il a quelque chose qui est arrivé et qui n'aurait pas dû arriver. Il faut voir pourquoi c'est arrivé. Mais il ne faut pas pointer [un coupable] directement… Quand j'ai lu juste le texte [ndlr : de la carte], [j'ai compris] ce qu'était la posture de l'organisation avant de dire 'c'est un tel'… Collectivement, qu'est-ce qu'on fait et comment qu'on agit? Est-ce que c'est des clients qui ont été affectés? Est-ce que c'est notre responsabilité envers les clients? [Faut-il] leur annoncer? etc. Oui, on va éventuellement arriver à qui était à la source de ça. Mais on ne fait pas de vendetta et pas de punition pour le plaisir. Mais à quelque part, il faut qu'il y ait une imputabilité. Il y a eu une erreur, on paie pour. » *(lien avec la valeur #10; à propos de la proposition « Pointer un coupable »)* • « C'est même secondaire de trouver le coupable et de prendre les mesures là-dessus. C'est plutôt [de voir] les responsabilités plus fondamentales envers les clients. Est-ce qu'on parle tout de suite au client ou on essaie de faire un cover up? À l'interne, tu peux me licencier parce que j'ai pesé sur le mauvais piton ou que je n'ai pas mis de patches et les hackers ont volé les cartes de crédit. Mais est-ce qu'on met ça sur le tapis? Et on ne parle pas au client? Ou bien on fait preuve de transparence? Je pense que c'est plutôt ça la réaction première. Puis, c'est dur de prendre ce genre de décisions-là si tu n'as pas de plan. Donc, encore, ça découle de la planification. Tu es confronté à une situation de crise, est-ce que tu as ton plan de crise? Est-ce que tu l'as répété? Est-ce que tu sais exactement ce qu'il faut faire? Il ne faut pas y penser; faut aller tout de suite à ça. C'est sûr que c'est dur si tu n'as pas réfléchi à ça avant, puis que c'est une situation difficile. […] Avoir un plan prêt là-dessus, comme réaction première, c'est quelque chose de très important… Mais, je vais le mettre après les réponses aux pressions… Qu'il y ait une gouvernance. D'abord, si on a une bonne planification, on sait ce qu'on doit faire… On calcule tout ça, le cadre normatif […], les tendances du marché, ce qui est l'attente du client etc. Puis, la réaction première va tenir compte de tout ce genre de choses. On n'agit pas sur l'impulsion. La réaction première est le fruit d'un travail qui prend en compte tout ça. » *(lien avec la valeur #2)*
Participant #11	9	9	• « Réagir au changement, mais de voir qu'on n'est pas déstabilisé par quelque chose qui se passe, que dans notre réponse aux incidents on [reste] compétent. En fait, [cette valeur], c'est en amont de l'autre [la valeur #6]. Opérationnellement, tu vois le problème et la réponse aux incidents. » *(lien avec la valeur #6)*

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.30 : Résultats (classements, points et commentaires) obtenus pour la valeur #8 (suite et fin)

Participant	Classement de la valeur (sur 10)	Points attribués	Commentaires sur cette valeur
Participant #12	9	9	• « Encore une fois, c'était parce que je n'étais pas d'accord avec la définition d'une part. Et deuxièmement, pour moi, ce n'est pas une valeur… » • « Ça peut être lié au précédent, à l'imputabilité, puis on essaie de trouver un coupable. C'est une possibilité. » *(lien avec la valeur #10)* • [Il propose une reformulation de cette valeur :] « Trouver un coupable ou trouver la source… Ça revient au même parce que c'est un problème humain. La source, c'est un être humain. C'est juste une question de sémantique. Puis l'autre, à l'opposé, la réaction est plutôt d'encourager les employés à partager leurs problèmes, incidents et difficultés, et les chances seront plus élevées. D'habitude, les incidents sont soit à cause de la politique, soit à cause des systèmes en place; c'est rapide à trouver. Puis, si ce n'est pas trouvé sur-le-champ, c'est trouvé plus tard. Les outils en place aujourd'hui permettent de savoir quand l'employé aurait dû le savoir. C'est donc pire, parce qu'il s'est passé quelque chose il y a six jours sur ton poste et tu ne l'as pas déclaré. Quand on revient à la formation, on réussit à avoir de meilleurs résultats. »
Participant #13	7	7	• La perception des pairs est très importante. Le regard des collègues fait plus mal que ta propre conscience. • Il préfère la fin du paragraphe que le début parce qu'il y a des organisations qui, même si elles ne pointent pas de coupable, ça encourage pas les gens à avoir une bonne pratique sécuritaire.
Participant #14	2	2	• *(Aucun commentaire)*
	Score global =	**71 pts**	

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels présentés dans le tableau 4.30 permettent d'arriver aux fréquences présentées dans le tableau 4.31. Ce tableau montre que trois participants ont placé cette valeur dans le premier tiers, un participant l'a fait au tiers du milieu, six autres l'ont classée dans le dernier tiers du classement et un participant l'a exclue de son classement.

Tableau 4.31 : Tableau des fréquences pour la valeur #8

	Position	Fréquence	Total
Premier tiers	1	1	3
	2	2	
	3	-	
	4	-	
Tiers du milieu	5	1	1
	6	-	
Dernier tiers	7	2	6
	8	1	
	9	2	
	10	1	
Exclusion	-	1	1

- **Analyse des résultats obtenus pour cette valeur**

La majorité des participants a placé cette valeur dans le dernier tiers du classement (#6, #9, #10, #11, #12 et #13), ce qui lui a valu un score global relativement élevé de 71 points (pour un score global variant de 11 à 121 points). Les participants étaient partagés quant à l'influence de cette valeur sur la variable dépendante. En effet, les propos des participants #4, #5, #6, #8, #9 et #13 montraient cette valeur avait un impact considérable sur la mise en œuvre de pratiques sécuritaires par les employés tandis que pour les autres participants (#7 et #12), son importance était contestable. En ce qui concerne le participant #14, son classement indiquait que cette valeur était importante, puisqu'il l'a placée dans le premier tiers.

L'analyse des propos des participants ayant placé cette valeur dans le dernier tiers du classement a révélé que leur décision était principalement basée sur deux raisons : l'importance moindre de cette valeur par rapport aux autres valeurs qui leur ont été présentées et l'inexactitude d'une des propositions qui lui sont liées.

En ce qui concerne la première raison, elle a été relevée dans les propos des participants #6, #7 #9, #10 et #12. Premièrement, le participant #6 a déclaré que cette valeur était importante avant de finalement la classer à la septième position de son classement. On semble pouvoir en déduire que bien qu'elle soit importante, cette valeur est d'importance moindre par rapport aux autres valeurs qui lui ont été présentées. Le constat à retirer des propos du participant #9 est le

même. En effet, celui-ci avait de la difficulté à déterminer quelle valeur était la plus importante entre la valeur #8 et la valeur #9 (« Réponse habituelle de l'organisation face aux pressions externes »). Cette difficulté à les départager proviendrait du fait qu'elles aient trait à la position de l'organisation (à l'externe et à l'interne). On retiendra toutefois qu'elles sont d'importance moindre puisqu'elles ont été placées en fin de classement par ce participant. Pour sa part, le participant #10 a dressé des liens entre cette valeur et les valeurs #2 (« Horizon temporel de la planification dans l'organisation »). Celui-ci a mentionné que cette valeur était secondaire puisque la planification était plus importante. En effet, son commentaire semblait pertinent puisque pour pouvoir réagir à un incident de sécurité de l'information, l'organisation devrait, au préalable, planifier ses actions. D'ailleurs ses propos se reflétaient dans son classement, puisqu'il a placé ces valeurs dans le premier tiers et dans le tiers du milieu de son classement. Enfin, le lien le plus important serait celui entre cette valeur et la valeur #10 (« Imputabilité »), relevé par les participants #7, #10 et #12. Le lien tissé semblait intéressant, puisque ces deux valeurs ont pour finalité de trouver le responsable d'un problème en sécurité de l'information. Toutefois, ces participants ont placé la valeur #10 à une plus haute position que cette valeur dans leur classement. Cela indique ainsi qu'entre ces deux valeurs, la valeur #10 semble plus importante. De plus, cela pourrait peut-être s'expliquer par la nature même des responsabilités que ces professionnels ont sur les épaules et par les défis qu'ils doivent surmonter dans leur contexte organisationnel.

En ce qui concerne la deuxième raison de ce classement qui tendait vers le derniers tiers, elle avait trait à l'inexactitude de la deuxième proposition (« À l'opposé, si la réaction est plutôt d'encourager les employés à partager leurs problèmes/incidents/difficultés, plus les chances sont élevées que ce sera aussi la même chose dans le cas de la sécurité de l'information, menant ainsi à la mise en œuvre de pratiques plus sécuritaires. ») liée à cette valeur. Tout d'abord, le participant #7 a exclu cette valeur de son classement car il était en complet désaccord avec cette proposition. Il pensait qu'il était inconcevable qu'une organisation puisse encourager le partage sans sanctionner ses employés ultérieurement. Si l'on se fie à ses propos, il semblerait donc que cette valeur n'ait pas d'influence sur la variable dépendante. De plus, le participant #13 a déclaré que, même si des organisations encourageaient le partage, cela n'encouragerait pas les employés à mettre en œuvre des pratiques sécuritaires. En somme, selon ces participants, que l'organisation pointe un coupable ou qu'elle encourage le partage, la réaction première d'une organisation n'influencerait pas la variable dépendante. Donc, dans un sens ou un autre, cette valeur n'influencerait pas la variable dépendante. D'autre part, le participant #11 a souligné le lien entre cette valeur et la valeur #6 (« Attitude générale des employés face au

changement »). Toutefois, ce lien semble sans conséquence pour cette analyse car il ne se base pas sur l'influence sur la variable dépendante.

L'analyse des classements et des propos des participants a remis en cause l'importance de cette valeur. Bien qu'une grande partie des participants aient relevé son importance, d'autres l'ont contestée et ont critiqué l'une des propositions qui lui sont liées. De ce fait, cette valeur doit être soumise à un examen global de l'ensemble des croyances afin de déterminer si cette croyance doit être conservée pour la sélection finale. Cet examen sera présenté à la section 4.2.2.

4.2.1.9 Valeur #9 : Réponse habituelle de l'organisation face aux pressions externes

VALEUR #9

Valeur partagée dans l'organisation qui réfère à la réponse habituelle de l'organisation face aux pressions provenant des clients, gouvernement, standards nationaux et internationaux, etc.

Plus l'organisation a tendance à adopter des comportements symboliques face aux obligations externes (clients, gouvernements, standards, etc.), plus élevées sont les chances qu'elle fera la même chose en ce qui a trait à la sécurité de l'information, au total menant à la mise en œuvre de pratiques moins sécuritaires. Au contraire, si l'organisation tend à prendre ces obligations/recommandations comme une occasion d'améliorer ses pratiques internes, les chances sont qu'elle fera la même chose en sécurité de l'information, ce qui mènera à la mise en œuvre de pratiques plus sécuritaires.

- **Résultats**

Par l'entremise des classements réalisés par les participants, cette valeur a obtenu entre un et dix points de la part des participants. De plus, aucun participant n'a écarté cette valeur de son classement. Des commentaires sur cette valeur ont été colligés pour chacun des participants, sauf pour les participants #7 (dans ce cas-ci, l'absence de commentaire peut s'expliquer par une prise de notes incomplète ou par le silence de ce dernier) et #11 (dans ce dernier cas, l'absence de commentaires est due au silence du participant). Les classements, les points attribués et les commentaires émis relatifs à cette valeur figurent dans le tableau 4.32.

Tableau 4.32 : Résultats (classements, points et commentaires) obtenus pour la valeur #9

Participant	Classement de la valeur (sur 10)	Points attribués	Commentaires sur cette valeur
Participant #4	10	10	• « Oui. Pour la valeur 9, c'est [pour moi], d'essayer d'être conforme, d'atteindre le niveau de conformité par rapport à être conforme. Et atteindre un niveau de conformité, c'est la façade. C'est dire 'Oui, barely good enough', on se rend là, on démontre qu'on le fait correctement, mais il n'y a pas d'intention derrière. *(à propos de la proposition « Symbolisme »)* Tandis que la [deuxième proposition], si on prend l'obligation au sérieux, ça donne aussi l'occasion de s'améliorer comme organisation et ça change beaucoup la culture. Ça a un gros impact. Je dis souvent à mes employés que la conformité, ce n'est pas assez. Parce que souvent, la conformité peut devenir péjorative. Je ne pense pas que la barre est si haute que ça en conformité de manière générale. » *(à propos de la proposition « Occasion d'amélioration »)*
Participant #5	2	2	• « J'hésite parce que je me dis que le moteur doit pas venir des obligations [de l'industrie] ou des standards des clients, il doit venir de la volonté de vouloir avoir un environnement plus sécuritaire. Donc, si on dit que l'organisation ait tendance à adopter des comportements symboliques suite aux obligations externes, c'est un mode réactif. Dans un mode réactif, tu peux, oui effectivement, avoir un comportement symbolique. » *(à propos de la proposition « Symbolisme »)* • « Si tu regardes en isolation, l'organisation qui agit comme ça, oui, ça peut avoir un impact parce qu'on veut juste dire qu'on est conformes, c'est sûr. Comme ça une organisation pourrait dire 'Ah, tu as des responsables de sécurité' ou 'tu as des responsables d'auditeurs internes' et, en fait, c'est juste pour l'apparence, juste pour être conforme. Mais dans le fond, tu ne les utilises pas à 100%. Donc, oui, c'est important si on le prend juste en isolation. » *(à propos de la proposition « Symbolisme »)*
Participant #6	10	10	• « Okay. Oui, c'est bon, j'aime ça, c'est vrai. » • « C'est un élément qui tient compte, pour moi, 'est-ce que c'est important la sécurité ou pas?' Ça rejoint vraiment ça. Ça, c'est une illustration de 'On ne pense pas que c'est important. On fait juste faire ce qu'il faut pour la conformité, mais ce n'est pas important'. Pour moi, c'est juste un exemple d'une entreprise pour qui ce n'est pas important la sécurité. C'est comme ça qu'elle va réagir. Donc, c'est juste un exemple concret de comment ce principe-là est appliqué. Par exemple, les gens qui font la reddition de comptes à [des organismes], eux autres veulent juste faire un show de boucane et bien paraître. Mais je ne suis pas sûr qu'ils influencent si directement que ça. »
Participant #7	2	2	• *(Aucun commentaire.)*
Participant #8	1	1	• « Tout à fait. Ça passe souvent par-là, d'ailleurs. »
Participant #9	9	9	• « C'est beau. Ça, on va le mettre relativement haut, celui-là. » • « Je suis d'accord avec les deux affirmations. Pour [les valeurs] #8 et #9… J'ai de la difficulté à mettre une préséance… C'est difficile de mettre un par rapport à l'autre. » *(lien avec la valeur #8)*
Participant #10	7	7	• « Oui. C'est important surtout dans la sécurité. »
Participant #11	7	7	• *(Aucun commentaire)*

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.32 : Résultats (classements, points et commentaires) obtenus pour la valeur #9 (suite et fin)

Participant	Classement de la valeur (sur 10)	Points attribués	Commentaires sur cette valeur
Participant #12	4	4	• « Il ne faut pas sous-estimer la pression qui vient de l'extérieur. Les gens vont faire de la sécurité de l'information pour les bonnes et pour les mauvaises raisons. Quand je dis mauvaises raisons, ce n'est pas pour des raisons d'éthique. C'est pour des raisons 'Qu'est-ce que le client, qu'est-ce que le fournisseur, qu'est-ce que le gouvernement va penser?'. Mais ils en font pareil. En réalité, c'est juste leur base de décision. C'est les bases qui sont éthiques, mais dans les faits, la pression externe est extrêmement efficace. Parce que l'éthique n'a pas un impact direct sur les revenus de l'entreprise, sur la valeur [économique] de l'entreprise. La mauvaise presse, oui. » • « Même s'il y a de la pression externe, ou si on pense qu'il y a de la pression externe, la formation et la connaissance sont plus importantes. Parce que même s'il y a de la pression externe et les gens n'ont aucune idée quoi faire, ce n'est pas mieux. Donc, la pression externe ne devient, pas inutile, mais elle est reléguée au second plan. » *(lien avec la valeur #5)*
Participant #13	4	4	• Il a juste dit que c'était important.
Participant #14	3	3	• Pour lui, l'impact est assez important.
	Score global =	**59 pts**	

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels présentés dans le tableau 4.32 permettent d'arriver aux fréquences présentées dans le tableau 4.33. Ce tableau montre que six participants ont placé cette valeur dans le premier tiers et cinq autres l'ont classée dans le dernier tiers du classement.

Tableau 4.33 : Tableau des fréquences pour la valeur #9

	Position	Fréquence	Total
Premier tiers	1	1	6
	2	2	
	3	1	
	4	2	
Tiers du milieu	5	-	-
	6	-	
Dernier tiers	7	2	5
	8	-	
	9	1	
	10	2	

- **Analyse des résultats obtenus pour cette valeur**

Le classement associé à cette valeur s'est avéré mitigé étant donné que les participants étaient partagés entre le premier tiers (#5, #7, #8, #12, #13 et #14) et le dernier tiers du classement (#4, #6, #9, #10, #11). Toutefois, cela lui a valu un score global relativement faible de 59 points (pour un score global variant de 11 à 121 points). Les propos des participants reflètent ce classement car ils sont également mitigés. Quant au participant 7, il l'a classée dans le premier tiers de son classement, ce qui laisse entendre qu'elle lui semble importante, tandis que le participant #11 l'a mise dans le dernier tiers de son classement, ce qui indique qu'elle lui parait être d'importance moindre.

Il s'avère ainsi pertinent de se pencher sur les propos des participants l'ayant placée dans le dernier tiers du classement afin de comprendre ce classement mitigé. Premièrement, les participants #9 et #10 ont déclaré qu'elle était importante. D'ailleurs, le participant #10 avait déclaré qu'il allait la placer en tête de classement, avant de lui attribuer la neuvième position. On peut aussi observer que le classement et les propos du participant #9 étaient aussi quelque peu contradictoires. On peut donc en déduire, dans les deux cas, que cette valeur a effectivement une influence sur la variable dépendante, mais qu'elle est d'importance moindre par rapport aux autres valeurs qui leur ont été présentées. Ceci semble expliquer la raison pour laquelle elle a été placée dans le dernier tiers du classement par ces deux participants.

En ce qui concernait le participant #4, il a affirmé que, si la pression externe était prise au sérieux, alors la conformité peut permettre à l'organisation de s'améliorer, mais aussi de changer la culture organisationnelle. Il a toutefois poursuivi avec des propos contradictoires, en déclarant que dans son organisation, pour adopter la conformité, « la barre n'est pas si haute » pour l'atteindre, et que cela ne laisse donc pas place à une grande amélioration en sécurité de l'information. Toutefois, le classement du participant semble sans conséquence car ses propos laissent indiquer qu'il a classé cette valeur en fonction des opportunités que son organisation pourrait retirer d'une plus grande conformité et non de son impact sur la variable dépendante.

Pour ce qui est du participant #6, il doutait de l'influence de cette valeur sur la variable dépendante. Il a ajouté que dans son secteur, la reddition de comptes à certaines institutions menait les organisations à adopter la conformité de manière symbolique. À son avis, l'adopter de cette manière n'exercerait pas d'influence sur la variable dépendante. Bien que cela confirme la deuxième proposition liée à cette valeur, cela ne s'applique qu'à son contexte organisationnel. En effet, les autres participants avaient stipulé que, dans un sens ou un autre, cette valeur avait une influence sur la variable dépendante.

Par ailleurs, des participants ont identifié des liens entre cette valeur et d'autres valeurs qui leur ont été présentées. Le participant #9 a mentionné qu'il lui était difficile de déterminer quelle était la valeur la plus importante entre cette valeur et la valeur #8 (« Réaction habituelle de l'organisation face aux problèmes »). Toutefois, la valeur #8 a trait à l'environnement interne alors que la valeur #9 considère l'environnement externe à l'organisation. Le participant #12 a, quant à lui, estimé que la valeur #5 (« Importance accordée au développement des ressources humaines ») était plus importante que celle-ci. Pour lui, il était primordial d'être éduqué en sécurité de l'information pour agir adéquatement en cas de pression externe. On pourrait donc en déduire que la valeur #9 n'influencerait la variable dépendante que de manière indirecte.

Ainsi, en considérant les classements et les propos des participants, on peut estimer que cette valeur a reçu un accueil mitigé parmi les participants. De plus, le lien de cette valeur avec la variable dépendante est peu clair. De ce fait, un examen global est nécessaire afin de déterminer si cette valeur doit être retenue pour la sélection finale. Cet examen figurera à la section 4.2.2.

4.2.10 Valeur #10 : Imputabilité

VALEUR #10

Valeur partagée dans l'organisation quant à l'imputabilité des employés, soit la responsabilité de chacun face aux conséquences des décisions prises et gestes posés.

Plus on tend au sein de l'organisation à assumer les conséquences des décisions prises et gestes posés, plus les employés se sentiront responsables et seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si on évolue dans un contexte organisationnel où personne n'est jamais responsable de rien, moins élevées sont les chances que les employés mettent en œuvre des pratiques sécuritaires.

- **Résultats**

Par l'entremise des classements réalisés par les participants, cette valeur a obtenu entre un et huit points de la part des participants. De plus, aucun participant n'a écarté cette valeur de son classement. Des commentaires sur cette valeur ont été colligés pour chacun des participants, sauf pour les participants #7 et #14 (dans ces derniers cas, l'absence de commentaires peut s'expliquer par une prise de notes incomplète ou par le silence des participants). Les classements, les points attribués et les commentaires émis relatifs à cette valeur figurent dans le tableau 4.34.

Tableau 4.34 : Résultats (classements, points et commentaires) obtenus pour la valeur #10

Participant	Classement de la valeur (sur 10)	Points attribués	Commentaires sur cette valeur
Participant #4	6	6	• « Oui. L'équilibre n'est pas facile à atteindre […] parce que, des fois, si l'imputabilité est mise en place d'une manière positive, c'est correct. Si on la met en place dans une culture de culpabilité, ça peut être un piège immense. »
Participant #5	4	4	• « Moi, je dirais que [c'est important] une responsabilisation quand on dit que c'est l'affaire de tous… 'T'as cliqué… Écoute, tu as fait une gaffe. Refais-la plus'. Mais il faut clairement que ce soit en lien avec le fait qu'il ne faut pas acculer les personnes… C'est [la manière dont] tu traites les personnes. Il faut vraiment qu'il y ait cette culture-là de dire 'On te tapera pas sur les doigts, mais assume [ton erreur]'. »
Participant #6	3	3	• « Oui… Totalement. » • « Si les gens ne se sentent pas responsables et pensent qu'il n'y aura pas de conséquences, il n'y a pas de motivation… Il y a très peu de motivation, il me semble, si tu ne te sens pas responsable. »
Participant #7	1	1	• *(Aucun commentaire)*
Participant #8	5	5	• « Oui, à tellement d'endroits. Effectivement, il faut mettre des règles en place, mais quand tu les respectes pas, si il n'y a jamais de conséquences et personne est responsable, ça servira pas à grand-chose. »
Participant #9	5	5	• « Imputabilité. Absolument. Je le mettrais après le respect des politiques… C'est bien beau d'avoir des politiques, mais si personne ne se sent responsable, ça ne sert à rien. » *(lien avec valeur #4)* • « C'est un des éléments les plus difficiles parce que les gens ne veulent pas être responsables. Ils sont bien prêts à dire que les politiques ont du sens, mais lorsqu'on leur dit 'Signe en bas, il peut y avoir des conséquences disciplinaires ou perdre ton emploi si tu ne les respectes pas', là, il y a plein de bémols… 'Oui, mais ce n'est pas nécessairement de ma faute.' Les gens sont très réticents. »
Participant #10	2	2	• « Quant à l'imputabilité… Moi, personnellement, j'aime beaucoup ça. Ce n'est pas une valeur partagée, par exemple, ou pas de la manière que moi, je le pense. Les gens me disent que je pousse trop ce concept. Mais j'aime beaucoup rendre les gens responsables et imputables de leurs actes, que ce soit bon ou moins bon. Vraiment partager… Ça découle de l'éthique… C'est ma façon de voir l'éthique… Le respect des normes et des politiques… Mais c'est aussi question d'imputabilité, la responsabilité de chacun face aux conséquences. Oui, ça ne veut pas dire qu'on est incités à ne pas respecter les règles et de bypasser tous les processus. Ça veut juste dire que tout le monde sait précisément qu'il y a des conséquences qui découlent de tout ce qu'on fait, which is fine. C'est bon. » *(lien avec la valeur #3)*

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.34 : Résultats (classements, points et commentaires) obtenus pour la valeur #10 (suite et fin)

Participant	Classement de la valeur (sur 10)	Points attribués	Commentaires sur cette valeur
Participant #11	3	3	• « L'imputabilité… Ce qu'on appelle l'accountability, il n'y en a pas dans [notre] secteur. Ça n'existe pas. Jamais personne n'a perdu sa job. » • « Ce n'est pas toujours facile [d'être imputable] autant dans le secteur public que dans le secteur privé aussi. La mobilité de nos higher-ups définit la possibilité de pouvoir les maintenir imputables. Un higher-up rentre dans la job. La première année, il a carte blanche. Il n'a pas besoin d'être compétent. La deuxième année, il faut qu'il puisse faire quelque chose. La troisième année, il est en train de partir, de se trouver une autre job. Fait qu'il y a une toute petite fenêtre [d'imputabilité]. […] La raison pour laquelle la sécurité fonctionne, c'est à cause du professionnalisme du middle manager. […] Puis ce n'est pas parce qu'ils se font dire. Parce qu'ils savent que s'ils ne le font pas, ça va leur prendre trois fois plus de temps pour résoudre le problème. »
Participant #12	8	8	• « Pour moi, le développement des connaissances [valeur #5] est un prérequis à la responsabilité [valeur #10], mais [est] intimement relié. 'Je te forme à devenir responsable et je m'attends donc à ce que tu deviennes responsable'. Ce n'est pas 'Je te forme à être responsable et huit autres priorités et après ça, j'espère que tu es responsable'. Donc, [ces valeurs] vont être une à côté de l'autre, mais #5 en premier et #10 par la suite. *(lien avec la valeur #5)* • « J'étais pas d'accord avec la définition. On dit que plus on tend, au sein de l'organisation, à assumer les conséquences des décisions déjà posées, plus les employés se sentiront responsables et seront motivés à mettre en œuvre des pratiques sécuritaires.' Faut faire attention parce que si on fait des chasses aux sorcières, à chaque fois, qui est exactement ça, il faut que les gens assument leurs conséquences de tout ce qu'ils font. Les gens ne se sentiront pas responsables et motivés. Ils vont sentir qu'ils vont devoir faire du 'cover your ass'. » *(à propos de la proposition « Assumer ses responsabilités »)* • « 'Puis à l'opposé, dans un contexte où personne n'est jamais responsable de rien, moins élevées sont les chances que les employés mettent en œuvre des pratiques sécuritaires.' Oui, mais dans le contexte où les gens sont responsables de rien, d'habitude, c'est des contextes avec des politiques hyper lourdes puis là, on se retrouve dans une valeur plus élevée au niveau du respect des politiques… » *(à propos de la proposition « Non responsables »)*
Participant #13	3	3	• « C'est tellement vrai! Ça se passe comme ça pas loin d'ici [ndlr : l'organisation dans laquelle il faisait son mandat]. »
Participant #14	1	1	• *(Aucun commentaire)*
	Score global =	**41 pts**	

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels présentés dans le tableau 4.34 permettent d'arriver aux fréquences présentées dans le tableau 4.35. Ce tableau montre que sept participants ont placé cette valeur dans le premier tiers, trois participants l'ont fait au tiers du milieu et un autre l'a classée dans le dernier tiers du classement.

Tableau 4.35 : Tableau des fréquences pour la valeur #10

	Position	Fréquence	Total
Premier tiers	1	2	7
	2	1	
	3	3	
	4	1	
Tiers du milieu	5	2	3
	6	1	
Dernier tiers	7	-	1
	8	1	
	9	-	
	10	-	

- **Analyse des résultats obtenus pour cette valeur**

La majorité des participants a placé cette valeur dans le premier tiers du classement (#5, #6, #7, #10, #11, #13 et #14), ce qui lui a valu un score global relativement faible, soit 41 points (pour un score global possible variant entre 11 et 121 points). Une grande partie des participants a jugé que cette valeur était une importante source d'influence sur la variable dépendante (#5, #6, #8, #9, #10). Pour ce qui est des participants #7 et #14, ils l'ont placée en première position de leur classement, ce qui indique que cette valeur leur est importante pour expliquer l'influence du contexte organisationnel sur la variable dépendante.

Par contre, les participants #4 et #12, malgré leur classement, ont précisé que l'imputabilité avait une influence sur la variable dépendante tant qu'elle ne s'effectuait pas dans une culture de culpabilisation ou par l'entremise d'une « chasse aux sorcières ». Ce contexte organisationnel pourrait rendre l'imputabilité inutile puisque les employés ne se sentiraient pas responsables de la mise en œuvre de pratiques sécuritaires et préféreraient éviter toute responsabilité afin d'éviter d'être sanctionnés. De plus, le participant #11 a déclaré que l'imputabilité n'existait pas dans son secteur. Le participant #12 a d'ailleurs déclaré que les caractéristiques de ce même secteur (par exemple, des politiques organisationnelles très lourdes) ne favorisaient pas le développement d'une valeur se rapportant à l'imputabilité. Pourtant, des participants œuvrant dans d'autres secteurs d'activité semblaient croire que l'imputabilité existait et qu'elle avait une influence sur la variable dépendante. Ainsi, les

critiques de ces participants semblaient sans conséquence pour l'analyse car elles s'inscrivaient dans un contexte organisationnel précis (telle la culture de culpabilité ou bien le secteur d'activité dans lequel œuvre le participant #11). De ce fait, on accorde peu d'importance au fait que le participant #12 ait classé cette valeur dans le dernier tiers du classement.

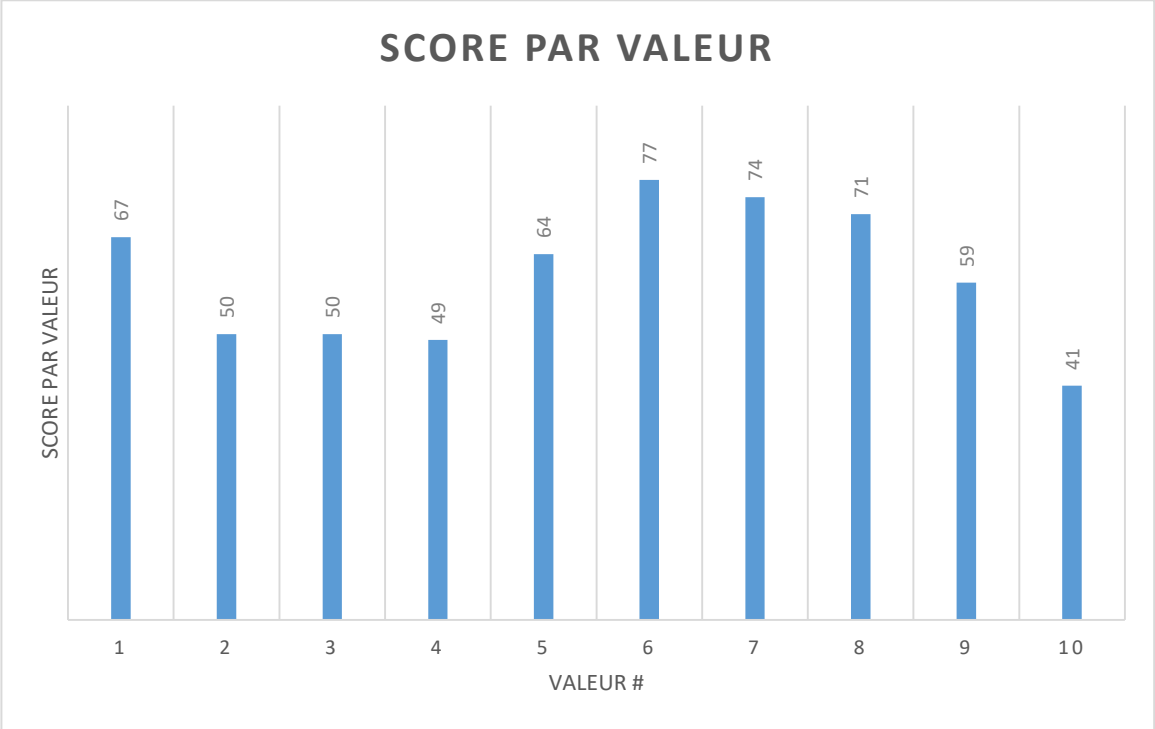
Par ailleurs, les propos des participants ont indiqué que cette valeur découlait de certaines des neuf valeurs qui leur ont été présentées. D'une part, le participant #10 a dressé un lien entre cette valeur et la valeur #3 (« Prédispositions éthiques de l'organisation »). Pour lui, l'imputabilité découle de l'éthique puisque le respect des normes et des règles organisationnelles est une étape préalable à l'imputabilité. En effet, l'imputabilité a lieu seulement si les employés ne se conforment pas aux normes ou aux règles organisationnelles. Le participant #9 a mentionné un lien entre cette valeur et la valeur #4 (« Attitude des employés envers la conformité »). Selon lui, sans l'imputabilité, avoir des politiques organisationnelles serait inutile. Pour le participant #12, la valeur #5 (« Importance accordée au développement des ressources humaines ») est un prérequis à cette valeur. D'après lui, il est nécessaire de former les employés à être responsable de la sécurité de l'information, et donc en être imputable. Ainsi, le tout ouvre la porte à l'idée que ces valeurs préparent le terrain pour qu'il y ait imputabilité en sécurité de l'information au sein de l'organisation.

Compte tenu du classement et des commentaires globalement positifs des participants, on peut affirmer que cette valeur semble exercer une influence importante sur la variable dépendante. Par conséquent, cette valeur est retenue pour la sélection finale.

4.2.2 Valeurs : Analyse globale et décisions

L'analyse individuelle de chacune des valeurs a permis de prendre une décision d'inclusion ou de rejet dans le cadre de plusieurs valeurs, mais certains résultats plus mitigés (notamment pour les valeurs #8 et #9) nécessitent la conduite d'une analyse comparative élargie pour déterminer si les résultats globaux pourraient alimenter notre réflexion. À cet effet, les analyses individuelles de la sous-section précédente et le score global attribué à chacune des valeurs (voir la figure 4.2) sont utilisés. Pour rappel, plus le score global figurant dans la figure 4.2 est faible, plus la valeur est susceptible d'influencer la variable dépendante selon les participants.

Figure 4.2 : Score obtenu pour chacune des valeurs suite à l'ensemble des classements



D'emblée, il est nécessaire de faire un récapitulatif des décisions qui ont été prises à l'issue des analyses individuelles des valeurs. Premièrement, il a été décidé de conserver les valeurs #2 (« Horizon temporel de la planification dans l'organisation »), #3 (« Prédispositions éthiques de l'organisation »), #4 (« Attitude des employés envers la conformité »), #5 (« Importance accordée au développement des ressources humaines »), #6 (« Attitude générale des employés face au changement ») ainsi que #10 (« Imputabilité ») pour la sélection finale de valeurs. Deuxièmement, les analyses individuelles des valeurs #1 (« Bases générales sur lesquelles sont prises les décisions dans l'organisation ») et #7 (« Force du réseau au sein de l'organisation ») se sont conclues par le rejet de ces dernières. Ainsi, les analyses individuelles des valeurs #8 et #9 ont démontré la nécessité de les soumettre à une analyse globale pour décider si elles pouvaient figurer ou non sur la liste finale de valeurs.

L'analyse individuelle de la valeur #8 (« Réaction habituelle de l'organisation face aux problèmes ») a également révélé le besoin de conduire un examen global de cette dernière. D'une part, plusieurs participants ont stipulé que l'une des propositions liées à cette valeur ne reflétait pas adéquatement la pratique. Cela a mené à la reformulation de cette proposition, mais il s'est avéré que dans un sens ou dans l'autre, celle-ci n'influençait plus la variable dépendante. D'autre part, les liens soulevés entre cette valeur et d'autres valeurs laissaient entendre qu'elle était d'importance moindre. La valeur #10 (« Imputabilité ») implique la même pratique que cette valeur (c'est-à-dire trouver le responsable d'un problème en sécurité

de l'information). Étant donné que la valeur #10 était plus importante pour les participants et qu'elle a été retenue pour la sélection finale, il s'avère pertinent, avec l'objectif de parcimonie, de ne pas conserver la valeur #8. De plus, la figure 4.2 montre que cette valeur a obtenu 71 points, qui est le troisième score le plus élevé parmi toutes les valeurs. Ces constats mènent à ne pas retenir cette valeur pour la sélection finale.

L'analyse individuelle de la valeur #9 (« Réponse habituelle de l'organisation face aux pressions externes ») a démontré le besoin d'effectuer un examen global de cette valeur. L'examen des propos des participants a révélé que cette valeur était susceptible d'influencer la variable dépendante, mais qu'au final, son importance était moindre par rapport aux autres valeurs qui ont été présentées aux participants. De plus, les propos recueillis semblaient démontrer que cette valeur influencerait de manière indirecte la variable dépendante. Par exemple, la pression externe d'une régulation n'encouragerait pas de manière significative la mise en œuvre de pratiques sécuritaires par les employés, mais influencerait plutôt la formation qui va les outiller à cet effet. Il faut également tenir compte de la figure 4.2, qui montre que cette valeur a obtenu 59 points, qui est le sixième score global le plus élevé parmi toutes les valeurs. Dans un souci de parcimonie, il vaut mieux accorder plus d'importance aux valeurs qui ont une influence importante et directe sur la variable dépendante. Ainsi, la valeur #9 n'est pas conservée pour la sélection finale.

À l'issue des analyses individuelles et globales, les décisions suivantes ont été prises :

- Six valeurs ont été retenues et seront incluses telles quelles dans la sélection finale :
    - Valeur #2 : Horizon temporel de la planification dans l'organisation
    - Valeur #3 : Prédispositions éthiques de l'organisation
    - Valeur #4 : Attitude des employés envers la conformité
    - Valeur #5 : Importance accordée au développement des ressources humaines
    - Valeur #6 : Attitude générale des employés face au changement
    - Valeur #10 : Imputabilité
- Quatre valeurs ne sont pas retenues pour la sélection finale :
    - Valeur #1 : Bases générales sur lesquelles sont prises les décisions dans l'organisation
    - Valeur #7 : Force du réseau au sein de l'organisation
    - Valeur #8 : Réaction habituelle de l'organisation face aux problèmes
    - Valeur #9 : Réponse habituelle de l'organisation face aux pressions externes

4.3 Caractéristiques du climat : résultats et analyses

Cette section présente les résultats du troisième exercice de priorisation, qui portait sur les 11 caractéristiques du climat qui avaient été relevées dans le chapitre 2. Il sera d'abord question d'analyser les résultats à l'aide d'une analyse individuelle, où les classements et les propos des participants sont examinés afin de déterminer si la caractéristique est importante pour expliquer l'influence du contexte organisationnel sur la variable dépendante. Dans le cas où l'analyse individuelle n'a pas abouti à une décision, la caractéristique du climat sera soumise à une analyse globale qui consiste à la comparer avec d'autres caractéristiques du climat. Cette analyse globale est ainsi présentée à la fin de la section afin de déterminer les caractéristiques du climat à retenir pour la sélection finale.

4.3.1 Caractéristiques du climat : résultats et analyses individuelles

Cette sous-section fait état des résultats recueillis lors des entrevues individuelles avec les professionnels en sécurité de l'information. Pour chaque caractéristique du climat, la carte sur laquelle elle est inscrite, les classements et les commentaires des participants ainsi qu'une analyse des résultats seront présentés.

4.3.1.1 Caractéristique du climat #1 : Soutien projeté par les gestionnaires

CARACTÉRISTIQUE DU CLIMAT #1

Cette caractéristique du climat organisationnel réfère aux gestes et comportements des gestionnaires par rapport à la sécurité de l'information.

Plus les gestionnaires ont tendance à montrer un appui à la sécurité de l'information (par leurs gestes, paroles, décisions et appuis concrets (comme des ressources financières), plus les employés comprendront que la sécurité de l'information est importante dans leur environnement de travail et seront motivés à mettre eux aussi en œuvre des pratiques sécuritaires. À l'opposé, si le message reçu des gestionnaires est que la sécurité de l'information a peu d'importance dans leur environnement de travail, plus les chances sont élevées que les pratiques sécuritaires ne seront pas mises en œuvre.

- **Résultats**

Par l'entremise des classements réalisés par les participants, cette caractéristique du climat a obtenu entre un et quatre points de la part des participants. De plus, aucun participant n'a écarté cette caractéristique du climat de son classement. Des commentaires sur cette caractéristique du climat ont été colligés pour chacun des participants, sauf pour le participant #14 (dans ce

dernier cas, l'absence de commentaires peut s'expliquer par une prise de notes incomplète ou par le silence du participant). Les classements, les points attribués et les commentaires émis relatifs à cette caractéristique du climat figurent dans le tableau 4.36.

Tableau 4.36 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #1

Participant	Classement de la caract. (sur 11)	Points attribués	Commentaires sur cette caractéristique du climat
Participant #4	4	4	• « Oui, mais je trouve qu'il y a un lien [entre] l'engagement et le rôle du gestionnaire, le premier représentant de l'organisation. Si on prêche par parole, par geste, par rapport à ça, on augmente la culture, on augmente aussi l'engagement de nos employés. On leur met ça un peu plus clair et ce qu'ils doivent faire. C'est le premier représentant. Donc, je le mettrais vraiment pile-poil avec l'engagement. » *(lien avec la caractéristique du climat #7)*
Participant #5	1	1	• « Oui. Je suis d'accord… Oui effectivement, c'est un élément qui influence. » • « J'accroche plus sur la première partie de l'énoncé qui dit 'Les employés comprendront que la sécurité de l'information est importante'. Donc, c'est sûr que si on voit qu'il y a beaucoup de mécanismes de sécurité, par exemple, des gardiens de sécurité, un SAS pour aller aux salles de serveurs et autres, tout ça montre l'importance. *(à propos de la proposition « Message appliqué »)* • La deuxième partie, je suis un peu moins sûr parce que ça dit 'Ils seront motivés à mettre eux aussi en œuvre des pratiques sécuritaires'. Tu peux être dans un environnement où il y a plusieurs contrôles de sécurité… Tu comprends l'importance, mais est-ce que, en voyant des caméras, des gardes de sécurité, ça te motive toi à adopter des comportements plus sécuritaires ? [Les autres valeurs], montrer du leadership, parler aux personnes, comprendre, sensibiliser, former... […] Je dirais [que cette valeur] facilite la compréhension [de ces valeurs]. […] Si on dit que c'est important et ils voient que, effectivement, il y a des caméras; il y a une voûte si on est dans une banque… Donc là, tout devient cohérent et c'est plus facile pour la personne d'adhérer, finalement. » *(à propos de la proposition « Message non appliqué »)*
Participant #6	2	2	• « Pour moi, c'est juste une illustration de cette [autre] caractéristique, de l'importance accordée au quotidien. Ça passe beaucoup par ton gestionnaire, lui, comment y réagit et qu'est-ce qu'il dit? Qu'est-ce qu'il fait? La caractéristique #1, c'est un exemple du #11. » *(lien avec la caractéristique du climat #11)*
Participant #7	3	3	• « C'est majeur. » • Il dit qu'elle doit aller au haut du classement des caractéristiques du climat. • L'importance accordée à la sécurité (caractéristique du climat #11) est la base à partir de laquelle découlent les caractéristiques #1 et #9. *(lien avec les caractéristiques du climat #9 et #11)*
Participant #8	1	1	• « C'est important. Notre président, il l'a déjà dit dans une conférence ici [ndlr : dans son organisation] que c'était important, mais si tous les gestionnaires [ne se préoccupent pas de la sécurité de l'information] et qu'il n'y a pas de conséquences, [les employés ne seront pas motivés à adopter des gestes sécuritaires].»

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.36 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #1 (suite)

Participant	Classement de la caract. (sur 11)	Points attribués	Commentaires sur cette caractéristique du climat
Participant #9	2	2	• « Oui. Plus on accorde d'importance à la sécurité, plus les employés seront motivés. » • « Si je n'ai pas de culture d'entreprise en sécurité et un climat organisationnel qui reflète l'importance [de la sécurité], l'employé peut me dire 'Mais moi, j'ai aucune espèce de connaissance que c'est important pour toi.' Si je n'ai jamais dit ce qu'il fallait faire, si j'ai les départements qui [sont hostiles] entre eux et disent que la sécurité, c'est de la foutaise et que bon… etc. Alors, je ne peux pas seulement punir ou récompenser. Si je n'explique pas mes attentes [pour les pratiques sécuritaires]… On dit toujours qu'on doit prêcher par l'exemple. Alors c'est pour ça que pour moi, le #11 était plus important. » *(lien avec les caractéristiques du climat #9 et #11)*
Participant #10	1	1	• « Tout à fait. Fort importante. » • « [Cette caractéristique], c'est le pouvoir de faire peur aux employés par la gestion. Il ne faut jamais la sous-estimer. »
Participant #11	4	4	• « Tu vois ton boss qui s'en moque; regarde, c'est clair… Ton désir pour la sécurité… C'est sûr… Tu ne te sens pas reconnu pour avoir le souci de la sécurité. C'est sûr que ça mine l'organisation, c'est sûr. »
Participant #12	1	1	• « Sans l'ombre d'un doute. Ce sont les gestes et comportements des gestionnaires par rapport à la sécurité de l'information. Puis pour moi, les gestes et comportements, ça inclut également le walk the talk, ça veut dire les ressources qu'on lui donne. C'est gestes, paroles, décisions et appuis concrets comme ressources financières, c'est en plein ça. »
Participant #13	2	2	• « Oui, c'est clair. »
Participant #14	4	4	• *(Aucun commentaire)*
	Score global =	**25 pts**	

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels présentés dans le tableau 4.36 permettent d'arriver aux fréquences présentées dans le tableau 4.37. Ce tableau montre que les 11 participants ont placé cette caractéristique du climat dans le premier tiers du classement.

Tableau 4.37 : Tableau des fréquences pour la caractéristique du climat #1

	Position	Fréquence	Total
Premier tiers	1	4	11
	2	3	
	3	1	
	4	3	
Tiers du milieu	5	-	-
	6	-	
	7	-	
Dernier tiers	8	-	-
	9	-	
	10	-	
	11	-	

- **Analyse des résultats obtenus pour cette caractéristique du climat**

Tous les participants ont placé cette caractéristique du climat dans le premier tiers du classement, ce qui lui a valu le score global le plus faible de 25 points (pour un score global possible variant entre 11 et 132 points). Les commentaires des participants étaient à l'image de ce classement car ils étaient tous positifs. En effet, tous les participants ont déclaré que cette caractéristique du climat avait une importante influence sur la mise en œuvre de pratiques sécuritaires par les employés. En ce qui concerne le participant #14, son classement semblait indiquer que cette caractéristique du climat lui était relativement importante puisqu'il l'a placée dans le premier tiers de son classement.

Outre l'importance de cette caractéristique du climat, les liens entre cette dernière et d'autres caractéristiques du climat ont été relevés à plusieurs reprises. Pour le participant #4, cette caractéristique du climat pourrait influencer la caractéristique du climat #7 (« Engagement organisationnel »). Suivant ses propos, les gestes du gestionnaire pourraient influencer les employés et, par conséquent, favoriser leur engagement. De plus, le participant #6 a mentionné qu'il existait un lien entre cette caractéristique du climat et la caractéristique du climat #11 (« Importance réelle accordée à la sécurité de l'information »). En effet, il a déclaré que la caractéristique du climat #1 était la matérialisation de la caractéristique du climat #11. Selon lui, si beaucoup d'importance est accordée à la sécurité de l'information au sein d'une organisation, alors les actions des gestionnaires vont aller dans le sens d'assurer la sécurité de

l'information. Le classement individuel du participant #6 indiquait cependant que ces caractéristiques du climat sont d'égale importance car il les a toutes deux classées en deuxième position. Les participants #7 et #9 étaient du même avis que le participant #6. D'après eux, les caractéristiques du climat #1 et #9 (« Récompenses/sanctions ») découlent de la caractéristique du climat #11 (« Importance réelle accordée à la sécurité de l'information »). Selon le participant #9, cette dernière teinte les gestes des gestionnaires et justifie les récompenses et les sanctions en sécurité de l'information. En somme, les liens relevés par les participants avec les autres caractéristiques du climat ont fait ressortir l'importance de cette caractéristique du climat. En effet, elle influencerait la variable dépendante de concert avec les autres caractéristiques et peut être considérée comme étant l'une des principales caractéristiques du climat du contexte organisationnel en sécurité de l'information.

En résumé, cette caractéristique du climat a unanimement été classée dans le premier tiers du classement et a seulement fait l'objet de commentaires positifs quant à l'importance de son influence sur la variable dépendante. De plus, les liens qui ont été soulevés entre cette dernière et les autres caractéristiques du climat ont mis l'accent sur son importance. De ce fait, cette caractéristique du climat est retenue pour la sélection finale.

4.3.1.2 Caractéristique du climat #2 : Communication organisationnelle

CARACTÉRISTIQUE DU CLIMAT #2

Cette caractéristique du climat organisationnel réfère à la capacité de l'organisation à communiquer des messages clairs par rapport à la sécurité de l'information.

Plus l'organisation arrive à communiquer des messages clairs quant à la sécurité de l'information (objectifs, importance, attentes, etc.), plus les employés seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si les messages sont absents ou confus, plus les chances sont élevées que les pratiques sécuritaires ne seront pas mises en œuvre.

- **Résultats**

Par l'entremise des classements réalisés par les participants, cette caractéristique du climat a obtenu entre deux et neuf points de la part des participants. De plus, aucun participant n'a écarté cette caractéristique du climat de son classement. Des commentaires sur cette caractéristique du climat ont été colligés pour chacun des participants, sauf pour les participants #7, #13 et #14 (dans ces derniers cas, l'absence de commentaires peut s'expliquer par une prise de notes

incomplète ou par le silence des participants). Les classements, les points attribués et les commentaires émis relatifs à cette caractéristique du climat figurent dans le tableau 4.38.

Tableau 4.38 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #2

Participant	Classement de la caract. (sur 11)	Points attribués	Commentaires sur cette caractéristique du climat
Participant #4	9	9	• « Oui. Le climat du message clair. Le ton de la haute direction ou de l'organisation, ce n'est pas nécessairement clair. Ça se veut un objectif global et il n'est pas nécessairement mesurable, atteignable. […] Si on avait des caractéristiques claires [dans mon organisation], elle y serait probablement, ça me permettrait de la voir [comme étant l'une des caractéristiques les plus importantes]. En fait, je pense que oui. Si on avait des valeurs claires… Une communication claire… Oui, définitivement [ce serait important]. »
Participant #5	6	6	• « Oui, je trouve que c'est important. Parce que, encore une fois, ça crée un sentiment d'appartenance de comprendre les attentes, l'importance des objectifs. Ça rentre dans tout ce qui est sensibilisation. Donc, communiquer aux employés ces messages-là, ça les éveille. » • « Je pense que ça devrait venir avant de bien comprendre pourquoi c'est important. Et après, tu es plus réceptif aux outils par la suite. Donc, je le placerais avant le #3. » *(lien avec la caractéristique du climat #3)*
Participant #6	9	9	• « Oui, tout à fait. Ça, c'est la clarté des messages et de quelle manière ça influence [les employés]. Je pense que… Absolument, [c'est important]. »
Participant #7	6	6	• *(Aucun commentaire)*
Participant #8	4	4	• « Effectivement. »
Participant #9	5	5	• « Le message clair, naturellement, c'est en premier. Effectivement, parce que si ton message est clair, que tu aimes ton entreprise, tu vas aller en fonction du message clair. Quand je parle, j'essaie de me convaincre moi-même. Alors que si j'aime mon entreprise, mais je ne sais pas comment faire… » • « Les caractéristiques du climat #11 et #2… Si l'organisation démontre par ses agissements que la sécurité est importante, même si on n'explique pas tout, on n'explique pas pourquoi, mais si les gens voient que c'est important, ils vont quand même avoir une attitude [sécuritaire]. Si on leur explique pourquoi, ils vont comprendre pourquoi c'est important pour l'entreprise. » *(lien avec la caractéristique du climat #11)*
Participant #10	2	2	• « Certainement. Mais ça, j'ai de la difficulté parce que je le vois comme transversal. Ça tient plutôt de l'aspect communication, donc je peux la retrouver dans tous les autres pamphlets sur le climat. C'est la communication. Bon, ben là, si je dois ressortir et l'identifier, je la mettrai quand même en deuxième [position dans le classement]. » • « Par contre, il ne faut jamais sous-estimer la force du message que la haute direction peut envoyer aux employés. C'est l'affaire la plus importante. Les gens ont naturellement tendance à se tourner vers [la haute direction] et de prendre tout message qui vient. Que ce soit vrai ou moins vrai. Mais c'est important ce qui est dit. »

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.38 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #2 (suite et fin)

Participant	Classement de la caract. (sur 11)	Points attribués	Commentaires sur cette caractéristique du climat
Participant #11	8	8	• « Oui, le message clair, le mot d'ordre, que ce soit un message éthique, que ce soit un message qu'il n'y a pas un système qui va se connecter sur le système s'il n'a pas été accrédité. On n'accrédite pas un système… Ça ne prend pas une journée. Vous ne mettez pas la sécurité au début; on n'accrédite pas le système. C'est des messages. C'est des messages, des valeurs… On voit le lien entre les deux [ndlr : entre cette caractéristique du climat et la variable dépendante]. C'est ça. »
Participant #12	2	2	• « Même si vous mettez des millions, si ce n'est pas clair quelles sont les attentes par rapport à la sécurité de l'information… Comme n'importe quel autre message clair, quel est le message, par rapport aux valeurs de l'entreprise, par rapport aux opérations, par rapport à la façon de vendre… Il faut que le message soit clair. »
Participant #13	9	9	• *(Aucun commentaire)*
Participant #14	9	9	• *(Aucun commentaire)*
	Score global =	**69 pts**	

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels présentés dans le tableau 4.38 permettent d'arriver aux fréquences présentées dans le tableau 4.39. Ce tableau montre que trois participants ont placé cette caractéristique du climat dans le premier tiers du classement, trois participants l'ont mise dans le tiers du milieu et cinq autres l'ont fait dans le dernier tiers du classement.

Tableau 4.39 : Tableau des fréquences pour la caractéristique du climat #2

	Position	Fréquence	Total
Premier tiers	1	-	3
	2	2	
	3	-	
	4	1	
Tiers du milieu	5	1	3
	6	2	
	7	-	
Dernier tiers	8	1	5
	9	4	
	10	-	
	11	-	

- **Analyse des résultats obtenus pour cette caractéristique du climat**

La majorité des participants a placé cette caractéristique du climat dans le tiers du milieu (#5, #7 et #9) et dans le dernier tiers du classement (#4, #6, #11, #13 et #14), ce qui lui a valu un score global moyennement élevé de 69 points (pour un score global possible variant entre 11 et 132 points). Toutefois, malgré des classements mitigés, les commentaires des participants étaient pour la plupart positifs (#4, #5, #6, #8, #9, #10, #11 et #12) par rapport à l'influence de cette caractéristique du climat sur la mise en œuvre de pratiques sécuritaires par les employés. En effet, pour la plupart d'entre eux, un message clair, qui exprime les attentes de la haute direction vis-à-vis la sécurité de l'information est vital pour influencer la mise en œuvre de pratiques sécuritaires par les employés. En ce qui concerne les participants #7, #13 et #14, leur classement indique qu'elle leur est d'importance moindre (puisqu'ils l'ont respectivement classée en sixième, neuvième et neuvième position)

D'autre part, quelques participants ont mentionné qu'il existait des liens entre cette caractéristique du climat et d'autres caractéristiques. Pour le participant #5, la communication organisationnelle est importante puisqu'elle permet aux employés d'être plus réceptifs à l'apprentissage de la sécurité de l'information (caractéristique du climat #3). Le participant #9 a stipulé qu'il y avait un lien entre cette caractéristique du climat et la caractéristique du climat #11 (« Importance réelle accordée à la sécurité de l'information »). Pour ce dernier, cette

caractéristique du climat affecte la caractéristique du climat #11. En effet, si on communique le message que la sécurité de l'information est importante au sein de l'organisation, alors les employés vont agir en conséquence. Ces liens pourraient justifier les commentaires positifs des participants car elle encourage les employés à agir de manière sécuritaire, mais aussi parce qu'elle pourrait influencer d'autres caractéristiques du climat.

Ainsi, malgré le classement mitigé de cette caractéristique, les commentaires tenus par les participants ont permis de mettre en exergue l'importance de cette caractéristique quant à l'influence de la variable dépendante. Par conséquent, cette caractéristique est conservée pour la sélection finale.

4.3.1.3 Caractéristique du climat #3 : Soutien à l'apprentissage

CARACTÉRISTIQUE DU CLIMAT #3

Cette caractéristique du climat organisationnel réfère aux moyens mis en place pour soutenir les employés dans la mise en œuvre des pratiques de sécurité.

Plus l'organisation met en place les outils qui permettent de soutenir la formation et le développement de connaissances en sécurité de l'information, plus les employés seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si les employés ne reçoivent pas le soutien nécessaire, plus les chances sont élevées que les pratiques sécuritaires ne seront pas mises en œuvre.

- **Résultats**

Par l'entremise des classements réalisés par les participants, cette caractéristique du climat a obtenu entre quatre et 11 points de la part des participants. De plus, aucun participant n'a écarté cette caractéristique du climat de son classement. Des commentaires sur cette caractéristique du climat ont été colligés pour chacun des participants, sauf pour les participants #7, #14 (dans ces cas-ci, l'absence de commentaires peut s'expliquer par une prise de notes incomplète ou par le silence des participants) et #12 (dans ce dernier cas, l'absence de commentaires est due au silence du participant). Les classements, les points attribués et les commentaires émis relatifs à cette caractéristique du climat figurent dans le tableau 4.40.

Tableau 4.40 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #3

Participant	Classement de la caract. (sur 11)	Points attribués	Commentaires sur cette caractéristique du climat
Participant #4	11	11	• « Oui, les outils… C'est une affaire, mais c'est comment on en favorise l'utilisation… Est-ce qu'on libère les gens pour le faire? […] La sécurité est souvent mêlée avec l'outil. On pense que la sécurité, c'est l'outil. Pour la formation, il faut faire attention que l'outil ne soit pas uniquement l'objectif. C'est ce qu'on en fait. On peut avoir le meilleur outil et si on ne libère pas du temps à nos employés, pour prendre le temps, si on ne valorise pas le temps qu'ils prennent pour faire ça… On peut avoir le meilleur outil au monde, il ne sera juste pas utilisé. »
Participant #5	8	8	• « Oui, ils seront motivés. Premièrement, c'est qu'ils vont comprendre, ils vont être sensibilisés. Puis, une fois que tu comprends quelque chose, c'est sûr que là, tu le gardes en tête. Donc, tu deviens forcément plus vigilant. Puis, si l'apprentissage, la sensibilisation, c'est bien fait, donc les personnes se sentent directement impliquées, là, c'est sûr qu'ils vont pouvoir même le transposer dans leur vie personnelle et vont pouvoir l'assimiler, l'absorber. Donc, oui [je suis d'accord]. S'ils ne comprennent pas, ils ne peuvent pas être très motivés, comme quand tu commences un nouveau travail. Une fois que tu maîtrises très bien ton domaine, là, ça fait une grosse différence. Donc, oui, je suis d'accord avec celle-là. » • « Dans le fond, je la mettrais peut-être plus en première position [du classement] parce que même si l'organisation a beaucoup de budget en sécurité, même si l'organisation a un fit, si l'employé a aucun intérêt, aucune connaissance en sécurité, je crois qu'il ne serait pas nécessairement en mesure de bien apprécier le fit et le support. Donc, ça aveugle un peu sur les autres éléments. » *(lien avec les caractéristiques du climat #1 et #6)*
Participant #6	10	10	• « Oui… cette question-là… [J'ai] une interrogation simplement parce que parfois les gens n'ont pas besoin des connaissances qu'on a développées, ou des compétences. C'est juste de la sensibilisation; c'est juste de comprendre pourquoi. Souvent, ce n'est pas une connaissance spécialisée dont les gens ont besoin. C'est juste de comprendre l'importance et leurs responsabilités. Parfois, […] c'est vraiment juste des communications. » *(lien avec la caractéristique du climat #2)*
Participant #7	4	4	• *(Aucun commentaire)*
Participant #8	11	11	• « Oui, mais il faut que le contenu soit pertinent et adapté à leur réalité. Mais oui, effectivement, s'il n'y a pas de formation et que tu ne me dis pas ce que j'ai à protéger, puis comment le protéger, je ne le protégerai pas. Mais il faut que ce soit concret. Souvent, je trouve que les formations sont trop théoriques. »
Participant #9	8	8	• « Je suis d'accord. Ça revient encore à former les employés. Lorsqu'on forme, les employés comprennent pourquoi, ça améliore la sécurité. Ils ont moins tendance à outrepasser quand c'est le cas et ils comprennent l'impact et, possiblement, les conséquences. »

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.40 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #3 (suite et fin)

Participant	Classement de la caract. (sur 11)	Points attribués	Commentaires sur cette caractéristique du climat
Participant #10	9	9	• « C'est vrai. Par contre, la formation en sécurité, c'est le 'Cendrillon' de la sécurité. Non seulement tu dépenses de l'argent pour une police d'assurance dont tu n'auras peut-être pas besoin, mais tu dois encore dépenser pour faire de la formation. Des fois, tu dois le faire, mais, dans ce cas-là, tu ne devrais pas le faire [sur une base] volontaire. C'est pour ça que j'aime mieux, l'étroite collaboration entre les gens et, si tu veux, l'autoformation et la création d'une culture forte, plutôt que de me fier sur la capacité de la haute direction de débloquer des montants importants pour envoyer tout le monde systématiquement en formation. »
Participant #11	6	6	• « Soutenir les employés dans l'apprentissage des pratiques sécuritaires. Si je me sens vu et que mon boss me demande de lui dire les choses que je veux améliorer en moi ou apprendre mieux. Là, je suis capable de me sentir soutenu et ça reflète tout un investissement. Absolument. »
Participant #12	6	6	• *(Aucun commentaire)*
Participant #13	10	10	• Il trouve plus ou moins que cette caractéristique du climat est importante parce qu'on peut avoir des organisations (par exemple, les banques) qui vont avoir accès au meilleur développement et aux meilleures connaissances, mais cela ne signifie pas toujours que ces formations vont être suivies de manière assidue. Par exemple, lorsque les employés du département de comptabilité sont « dans le rush » à la fin du mois, le développement des connaissances en sécurité devient leur dernière priorité.
Participant #14	8	8	• *(Aucun commentaire)*
Score global =		**91 pts**	

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels présentés dans le tableau 4.40 permettent d'arriver aux fréquences présentées dans le tableau 4.41. Ce tableau montre qu'un participant a placé cette caractéristique du climat dans le premier tiers du classement, deux participants l'ont mise dans le tiers du milieu et huit autres l'ont fait dans le dernier tiers du classement.

Tableau 4.41 : Tableau des fréquences pour la caractéristique du climat #3

	Position	Fréquence	Total
Premier tiers	1	-	1
	2	-	
	3	-	
	4	1	
Tiers du milieu	5	-	2
	6	2	
	7	-	
Dernier tiers	8	3	8
	9	1	
	10	2	
	11	2	

- **Analyse des résultats obtenus pour la caractéristique du climat**

La majorité des participants (#4, #5, #6, #8, #9, #10, #13 et #14) a placé cette caractéristique du climat dans le dernier tiers du classement, ce qui lui a valu un score global relativement élevé, soit 91 points (pour un score global possible variant entre 11 et 132 points). Les propos des participants reflétaient aussi ce classement car peu de participants (#5, #8, #9 et #11) ont stipulé que cette caractéristique du climat était importante. Quant aux participants #7, #12 et #14, leur classement respectif laissait entendre que cette caractéristique du climat semblait importante pour le participant #7 (car il l'a placée dans le premier tiers) et d'importance moindre pour les participants #12 et #14 (puisqu'ils l'ont placée dans le tiers du milieu et dans le dernier tiers).

Les participants qui ont placé cette caractéristique dans le dernier tiers ont formulé des commentaires critiques quant à l'efficacité des formations en sécurité de l'information. Ainsi, les participants #6 et #8 ont déclaré qu'elles n'étaient pas adaptées à la réalité, car elles étaient trop souvent théoriques. Sur ces dires, on pourrait donc penser que les formations en sécurité de l'information ne représenteraient pas une plus-value qui encouragerait les employés à mettre en œuvre des pratiques sécuritaires. De plus, les participants #4, #5 et #13 ont précisé que cette caractéristique du climat était efficace si les employés avaient un intérêt pour la sécurité de l'information, et qu'ils libéraient du temps afin de suivre les formations liées au domaine. Or,

le participant #13 a mentionné que ces formations étaient souvent l'une des dernières priorités dans certaines organisations (surtout si elles n'y étaient pas obligatoires). Le participant #10, quant à lui, pensait que cette caractéristique du climat ne pouvait s'appliquer dans une organisation qui ne disposait pas beaucoup de fonds pour la formation en sécurité de l'information.

Le participant #5 a fait remarquer que cette caractéristique du climat était liée aux caractéristiques du climat #1 (« Soutien projeté aux gestionnaires ») et #6 (« Adéquation aux tâches »). La caractéristique du climat #3, traitée ici, est, selon lui, la plus importante. Même si les organisations disposent de ressources pour la sécurité de l'information et que celle-ci soit adaptée aux tâches des employés, ils seraient inutiles si les employés n'ont aucune connaissance en la matière. Le participant #6 n'était pas du même avis. Il a d'ailleurs fait le lien entre cette caractéristique du climat et la caractéristique du climat #2 (« Communication organisationnelle »). Il a mentionné que les employés n'avaient pas besoin d'avoir des connaissances en sécurité de l'information puisque la sensibilisation à la sécurité de l'information suffit à les motiver à mettre en œuvre les pratiques sécuritaires définies. Ceci peut sembler soutenir l'une des composantes de la variable dépendante, soit la conformité. En d'autres termes, la communication a un impact plus important que la formation sur les employés, ce qui remet en question l'importance de cette caractéristique du climat.

Ainsi, le classement des participants montre que cette caractéristique du climat a peu d'influence sur la mise en œuvre de pratiques sécuritaires par les employés. Les commentaires des participants viennent souligner ce fait, puisque la plupart d'entre eux ont déclaré qu'ellen'avait pas d'impact sur les employés (par exemple, les formations sont trop théoriques et non arrimées aux activités des employés) et qu'elle était difficile à appliquer dans la pratique (par exemple, les formations ne sont pas suivies si le temps et l'intérêt n'y sont pas ou bien elles sont trop coûteuses pour certaines organisations). Par conséquent, cette caractéristique n'est pas retenue pour la sélection finale.

4.3.1.4 Caractéristique du climat #4 : Implication des employés

CARACTÉRISTIQUE DU CLIMAT #4

Cette caractéristique du climat organisationnel renvoie à l'implication des employés aux étapes du cycle de vie des pratiques de sécurité de l'information.

Plus les employés se sentent impliqués dans l'élaboration et l'évolution des pratiques de sécurité, plus les employés seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si les employés ne se sentent pas impliqués, plus élevées sont les chances que les pratiques sécuritaires ne seront pas mises en œuvre.

- **Résultats**

Par l'entremise des classements réalisés par les participants, cette caractéristique du climat a obtenu entre deux et 11 points de la part des participants. De plus, aucun participant n'a écarté cette caractéristique du climat de son classement. Des commentaires sur cette caractéristique du climat ont été colligés pour chacun des participants, sauf pour les participants #8 (dans ce cas-ci, l'absence de commentaires est due au silence de ce dernier) et #14 (dans ce dernier cas, l'absence de commentaires peut s'expliquer par une prise de notes incomplète ou par le silence du participant). Les classements, les points attribués et les commentaires émis relatifs à cette caractéristique du climat figurent dans le tableau 4.42.

Tableau 4.42 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #4

Participant	Classement de la caract. (sur 11)	Points attribués	Commentaires sur cette caractéristique du climat
Participant #4	4	4	• « Absolument. Ça habilite les gens. J'ai eu à implanter un nouveau programme de sécurité pour [nom de la compagnie] en 2004, qui était imposé par le groupe. Il fallait mettre des nouveaux contrôles en place. Et ceux qui ont le mieux fonctionné et qui existent encore aujourd'hui – sont ceux pour lesquels je suis allé voir les gens pour leur demander comment ils voulaient le faire. À l'époque, c'était des accès pour des programmeurs pour qu'ils puissent faire du trouble shooting et qu'ils puissent faire de l'analyse quand on avait des problèmes. Ces gens-là perdaient tous leurs accès du jour au lendemain. J'étais la personne qui leur annonçait avec mes deux semaines d'ancienneté dans la compagnie et j'avais beaucoup de résistance au changement. Puis, je leur ai demandé 'Comment voulez-vous qu'on le fasse? Qu'est-ce que vous pensez qui serait la meilleure façon de faire ça?'. Et du jour au lendemain, ils ont créé un nouveau rôle, quelqu'un qui ne programmait plus, et qui faisait du contrôle, qui faisait de la validation, qui pouvait faire tout ça et dont c'était le rôle de faire ça. 'On va le faire comme ça.' Je n'ai jamais eu de résistance là-dessus. » *(à propos de la proposition « Implication »)* • Il est clair [qu'on ne puisse pas impliquer toute l'organisation]. […] Cette thématique-là, pour moi, il faut sortir à l'extérieur de l'équipe de sécurité et aller chercher des joueurs clé. Il y a des gens brillants dans les organisations et faut juste les trouver. […] Ce sont des sortes d'agents du changement… » *(à propos de la proposition « Implication »)*
Participant #5	5	5	• « Oui, ça crée un sentiment d'appartenance. Ça, c'est clair. S'ils sont impliqués, ils vont comprendre davantage… Ça va aider à plusieurs aspects. Donc, oui, je dirais que c'est un facteur important. » • « [Il est] moins important que le lien affectif à l'organisation. Je le mettrais en troisième position [du classement]. Parce que ça crée un sentiment d'appartenance. Dès que tu as un sentiment d'appartenance, tu veux contribuer au bien-être de l'entreprise. Donc, ça va avoir beaucoup d'effets positifs. » *(lien avec la caractéristique du climat #7)*
Participant #6	11	11	• « Oui. C'est l'implication des employés dans la conception des pratiques de sécurité. Sûrement, mais je ne suis pas sûr que c'est le premier [dans le classement]. » • « Mais c'est sûr que moi, je réfléchis et je me dis 'On est [nombre] employés [dans mon organisation]… Je ne vois pas trop comment on ferait ça'. Mais je suis convaincu que ça a un impact. [Mais ce n'est] probablement pas celui-là qui a l'impact principal. Comment est-ce que je peux tous les impliquer? Ça marche peut-être pour une PME. » *(à propos de la proposition « Implication »)*
Participant #7	8	8	• Au niveau organisationnel, l'impact n'est pas fort. • Certains ne veulent pas être impliqués; d'autres oui, mais ça dépend beaucoup de l'individu. *(à propos de la proposition « Implication »)*
Participant #8	6	6	• *(Aucun commentaire)*

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.42 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #4 (suite et fin)

Participant	Classement de la caract. (sur 11)	Points attribués	Commentaires sur cette caractéristique du climat
Participant #9	6	6	• « Effectivement. La participation aux requis de sécurité, à la rédaction des politiques, ce n'est que rédiger une politique et ensuite, la distribuer pour [obtenir des] commentaires, peu importe les commentaires qu'on reçoit. Juste le fait de distribuer, les gens se sentent parties prenantes. Quand ils sont parties prenantes, ils sont beaucoup plus enclins à respecter parce qu'on leur a demandé leur avis. Alors que l'inverse, même s'ils n'ont pas de commentaires, si on ne leur demande pas leur avis, ils peuvent être réticents. »
Participant #10	6	6	• « La ligne est fine entre le sentiment d'être écouté versus le sentiment de faire la job de l'autre. Donc, tout le monde aime ça quand on demande leur avis et comment intégrer ça pour que ce soit convivial et sécuritaire en même temps. Il faut que ça se passe rapidement et il ne faut pas les achaler trop parce que ça ne leur tente pas. Donc, il faut qu'ils se sentent écoutés, mais pas achalés. » *(à propos de la proposition « Implication »)* • « [Je mettrais cette caractéristique] au même niveau que [le fit entre les pratiques de la sécurité et les tâches à réaliser]. En fait, je vais dire que, vite comme ça, je considère que ces deux [caractéristiques] peuvent être interchangeables. Donc, si vous avez absolument besoin de les ordonner, vous mettez l'un ou l'autre. » *(lien avec la caractéristique du climat #6)*
Participant #11	9	9	• « On voit ça. C'est un petit peu une façon de faire devant l'inconnu. » • « [Je trouve que] ça ne donne rien de leur parler [ndlr : parler des politiques de sécurité aux employés]. Oui, ça a un rapport à la planification, les pratiques sécuritaires de sécurité et les tâches à réaliser, donc la priorisation, le tactique, le stratégique. Si j'identifie bien l'état de sécurité dans lequel je suis, je peux identifier mes risques et les priorités, les tâches et où on s'en va. Une fois que tu sais où tu t'en vas, [c'est à ce moment qu'il faut impliquer les employés]. » *(à propos de la proposition « Implication »)*
Participant #12	10	10	• « Pour moi, les employés se sentent impliqués si un ou deux employés sont impliqués, mais en général, c'est pas une démocratie. Et ce n'est pas parce qu'on est une petite compagnie. Ce que j'ai vu dans des entreprises plus grosses, tu impliques les personnes qui sont en charge du processus. […] Et deuxièmement, ils n'ont pas tous l'expertise. Dans certains cas, ils ne peuvent même pas imaginer ce qui s'en vient ou ce qui a lieu présentement [dans l'organisation]. Mais pour revenir à ce qu'on disait plus tôt, la plupart des gens, s'ils pouvaient ne pas s'impliquer [dans tout], ils seraient contents et ils préféreraient ça. » *(à propos de la proposition « Implication »)*
Participant #13	5	5	• « Oui, c'est bon. »
Participant #14	2	2	• *(Aucun commentaire)*
Score global = 72 pts			

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels présentés dans le tableau 4.42 permettent d'arriver aux fréquences présentées dans le tableau 4.43. Ce tableau montre que deux participants ont placé cette caractéristique du climat dans le premier tiers du classement, cinq participants l'ont mise dans le tiers du milieu et quatre autres l'ont fait dans le dernier tiers du classement.

Tableau 4.43 : Tableau des fréquences pour la caractéristique du climat #4

	Position	Fréquence	Total
Premier tiers	1	-	2
	2	1	
	3	-	
	4	1	
Tiers du milieu	5	2	5
	6	3	
	7	-	
Dernier tiers	8	1	4
	9	1	
	10	1	
	11	1	

- **Analyse des résultats obtenus pour la caractéristique du climat**

La majorité des participants a placé cette caractéristique du climat dans le tiers du milieu (#5, #8, #9, #10 et #13) et dans le dernier tiers (#6, #7, #11 et #12) du classement, ce qui lui a valu un score global relativement élevé, soit 72 points (pour un score global possible variant entre 11 et 132 points). Les commentaires de ces participants reflétaient ce classement puisque plusieurs d'entre eux pensaient qu'elle était importante, mais que son impact sur la mise en œuvre de pratiques sécuritaires était faible (#6, #7) voire plus faible que pour d'autres caractéristiques du climat (#10). De plus, certains participants (#6, #11 et #12) ont spécifié que cette caractéristique du climat était difficilement applicable dans la pratique, surtout dans une grande organisation, où il faudrait alors impliquer des milliers d'employés. Certains remettaient même en question le désir des employés d'être impliqués dans les décisions touchant la sécurité de l'information (#4, #7 #10).

Le participant #4, qui a placé cette caractéristique du climat dans le premier tiers du classement, trouvait qu'impliquer tous les employés était peu faisable et que l'on doit plutôt impliquer des joueurs clé qui agiraient comme des agents de changement. On pourrait se demander si les pratiques liées à cette caractéristique peuvent réellement être appliquées en organisation. Cela remettrait donc en cause l'importance de cette caractéristique du climat.

Par ailleurs, certains participants ont également relevé des liens avec d'autres caractéristiques du climat. Lorsqu'il a exprimé son avis, le participant #5 a fait un lien entre cette caractéristique du climat et la caractéristique du climat #7 (« Engagement organisationnel »). D'après lui, cette caractéristique du climat ne serait qu'une conséquence du lien affectif qui relie l'employé à son organisation. De ce fait, on peut affirmer que l'implication des employés est d'importance moindre pour influencer les employés à mettre en œuvre des pratiques sécuritaires. Par ailleurs, le participant #10 a mentionné que cette caractéristique du climat était aussi importante que la caractéristique du climat #6 (« Adéquation aux tâches »). Néanmoins, il n'a pas été plus explicite quant à la nature de ce lien. Ce lien ne peut donc pas être mis à profit dans cette analyse.

Les participants ont, en grande majorité, placé cette caractéristique du climat dans le tiers du milieu et dans le dernier tiers du classement. De plus, les commentaires des participants laissaient entendre que cette caractéristique du climat n'exercerait qu'une faible influence sur la variable dépendante et qu'elle n'est pas toujours applicable dans la réalité. Par conséquent, cette caractéristique n'est pas retenue pour la sélection finale.

4.3.1.5 Caractéristique du climat #5 : Adéquation au contexte organisationnel

CARACTÉRISTIQUE DU CLIMAT #5

Cette caractéristique du climat organisationnel réfère à l'adéquation (le « fit ») entre les pratiques de sécurité de l'information dans l'organisation et les caractéristiques du contexte organisationnel.

Plus les pratiques de sécurité de l'information définies sont en adéquation avec les caractéristiques du contexte organisationnel comme la culture et les pratiques d'affaires, plus les employés seront enclins à mettre en œuvre ces pratiques sécuritaires. À l'opposé, s'il y a un « misfit » entre les pratiques de sécurité de l'information et les caractéristiques du contexte organisationnel, plus élevées sont les chances que les pratiques sécuritaires ne seront pas mises en œuvre.

- **Résultats**

Par l'entremise des classements réalisés par les participants, cette caractéristique du climat a obtenu entre un et 11 points de la part des participants. De plus, aucun participant n'a écarté cette caractéristique du climat de son classement. Des commentaires sur cette caractéristique du climat ont été colligés pour chacun des participants, sauf pour les participants #7 et #14 (dans ces derniers cas, l'absence de commentaires peut s'expliquer par une prise de notes

incomplète ou par le silence des participants). Les classements, les points attribués et les commentaires émis relatifs à cette caractéristique du climat figurent dans le tableau 4.44.

Tableau 4.44 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #5

Participant	Classement de la caract. (sur 11)	Points attribués	Commentaires sur cette caractéristique du climat
Participant #4	1	1	• « C'est clair. Ça, on le voit beaucoup au quotidien. Ça, je peux vous en parler longtemps parce qu'il y a un misfit dans notre organisation. Un misfit entre la culture de l'organisation et la sécurité. C'est deux objectifs qui ne sont pas alignés. Pour le climat, on le voit. Il y a des gens qui peuvent être tiraillés ou des gens qui peuvent être très polarisés. »
Participant #5	9	9	• « Je trouve que ça touche les autres [caractéristiques du climat] parce que, ici, on dit 'Un fit avec le contexte'. Ça, ça veut dire que dans un domaine [industriel], dans un domaine financier, dans un domaine d'infrastructure critique, c'est sûr que c'est des contextes différents. Mettons que le profil de menaces est différent. Donc, c'est sûr que la sécurité va être ajustée en fonction justement des profils de menaces et des risques, en fonction de notre contexte. Mais les autres… les autres points dont on a discuté tantôt, on parlait d'un fit aussi… Donc, le fit entre les pratiques de sécurité de l'information dans l'organisation et les tâches à réaliser… [La caractéristique] #5, je la vois plus quand on crée un programme de sécurité. Lorsqu'on veut mettre les pratiques de sécurité dans une entreprise, on doit justement avoir un fit. Ou sinon, notre programme de sécurité, notre cadre de gouvernance n'est pas aligné avec notre domaine. Donc, je le vois plus à haut niveau. Est-ce que les employés vont vraiment regarder le fit avec l'industrie? Parce que, là, on commence à être plus loin des éléments du quotidien ou des éléments qui vont influencer notre motivation et nos actions, notre vigilance. C'est définitivement un élément essentiel pour mettre en place un bon programme de sécurité. Est-ce que ça va influencer les employés? Je suis moins certain. » *(lien avec la caractéristique du climat #6)*
Participant #6	5	5	• « Oui, tout à fait. C'est sûr. C'est vraiment important.» • « Ça va vraiment ensemble ces deux [caractéristiques]: le fit des pratiques avec les tâches, puis l'autre élément qui était [le fit] avec l'organisation. Ça va un peu ensemble dans le sens que si, par exemple, le contexte organisationnel fait qu'on doit aller très rapidement, les choses changent très rapidement, on est beaucoup dans l'innovation, on lance constamment de nouveaux produits. […] C'est sûr que, dans les tâches, si on amène énormément de lourdeur, ça suit pas. Pour moi, ça va comme ensemble. Ce n'est pas exactement la même chose, mais il doit certainement y avoir un lien entre les deux. On doit pouvoir retrouver probablement le pendant de ça. Ces deux éléments-là, c'est vraiment de fitter autant avec la tâche qu'avec le contexte.» *(lien avec la caractéristique du climat #6)*
Participant #7	10	10	• *(Aucun commentaire)*
Participant #8	7	7	• « Oui, si tu essaies d'imposer des pratiques de sécurité avec une culture qui est très 'laisser-aller', tu vas avoir un clash autant des deux bords. Très souvent, nous autres, avec les gars en sécurité ou les experts en sécurité, on arrive avec nos normes et on pogne notre ISO, 'c'est comme ça tu devrais faire ça, ta sécurité'. Puis, finalement, tu te demandes pourquoi ça ne fonctionne pas. Tu n'as pas pris le temps de regarder comment ça fonctionnait, comment l'organisation était structurée, comment les gens travaillent. C'est évident. »

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.44 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #5 (suite et fin)

Participant	Classement de la caract. (sur 11)	Points attribués	Commentaires sur cette caractéristique du climat
Participant #9	3	3	• « Absolument. Oui. Il ne faut pas faire des politiques pour faire des politiques. Il faut que les politiques soient mises dans un contexte, rédigées selon les pratiques d'affaires et la culture d'entreprise. Les politiques de sécurité, au Cirque du Soleil, puis les politiques de sécurité au SPVM, c'est deux univers complètement différents. » [ndlr : Le participant ne provient pas de l'une ou l'autre des deux organisations citées en exemple]
Participant #10	10	10	• « Oui, il y a une corrélation. Ce n'est pas universel. Je dirais, ça peut dépendre de certains critères. »
Participant #11	10	10	• « Oui. Le fit entre les pratiques sécuritaires et le contexte organisationnel. C'est ce qu'on voit dans l'environnement en ce moment avec les business needs for security. Quels sont tes besoins de sécurité pour ton système? C'est quoi le programme que tu supportes avec ton système? C'est là que tu vas obtenir le contexte organisationnel. [Dans ce contexte organisationnel], c'est en train de se mettre en place; ce n'est pas encore un acquis. C'est plus acquis dans [d'autres contextes]. »
Participant #12	5	5	• « Le fit au niveau des pratiques et le contexte organisationnel. J'ai trouvé que le contexte organisationnel, c'est très clair [en théorie], mais pour moi, c'est très large. Pour te donner deux exemples : [cette caractéristique] est, pour moi, liée à [la caractéristique] # 6 qui est 'tâches au quotidien'. Donc, je trouvais que c'était mal défini, à mon avis. Puis, il est inclus dans #6. Soit je le mets tout de suite après, soit je l'enlève complètement. Mais je ne le mettrais pas plus bas parce que, pour moi, ils sont liés. [ndlr : en parlant de la position de la caractéristique #5 dans le classement] » *(lien avec la caractéristique du climat #6)* • « Des fois, il y en a certains qui sont redondants. […] Je pense au climat, avec la caractéristique #11, on peut déduire [les caractéristiques] #5 et #6; pas besoin de le demander. La caractéristique #11 est bien cernée, bien ciblée, [les caractéristiques] #5 et #6 le sont moins, elles ne sont pas aussi pertinentes. » *(lien avec les caractéristiques du climat #6 et #11)*
Participant #13	3	3	• « C'est très vrai. »
Participant #14	11	11	• *(Aucun commentaire)*
	Score global =	**74 pts**	

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels présentés dans le tableau 4.44 permettent d'arriver aux fréquences présentées dans le tableau 4.45. Ce tableau montre que trois participants ont placé cette caractéristique du climat dans le premier tiers du classement, trois participants l'ont mise dans le tiers du milieu et cinq autres l'ont fait dans le dernier tiers du classement.

Tableau 4.45 : Tableau des fréquences pour la caractéristique du climat #5

	Position	Fréquence	Total
Premier tiers	1	1	3
	2	-	
	3	2	
	4	-	
Tiers du milieu	5	2	3
	6	-	
	7	1	
Dernier tiers	8	-	5
	9	1	
	10	3	
	11	1	

- **Analyse des résultats obtenus pour la caractéristique du climat**

Cette caractéristique du climat a obtenu un classement mitigé de la part des participants puisqu'elle a été placée de manière à peu près égale dans chacun des tiers du classement. Cela lui a valu un score global relativement élevé, soit 74 points (pour un score global possible variant entre 11 et 132 points). Une partie des participants (#4, #6, #8, #9, #11, #13) croyait fermement que cette caractéristique était importante pour influencer la variable dépendante. Les participants #5 et #10 ont partagé le même avis, mais ils ont toutefois nuancé leurs propos. En ce qui concerne les participants #7 et #14, leur classement indiquait qu'elle leur semblait être d'importance moindre puisqu'ils l'ont classée dans le dernier tiers du classement.

Les critiques à l'encontre de cette caractéristique provenaient principalement des participants #5 et #12. Ils ont précisé que cette caractéristique du climat se situait à une échelle trop globale pour pouvoir influencer les employés de manière significative (étant donné qu'elle a trait au contexte organisationnel). En outre, le participant #5 a ajouté que cette caractéristique du climat aurait une influence globale, mais une faible incidence sur les activités quotidiennes des employés, et par conséquent, peu d'influence sur la mise en œuvre de pratiques sécuritaires par ces derniers.

Ainsi, la caractéristique du climat #6 (« Adéquation aux tâches ») serait davantage susceptible d'influencer la variable dépendante si l'on se fie aux dires des participants #5 et #6. Bien

qu'elles soient étroitement liées, il se pourrait que la caractéristique du climat #6 soit plus influente sur la variable dépendante, cette dernière concernant davantage le quotidien des employés. En effet, elle touche principalement aux activités quotidiennes des employés alors que la caractéristique #5 a trait au contexte organisationnel. D'ailleurs, le participant #12 a également établi un lien entre cette caractéristique du climat et la caractéristique du climat #11 (« Importance réelle accordée à la sécurité de l'information »). D'après lui, si la sécurité de l'information est importante au sein d'une organisation, alors le contexte organisationnel et les tâches vont être adaptées dans le but d'encourager la mise en œuvre de pratiques sécuritaires. Toutefois, on pourrait faire ce lien avec toutes les autres caractéristiques du climat. Si la sécurité de l'information est importante au sein de l'organisation, il va de soi que les aspects pouvant encourager la mise en œuvre de pratiques sécuritaires seraient pris en considération.

Ainsi, l'analyse des classements et des propos liés à cette caractéristique du climat a mis en exergue son importance moindre. Avant de déterminer si elle doit être retenue ou exclue de la sélection finale, il s'avérerait pertinent d'analyser la caractéristique du climat #6 (« Adéquation aux tâches ») puisqu'elles semblent étroitement liées. Par conséquent, un examen global de cette caractéristique du climat est nécessaire afin de déterminer si elle doit être retenue pour la sélection finale. Cet examen sera présenté à la section 4.3.2.

4.3.1.6 Caractéristique du climat #6 : Adéquation aux tâches

CARACTÉRISTIQUE DU CLIMAT #6

Cette caractéristique du climat organisationnel réfère à l'adéquation (le « fit ») entre les pratiques de sécurité de l'information dans l'organisation et les tâches à réaliser.

Plus les pratiques de sécurité de l'information définies sont en adéquation avec la tâche (effort minimal, impact marginal sur le rendement, etc.), plus les employés seront enclins à mettre ces pratiques sécuritaires en œuvre. À l'opposé, si les pratiques ajoutent une lourdeur au travail quotidien, plus les chances sont élevées que les pratiques sécuritaires ne seront pas mises en œuvre.

- **Résultats**

Par l'entremise des classements réalisés par les participants, cette caractéristique du climat a obtenu entre trois et 11 points de la part des participants. De plus, aucun participant n'a écarté cette caractéristique du climat de son classement. Des commentaires sur cette caractéristique du climat ont été colligés pour chacun des participants, sauf pour les participants #7, #14 (dans ces cas-ci, l'absence de commentaires peut s'expliquer par une prise de notes incomplète ou

par le silence des participants) et #11 (dans ce dernier cas, l'absence de commentaire est due au silence du participant). Les classements, les points attribués et les commentaires émis relatifs à cette caractéristique du climat figurent dans le tableau 4.46.

Tableau 4.46 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #6

Participant	Classement de la caract. (sur 11)	Points attribués	Commentaires sur cette caractéristique du climat
Participant #4	3	3	• « C'est clair. Si les personnes [mettent en œuvre les pratiques sécuritaires], et que ça leur complexifie le travail et ça les rend inaccessibles ou ça va retarder leurs efforts, [ils ne vont pas apprécier ça]. C'est clair. Oui. »
Participant #5	10	10	• « Si je le reprends juste pour valider que je comprends bien, l'exemple qu'on donne, on évalue que le risque est faible, et pourtant, il y a plein de contrôles de sécurité, donc ça alourdit inutilement un processus parce que justement les contrôles de sécurité ne sont pas en adéquation avec le risque réel. Le risque n'est pas indiqué, mais si on parle justement de proportionnalité, on dit qu'il faut que les mesures de sécurité soient proportionnelles aux risques, proportionnelles aux enjeux. Donc, dans cette optique-là, si on doit le comprendre de cette façon-là, je dirais que oui, je suis d'accord. S'il y a un manque d'adéquation, ça va avoir une grosse influence sur la crédibilité. Donc, si une personne est obligée de respecter plein de contrôles de sécurité, et puis, il se rend compte qu'il y a des contrôles inutiles… parce que les employés sont intelligents… Donc là, clairement, il va se détacher, et puis on n'aura plus de crédibilité. S'il y a quelque chose de vraiment important, on dit qu'il faudrait mettre tel contrôle. Donc, oui, effectivement, je suis d'accord. Quand une personne voit des incohérences, c'est sûr que ça a un gros impact sur le climat. »
Participant #6	5	5	• « Oui. C'est la lourdeur des pratiques de sécurité versus les tâches. » • « Ça va vraiment ensemble ces deux [caractéristiques] : le fit des pratiques avec les tâches, puis l'autre élément qui était [le fit] avec l'organisation. Ça va un peu ensemble dans le sens que si, par exemple, le contexte organisationnel fait qu'on doit aller très rapidement, les choses changent très rapidement, on est beaucoup dans l'innovation, on lance constamment de nouveaux produits… C'est sûr que, dans les tâches, si on amène énormément de lourdeur, ça suit pas. Pour moi, ça va comme ensemble, ce n'est pas exactement la même chose, mais il doit certainement y avoir un lien entre les deux. On doit pouvoir retrouver probablement le pendant de ça. Ces deux éléments-là, c'est vraiment de fitter autant avec la tâche qu'avec le contexte. C'est vraiment important. » *(lien avec la caractéristique du climat #5)*
Participant #7	7	7	• *(Aucun commentaire)*
Participant #8	8	8	• « Effectivement. Ça, c'est toujours un problème parce que les gens pensent que tu leur en rajoutes une. Mais non, il faut que tu le fasses de cette façon-là. 'Tu me rajoutes de l'effort'. 'Non, c'est la façon de le faire.' Ça devrait être inclus dans la tâche. Et non rajoutée. »
Participant #9	4	4	• « Je le mettrais en deuxième lieu, après la caractéristique #5. Un fit organisationnel qui fait du sens et qui va tenir compte de la lourdeur. On ne veut pas faire travailler les gens inutilement, pour rien. » *(lien avec la caractéristique du climat #5)*
Participant #10	6	6	• « Oui, c'est vrai. Il ne faut pas que la sécurité soit perçue comme un fardeau incommensurable. les gens sont très peu ouverts à prendre la charge supplémentaire par rapport à la sécurité. »
Participant #11	11	11	• *(Aucun commentaire)*

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.46 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #6

Participant	Classement de la caract. (sur 11)	Points attribués	Commentaires sur cette caractéristique du climat
Participant #12	4	4	• « [Ça représente] l'importance accordée au quotidien à la sécurité de l'information. On a mis de l'argent; on a mis les choses claires [dans les messages communiqués], mais, au quotidien, on y met de l'importance, mais c'est quoi le fit de la sécurité de l'information sur tout le reste? Il y a quand même une bonne corrélation. Pour moi, la sécurité de l'information est inversement proportionnelle à la convivialité. C'est certain que ce n'est pas gratuit et ça a toujours un impact. À la limite, les gens sont prêts à pardonner certaines choses s'ils voient qu'il y a un effort sincère pour l'améliorer. S'ils voient de petits changements, mais constants, vu qu'il y a quand même une bonne communication pour expliquer tout ça et que les gens comprennent pourquoi on fait les choses. Finalement, si les gens comprennent l'importance qu'on lui donne, il y a une certaine forme d'adéquation avec les tâches et les objectifs de l'entreprise. » *(lien avec les caractéristiques du climat #1, #2 et #11)* • « [Je place la caractéristique] #11 avant [la caractéristique] #6. La #6, c'est un cas particulier [et] est fortement corrélée à la #11. » *(lien avec la caractéristique du climat #11)* • « Le fit au niveau des pratiques et le contexte organisationnel. C'est très clair [en théorie], mais pour moi, c'est très large. Pour donner deux exemples : [cette caractéristique] est, pour moi, liée à [la caractéristique] # 6 qui est 'tâches au quotidien'. Donc, je trouvais que c'était mal défini, à mon avis. Puis il est inclus dans #6. Soit je le mets tout de suite après, soit je l'enlève complètement, mais je ne le mettrais pas plus bas parce que, pour moi, ils sont liés. [ndlr : en parlant de la position de la caractéristique #5 dans le classement] » *(lien avec la caractéristique du climat #5)* • « Des fois, il y en a certains qui sont redondants. Je pense au climat, avec la caractéristique #11, on peut déduire [les caractéristiques] #5 et #6; pas besoin de le demander. La caractéristique #11 est bien cernée, bien ciblée, [les caractéristiques] #5 et #6 le sont moins, ils ne sont pas aussi pertinents. » *(lien avec les caractéristiques du climat #5 et #11)*
Participant #13	4	4	• « Ça ne peut pas être plus clair que ça. Dès que c'est tough (la mise en œuvre de pratiques sécuritaires), ils ne veulent pas le faire (les appliquer). »
Participant #14	6	6	• *(Aucun commentaire)*
	Score global =	**68 pts**	

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels présentés dans le tableau 4.46 permettent d'arriver aux fréquences présentées dans le tableau 4.47. Ce tableau montre que quatre participants ont placé cette caractéristique du climat dans le premier tiers du classement, quatre participants l'ont mise dans le tiers du milieu et trois autres l'ont fait dans le dernier tiers du classement.

Tableau 4.47 : Tableau des fréquences pour la caractéristique du climat #6

	Position	Fréquence	Total
Premier tiers	1	-	4
	2	-	
	3	1	
	4	3	
Tiers du milieu	5	1	4
	6	2	
	7	1	
Dernier tiers	8	1	3
	9	-	
	10	1	
	11	1	

- **Analyse des résultats obtenus pour la caractéristique du climat**

Le classement lié à cette caractéristique du climat est mitigé puisque les participants l'ont placée presque uniformément dans les trois tiers du classement. Cela lui a valu un score global relativement élevé de 68 points (pour un score global possible variant entre 11 et 132 points). Malgré certains classements, une grande partie des participants (#4, #5, #6, #8, #9, #10 et #13) a souligné l'importance de cette caractéristique du climat pour influencer la variable dépendante. Le participant #12 a également soulevé l'influence que cette caractéristique pourrait exercer sur la variable dépendante, mais il a nuancé ses propos en tissant des liens entre cette caractéristique et d'autres caractéristiques du climat (cela sera mentionné dans le paragraphe suivant). Par ailleurs, on doit se fier au classement des participants #7, #11 et #14 pour connaître leur avis quant à cette caractéristique du climat. Ainsi, on pourrait croire qu'elle leur est d'importance moindre pour influencer la variable dépendante puisqu'ils l'ont placée dans le tiers du milieu et dans le dernier tiers de leur classement.

Comme mentionné dans l'analyse de la caractéristique du climat #5 (« Adéquation au contexte organisationnel »), certains participants (#6, #9 et #12) ont pensé que cette caractéristique du climat et la caractéristique du climat #5 étaient étroitement liées car elles avaient trait aux processus d'affaires. Le participant #5 a d'ailleurs précisé que cette caractéristique du climat avait plus d'influence sur les employés puisqu'elle touchait davantage leurs activités réalisées au quotidien. Tel qu'il a été évoqué précédemment, on pourrait penser à fusionner ces deux

caractéristiques du climat. D'autre part, le participant #12 a ajouté que cette caractéristique du climat était également liée aux caractéristiques #1 (« Soutien projeté par les gestionnaires »), #2 (« Communication organisationnelle ») et #11 (« Importance réelle accordée à la sécurité de l'information »). D'après lui, s'il y a adéquation aux tâches de la sécurité de l'information, c'est parce que des fonds ont été débloqués pour ce faire, que le changement et sa raison d'être ont été communiqués aux employés, mais surtout parce que la sécurité de l'information est importante au sein de l'organisation. Bien que ces liens soient pertinents, il faut surtout mettre l'accent sur le lien entre cette caractéristique et la caractéristique #5 (« Adéquation au contexte organisationnel »), car si l'on se fie aux propos de plusieurs participants, elles seraient étroitement liées.

Par conséquent, compte tenu de ce classement en demi-teinte et des commentaires qui évoquent le lien étroit de cette caractéristique du climat et de la caractéristique du climat #5 (indiquant une possibilité de les fusionner), un examen global est nécessaire. Cet examen sera présenté à la section 4.3.2.

4.3.1.7 Caractéristique du climat #7 : Engagement organisationnel

CARACTÉRISTIQUE DU CLIMAT #7

Cette caractéristique du climat organisationnel renvoie au lien affectif qui unit les employés à l'organisation.

Plus les employés ont un sentiment partagé d'attachement à l'organisation, plus ils seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, plus un désengagement général est présent, plus les chances sont élevées que les pratiques sécuritaires ne seront pas mises en œuvre.

- **Résultats**

Par l'entremise des classements réalisés par les participants, cette caractéristique du climat a obtenu entre un et 11 points de la part des participants. De plus, aucun participant n'a écarté cette caractéristique du climat de son classement. Des commentaires sur cette caractéristique du climat ont été colligés pour chacun des participants, sauf pour les participants #13 et #14 (dans ces derniers cas, l'absence de commentaires peut s'expliquer par une prise de notes incomplète ou par le silence des participants). Les classements, les points attribués et les commentaires émis relatifs à cette caractéristique du climat figurent dans le tableau 4.48.

Tableau 4.48 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #7

Participant	Classement de la caractéristique (sur 11)	Points attribués	Commentaires sur cette caractéristique
Participant #4	4	4	• « On vient de finir notre sondage d'engagement. [L'engagement] est beaucoup discuté dans l'organisation au point de vue gestion. Si ce n'était pas des employés engagés, je pense que la sécurité ne serait pas le premier des problèmes. […] Une culture d'engagement, c'est d'avoir la volonté que quelque chose de plus gros que nous réussisse. Donc, oui, je pense que je le mettrai quand même assez haut [dans le classement]. Oui, ça, je le mettrais avec implication, l'engagement. » *(lien avec la caractéristique du climat #4)*
Participant #5	2	2	• « Oui, sentiment d'appartenance, c'est un point très important. » • « Je le mettrais même en première position [dans le classement] parce que, même si tu n'as pas nécessairement toutes les formations, la sensibilisation à la sécurité, si tu as un sentiment d'appartenance, tu vas vouloir de facto que l'entreprise soit bien protégée. Tu vas avoir des réflexes, parce que tu vas être engagé. » *(lien avec la caractéristique du climat #3)*
Participant #6	1	1	• « Oui, totalement. C'est super important. L'engagement des gens au niveau de l'organisation. » • « Pour moi, c'est vraiment le premier. Le lien affectif. Dans le fond, l'engagement des employés dans l'organisation. C'est sûr que si tu as un employé qui n'est pas engagé et qui est démobilisé, il se moque un peu qu'on accorde de l'importance à la sécurité. »
Participant #7	9	9	• Selon lui, cette caractéristique du climat devrait avoir un impact important en théorie, mais on ne le remarque pas en pratique.
Participant #8	10	10	• « Effectivement. Sentiment d'attachement à l'organisation. De plus en plus rare, ça. C'est rare que tu rentres à une place et te dire 'Je vais faire 35 ans ici'. Oui, oui. Effectivement. Tu peux être attaché, mais si [la sécurité de l'information] n'est pas importante pour l'entreprise… »
Participant #9	7	7	• « Oui, absolument. J'ai plus intérêt à m'assurer que ma famille est en sécurité à la maison que la famille de mon voisin. Effectivement. » • « Puis [comparée à la caractéristique] #7, en comprenant pourquoi c'est important pour l'entreprise, mais là, ils ont un sentiment d'appartenance, ils vont agir en fonction du bien-être de l'entreprise. Dans une municipalité, tu vas avoir la police qui va être présente pour voir à la sécurité. On ne connaît pas nécessairement les règlements, tous les règlements municipaux, mais on voit que les policiers sont là pour les faire respecter. Et là, on les explique lors d'un conseil municipal. Mais, même si on ne l'explique pas, les policiers l'appliquent et si j'aime ma ville, je veux que tout le monde soit heureux de tout ça. » *(lien avec la caractéristique du climat #11)*

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.48 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #7 (suite et fin)

Participant	Classement de la caractéristique (sur 11)	Points attribués	Commentaires sur cette caractéristique
Participant #10	8	8	• « Oui, c'est vrai. [Mais] je qualifierais ça plutôt de sentiment d'appartenance plutôt que lien affectif. Il faut qu'ils s'identifient à l'organisation. On ne peut pas leur demander qu'ils aiment leurs collègues de travail, mais ils doivent se sentir solidaires et dans le même bateau. »
Participant #11	2	2	• « Lien affectif, travailler ensemble… Je me sens supporté, je me sens pas bullied dans l'entreprise. Absolument. Et ça, c'est encore nécessaire, mais ce n'est pas ça qui fait ton travail. Si tu ne l'as pas, tu ne garderas pas tes employés longtemps. »
Participant #12	8	8	• « Le lien affectif qui unit les employés de l'organisation. Ça, c'est plus du vécu. D'une part, les gens veulent pas se faire pogner, ne veulent pas se faire dire par le groupe de sécurité de l'information… Je voudrais pas pogner un virus parce je sais qu'il y a un peer pressure, là, et ce n'est pas le fun. Tout le monde le sait. Et si tu ne le dis pas, tout le monde va le savoir, ce qui va être pire. Mais l'autre affaire, c'est que tu ne veux pas, parce que toi, tu as fait une niaiserie, tu as cliqué alors que tu n'aurais pas dû, ça pourrait impacter les emplois d'autres personnes et ça va vraiment mal. […] Donc, le peer pressure, ou l'attachement sincère, a un impact… Mais c'est un détail par rapport à tout le reste [des caractéristiques du climat]. »
Participant #13	11	11	• *(Aucun commentaire)*
Participant #14	10	10	• *(Aucun commentaire)*
	Score global =	**72 pts**	

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels présentés dans le tableau 4.48 permettent d'arriver aux fréquences présentées dans le tableau 4.49. Ce tableau montre que quatre participants ont placé cette caractéristique du climat dans le premier tiers du classement, un participant l'a mise dans le tiers du milieu et six autres l'ont fait dans le dernier tiers du classement.

Tableau 4.49 : Tableau des fréquences pour la caractéristique du climat #7

	Position	Fréquence	Total
Premier tiers	1	1	4
	2	2	
	3	-	
	4	1	
Tiers du milieu	5	-	1
	6	-	
	7	1	
Dernier tiers	8	2	6
	9	1	
	10	2	
	11	1	

- **Analyse des résultats obtenus pour la caractéristique du climat**

La majorité des participants a placé cette caractéristique du climat dans le dernier tiers (#7, #8, #10, #12, #13 et #14) et dans le tiers du milieu (étant donné que le participant #9 l'a placée à la septième position) du classement, ce qui lui a valu un score global relativement élevé, soit 72 points (pour un score global possible variant entre 11 et 132 points). Pourtant, malgré ce classement aux extrêmes, les commentaires concernant cette caractéristique du climat étaient globalement positifs. Pour ce qui est des participants #13 et #14, il est nécessaire de se pencher sur leur classement afin de connaître leur avis sur cette caractéristique. En outre, le fait qu'ils l'aient placée dans le dernier tiers de leur classement sous-entend qu'elle est d'importance moindre pour eux.

Les participants #7 et #12 ont questionné l'importance de cette caractéristique du climat. D'une part, le participant #7 a déclaré que cette caractéristique du climat n'aurait de l'impact qu'en théorie. D'autre part, le participants #12 a dit que cette caractéristique du climat pourrait influencer la variable dépendante, mais avec moins d'intensité que les autres caractéristiques du climat.

Tel qu'il a été mentionné dans une autre section, le participant #4 a remarqué l'existence d'un lien entre cette caractéristique du climat et la caractéristique du climat #4 (« Implication des employés »). D'après lui, le lien affectif encourage les employés à se mobiliser et à s'impliquer

dans les processus liés à la sécurité de l'information. De ce fait, on pourrait penser que cette caractéristique du climat influence directement la variable dépendante, contrairement à la caractéristique du climat #4. Pour ce qui est du participant #5, il estimait que la caractéristique du climat #3 (« Soutien à l'apprentissage ») était plus importante que celle-ci puisqu'avec un fort engagement organisationnel, les employés voudront que l'organisation soit protégée, et ce, même s'ils n'ont pas été sensibilisés ou formés à la sécurité de l'information. Quant au participant #9, il a mentionné que cette caractéristique du climat était liée avec la caractéristique du climat #11 (« Importance réelle accordée à la sécurité de l'information »). En effet, si les employés comprennent que la sécurité de l'information est importante au sein de l'organisation, alors ils vont développer un sentiment d'appartenance et agir pour le bien-être de cette dernière, et inversement. Ainsi, il semblerait que les autres caractéristiques du climat soient plus importantes pour influencer la variable dépendante que cette caractéristique.

Ainsi, les classements et les commentaires des participants ont révélé que cette caractéristique était d'importance moindre pour influencer la variable dépendante. En effet, elle a tout d'abord été majoritairement placée dans les deux derniers tiers du classement. De plus, les liens relevés par les participants laissaient entendre que les autres caractéristiques seraient davantage susceptibles d'exercer une influence sur la variable dépendante. Par conséquent, par souci de parcimonie, cette caractéristique n'est pas retenue pour la sélection finale.

4.3.1.8 Caractéristique du climat #8 : Communication des problèmes/erreurs

CARACTÉRISTIQUE DU CLIMAT #8

Cette caractéristique du climat organisationnel réfère à la possibilité de discuter ouvertement dans l'environnement de travail des problèmes/erreurs liés à la mise en œuvre des pratiques de sécurité de l'information.

Plus l'environnement de travail permet de discuter ouvertement des problèmes/erreurs liés à la mise en œuvre des pratiques de sécurité, plus les employés seront enclins à communiquer les problèmes/erreurs rencontrés, le tout favorisant la mise en œuvre de pratiques sécuritaires. À l'opposé, si l'environnement favorise plutôt de ne pas révéler et même de cacher les problèmes/erreurs, moins élevées sont les chances que les employés mettront en œuvre de pratiques sécuritaires.

- **Résultats**

Par l'entremise des classements réalisés par les participants, cette caractéristique du climat a obtenu entre un et neuf points de la part des participants. De plus, aucun participant n'a écarté

cette caractéristique du climat de son classement. Des commentaires sur cette caractéristique du climat ont été colligés pour chacun des participants, sauf pour les participants #7 et #14 (dans ces derniers cas, l'absence de commentaires peut s'expliquer par une prise de notes incomplète ou par le silence des participants). Les classements, les points attribués et les commentaires émis relatifs à cette caractéristique du climat figurent dans le tableau 4.50.

Tableau 4.50 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #8

Participant	Classement de la caract. (sur 11)	Points attribués	Commentaires sur cette caractéristique du climat
Participant #4	2	2	• « Je pense que c'est très important l'ouverture, la transparence, l'honnêteté par rapport à ce qu'on voit, ce qu'on décèle. Il faut que ce soit encouragé. Souvent, la sécurité, c'est qu'on a trouvé un problème, on a trouvé un élément qui fonctionne moins bien, qui porte atteinte à la sécurité. Il faut qu'on ait une culture, faut qu'on ait un climat d'ouverture à retenir cette information pour pouvoir l'adresser directement.»
Participant #5	3	3	• « Totalement d'accord. Parce que si le monde développe justement ce réflexe de parler des éléments non conformes ou des problèmes de sécurité, donc on les encourage… J'imagine que, si on les encourage, on ne les punira pas. On va même les récompenser parce qu'ils ont trouvé, ils ont discuté. […] On peut le voir lorsqu'on parle de déclaration des incidents; il y a beaucoup de bienfaits de déclarer les incidents. Un, ça met en évidence, donc on peut le gérer, on peut l'améliorer. Parce que si on refoule, on va démobiliser, selon moi. Si on ne peut pas parler des problèmes de sécurité, ou si c'est une culture du silence, les personnes vont ruminer et, bien sûr, ils vont garder en tête. […] Je suis 100% d'accord avec ça. » • « Je le mettrais peut-être tout de suite après la caractéristique #7. Donc, le premier qui était un lien affectif, un lien d'attachement à l'entreprise, donc ça, c'est important. Ensuite, qu'on puisse en parler ouvertement quand on trouve des problèmes de sécurité. Ensuite, ça, ça peut venir à être appuyé par des outils en place qui montrent la cohérence. » *(lien avec la caractéristique du climat #7)*
Participant #6	8	8	• « Oui… Ça aussi, c'est vraiment important. C'est sûr que si les gens ont peur de faire état des problèmes ou des erreurs, on ne travaille pas sur l'amélioration dans ce temps-là. C'est tout de suite camouflé, éteint, et on ne travaille pas réellement à s'améliorer. Ça a une influence directe. »
Participant #7	5	5	• *(Aucun commentaire)*
Participant #8	5	5	• « Il y en avait un autre qui lui ressemblait tantôt… 'Discuter ouvertement les problèmes et erreurs'. Ça revient à dire comme tantôt. Tu pointes toujours un coupable ou tu cherches… » *(lien avec la valeur #8)*
Participant #9	9	9	• « Okay. »
Participant #10	3	3	• « Ça, ça s'applique à tout, mais aussi à la sécurité. En temps normal, je mettrais ça à la première place [du classement], l'ouverture de la capacité de discuter ouvertement des problèmes que vous rencontrez, des efforts, etc. » • « Par contre, il ne faut jamais sous-estimer la force du message que la haute direction peut envoyer aux employés. C'est l'affaire la plus importante. Les gens ont naturellement tendance à se tourner vers elle et de prendre tout message qui vient. Mais c'est important ce qui est dit. Donc, c'est pour ça que je mettrais ça en deuxième [position du classement]. » *(lien avec la caractéristique du climat #2)*
Participant #11	1	1	• « Ça, je le vois surtout dans certains ministères, dans certaines entreprises, où tu sens que le chef de tel groupe, tout ce qu'il veut faire, c'est trouver quelqu'un comme responsable du trouble pour pouvoir blâmer. Tu ne te sens pas [forcément] habilité. Tu sens l'épée de Damoclès sur ta tête. Alors le climat de travail [pourrait être négatif]. »

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.50 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #8 (suite et fin)

Participant	Classement de la caract. (sur 11)	Points attribués	Commentaires sur cette caractéristique du climat
Participant #12	9	9	• « Possibilité de discuter ouvertement de l'environnement de travail, des problèmes, erreurs. Un peu comme pour les valeurs, c'était dans le bas. Je comprends que, dans le pire cas, si l'environnement favorise à ne pas révéler et même à cacher les problèmes, moins élevées sont les chances que les employés mettent en œuvre des pratiques sécuritaires. C'est vrai, mais entre cacher des pratiques sécuritaires et s'assurer que les gens sont formés, même pour cacher des problèmes, il faut que tu comprennes le problème. » *(lien avec la valeur #5 et #8)*
Participant #13	6	6	• « Oui, d'accord avec ça. »
Participant #14	3	3	• *(Aucun commentaire)*
	Score global =	**54 pts**	

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels présentés dans le tableau 4.50 permettent d'arriver aux fréquences présentées dans le tableau 4.51. Ce tableau montre que cinq participants ont placé cette caractéristique du climat dans le premier tiers du classement, trois participants l'ont mise dans le tiers du milieu et trois autres l'ont fait dans le dernier tiers du classement.

Tableau 4.51 : Tableau des fréquences pour la caractéristique du climat #8

	Position	Fréquence	Total
Premier tiers	1	1	5
	2	1	
	3	3	
	4	-	
Tiers du milieu	5	2	3
	6	1	
	7	-	
Dernier tiers	8	1	3
	9	2	
	10	-	
	11	-	

- **Analyse des résultats obtenus pour la caractéristique du climat**

Cette caractéristique du climat a fait l'objet d'un classement mitigé puisqu'elle a été placée dans les trois tiers du classement. On note toutefois une légère majorité au niveau du premier tiers du classement. Cela lui a valu un score global relativement faible de 54 points (pour un score global possible variant entre 11 et 132 points). Par contre, malgré ce classement mitigé, aucun des participants n'a exprimé de propos remettant en cause l'influence de cette caractéristique sur la variable dépendante. Au contraire, la plupart des participants ont souligné son importance (#4, #5, #6, #9, #10, #11 et #13), même si certains d'entre eux ont classé cette caractéristique dans le dernier tiers du classement (#6 et #9). En ce qui concerne les participants #7 et #14, il s'avère nécessaire de se pencher sur leur classement afin de connaître leur avis par rapport à cette caractéristique. Ainsi, elle doit leur sembler importante puisqu'ils l'ont classée dans le premier tiers du classement.

Plusieurs liens entre cette caractéristique et d'autres caractéristiques du climat ou des valeurs ont été relevés par quelques participants. Le participant #5 a trouvé que cette caractéristique du climat était liée à la caractéristique #7 car, selon son expérience, il est important d'avoir un lien affectif avec son organisation. Cela faciliterait la communication entre les employés. Les participants #8 et #12 ont mentionné que cette caractéristique du climat était liée à la valeur #8 (« Réaction habituelle de l'organisation face aux problèmes »). Pour le participant #8,

communiquer les problèmes mène ultimement à pointer ou à chercher un coupable. Le participant #12, quant à lui, pensait qu'à l'instar de la valeur #8, cette caractéristique du climat était d'importance moindre. D'après lui, former ses employés (valeur #5 – « Importance accordée au développement des RH ») a un impact plus significatif sur la variable dépendante que de pointer un coupable. Enfin, le participant #10 a souligné le fait que la communication au sein d'une organisation était essentielle. Cependant, la communication de la haute direction (valeur #2 – « Communication organisationnelle ») est la forme de communication la plus importante pour influencer la variable dépendante. L'analyse des liens a révélé que cette caractéristique est d'importance moindre par rapport aux autres caractéristiques. En effet, en examinant les classements de ces participants, on remarque que la caractéristique du climat a toujours obtenu un score plus élevé que les caractéristiques qui lui sont liées, démontrant ainsi sa grande importance.

Bien que les commentaires des participants se sont avérés globalement positifs en ce qui concerne l'importance de cette caractéristique du climat, le constat n'est pas le même pour le classement. En effet, cette caractéristique a été classée dans tous les tiers du classement. D'autre part, les liens établis par les participants ont indiqué qu'elle était d'importance moindre. En raison de l'absence de commentaires négatifs qui pourraient expliquer ce classement mitigé, un examen global est nécessaire. Il sera présenté à la section 4.3.2.

4.3.1.9 Caractéristique du climat #9 : Récompenses/sanctions

CARACTÉRISTIQUE DU CLIMAT #9

Cette caractéristique du climat organisationnel réfère à la façon dont le respect des pratiques de sécurité de l'information est encouragé ou le manque de respect de celles-ci est réprimandé.

Plus l'organisation récompense le respect des pratiques de sécurité de l'information définies, plus les employés seront motivés à mettre en œuvre ces pratiques. Plus l'organisation sanctionne vraiment le non-respect des pratiques de sécurité de l'information, plus les chances sont élevées que les employés mettront en œuvre les pratiques sécuritaires définies.

- **Résultats**

Par l'entremise des classements réalisés par les participants, cette caractéristique du climat a obtenu entre un et 11 points de la part des participants. De plus, aucun participant n'a écarté cette caractéristique du climat de son classement. Tous les participants ont d'autant plus émis des commentaires par rapport à cette caractéristique du climat. Les classements, les points

attribués et les commentaires émis relatifs à cette caractéristique du climat figurent dans le tableau 4.52.

Tableau 4.52 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #9

Participant	Classement de la caract. (sur 11)	Points attribués	Commentaires sur cette caractéristique du climat
Participant #4	7	7	• « Oui. Célébrer nos succès. On entend beaucoup trop parler de dérogation et quand quelqu'un fait la job correctement, le fait bien, on ne le célèbre pas. Je pense que c'est un élément important. » • [ndlr : La chercheure lui demande s'il allait être sanctionné s'il ne respectait pas les règles dans l'organisation du participant.] « Je ne crois pas. Il va peut-être avoir un rapport de vérification qui va sortir. C'est sûr que ça monte à la haute direction. Une sanction? Je ne crois pas. Dans la formule… C'est drôle parce qu'on a eu une discussion récente sur l'ancienne formule qu'on avait quand on faisait partie de [nom compagnie]. Quand on n'était pas sécuritaire, il y avait des sanctions financières; ils demandaient des réserves financières. Il y avait une auto-évaluation qui était faite annuellement. […] C'était vraiment un programme complet sur l'évaluation, comment on traitait les risques. Si les réponses n'étaient pas adéquates, elles étaient évaluées par une tierce partie dans l'organisation, les groupes régionaux et, puis, ils nous demandaient de garder des réserves financières sur le côté pour pallier aux risques. C'était comme ça que [ndlr : nom de sa compagnie] fonctionnait à l'époque. Ce que je trouvais intéressant, c'est que ça forçait une certaine forme de confrontation sur comment on abordait les risques. […] C'était perçu très négativement. Mais pour quelqu'un qui était à l'époque analyste de risque, un peu data geek, et qui regardait ces chiffres-là et qui regardait l'ensemble … le thinking derrière était très intéressant. Ça ne valorisait pas le succès, mais ça sanctionnait une prise de risque inutile. Je pense que [ça fonctionnait], parce qu'à l'époque, […] la sécurité était pire qu'elle était aujourd'hui. […] Donc, est-ce qu'on pourrait argumenter que l'outil provoquait le discours [qui] provoquait la culture de sécurité ? Moi, je pense que oui. […] Il n'y a rien comme jouer dans les poches du monde pour les faire penser. »
Participant #5	3	3	• « Oui, mais c'est très en lien avec préconiser, justement, un environnement de travail où on peut parler des problèmes, des erreurs. Donc, si on peut en parler, j'imagine qu'il n'y a pas justement de sanctions. Donc, ça va de pair avec la caractéristique du climat #8. Je pense qu'elles sont très reliées parce que tu ne peux pas préconiser justement l'ouverture si tu sanctionnes. Ou sinon, c'est inefficace, c'est non-effectif. Donc, je dirais que [les caractéristiques] #8 et #9, je les mettrais ensemble. » *(lien avec la caractéristique du climat #8)*
Participant #6	7	7	• « Oui, c'est super important, c'est sûr. Je ne sais pas dans quelle mesure, par exemple… Si tu récompenses, ça va les inciter et si tu les sanctionnes, ça va les inciter. Moi, ma question, c'est lequel des deux fonctionne le mieux? Je pense que oui, ça a une influence, mais je ne sais pas lequel marche le mieux. »
Participant #7	2	2	• L'importance accordée à la sécurité (caractéristique #11) est la base à partir de laquelle climat #9 et #1 découlent. *(lien avec les caractéristiques du climat #1, #11)*

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.52 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #9 (suite)

Participant	Classement de la caract. (sur 11)	Points attribués	Commentaires sur cette caractéristique du climat
Participant #8	3	3	• « Effectivement… Moins [importante]. » • « Je vais donner un exemple… On a une personne. Je pense qu'on a refait son poste de travail huit fois en dedans de quatre mois parce qu'elle infectait toujours [son poste de travail] avec des virus… À un moment donné, 'Apprenez ou sinon, vous êtes dehors'. Là, tu es obligé de négocier avec son gestionnaire, mais en réalité, ça devrait être… 'Ça fait trois fois qu'on t'attrape et c'est de la négligence'. Il y avait tout un dossier. La personne allait sur des sites qu'elle [n'était pas autorisée à visiter] ou arrivait avec sa clé USB… Elle avait déjà même wipé sa machine pour installer son Windows 10 personnel. […] Mais dans une organisation comme [ndlr : nom de l'organisation qui a racheté la sienne], faire ça, tu es congédié. Ce n'est même pas négociable. Tu altères un équipement informatique pour installer tes propres logiciels? C'est un motif de congédiement. Ici, on va te rencontrer, mais il n'y a pas de sanction. J'ai pas encore de levier pour dire 'Ben là, dans la politique, ça dit que vous ne devez pas altérer, mais il n'y a pas de conséquences'. C'est une règle sans conséquence. Ça va changer complètement. Ça va être un travail sur trois-quatre ans. »

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.52 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #9 (suite)

Participant	Classement de la caract. (sur 11)	Points attribués	Commentaires sur cette caractéristique du climat
Participant #9	10	10	• « Ouais… La caractéristique #9 est importante, c'est-à-dire tu auras beau tout avoir, mais si j'ai des délinquants, et qu'il n'y a aucune conséquence. Regarde, 'Sue me'. C'est un peu ça qu'ils vont dire. » • « J'ai hésité. Pour moi, le principe de récompense n'est pas une bonne chose. Tu ne dois pas agir sécuritairement en espérant qu'on te récompense. Tu agis sécuritairement parce que c'est ça qu'il faut faire. Alors moi, j'ai jamais donné un bonbon à mes enfants, à mon plus vieux, parce qu'il n'a pas battu son petit frère. Je lui ai fait comprendre qu'il ne fallait pas le faire. Alors, c'est pour ça, moi, la récompense, ça peut être pervers au moment où tu cesses de donner la récompense. Là, la pratique va cesser… » *(à propos de la proposition « Récompenses »)* • « Les sanctions… C'est graduel, selon l'importance du non-respect de la règle. Ça peut être une rencontre. Ça peut être une note dans le dossier. Ça peut être une suspension. Ça peut être le renvoi. Ça dépend… Mais encore une fois, la punition va être justifiée selon les climats antérieurs. Alors, si je n'ai pas de culture d'entreprise en sécurité et un climat organisationnel qui reflète l'importance [de la sécurité], l'employé peut me dire 'Mais moi, j'ai aucune espèce de connaissance que c'est important pour toi.' Si je n'ai jamais dit ce qu'il fallait faire, si j'ai les départements qui [sont hostiles] entre eux et disent que la sécurité, c'est de la foutaise et que bon. Alors, je ne peux pas seulement punir ou récompenser. Si je n'explique pas mes attentes [pour les pratiques sécuritaires]… On dit toujours qu'on doit prêcher par l'exemple. Alors, c'est pour ça que, pour moi, [la caractéristique] #11 était plus importante. » *(lien avec les caractéristiques #1 et #11; à propos de la proposition « Sanctions »)* • « Pourquoi j'ai mis [la caractéristique] #9 avant [la caractéristique] #10? C'est que, pour moi, on doit avoir une confiance contrôlée de nos employés, qu'il n'y ait pas une confiance aveugle. » *(lien avec la caractéristique du climat #10)*
Participant #10	5	5	• « Oui. Parfait. Je vais le mettre après [la caractéristique #8], celui-là. C'est quand même proche. » *(lien avec la caractéristique du climat #8)*
Participant #11	5	5	• « La façon dont le respect des pratiques sécuritaires est encouragé ou le manque de respect de celle qui est réprimandée… Donc, ça a rapport à l'imputabilité. C'est l'un égale l'autre. » *(lien avec la valeur #10)*

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.52 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #9 (suite et fin)

Participant	Classement de la caract. (sur 11)	Points attribués	Commentaires sur cette caractéristique du climat
Participant #12	11	11	• « Ça, la définition… Je ne suis pas d'accord. 'La façon dont le respect des pratiques de sécurité est encouragé ou manque de respect de ceci est réprimandé'. […] Finalement, je regarde et je me dis que, par rapport à tout le reste, c'est redondant en quelque part dans tout le reste. Ce n'est pas clair et ça pose des hypothèses avec lesquelles je ne suis pas d'accord. » • « Et on y va avec une double négation parce qu'on dit 'Récompense le respect… Plus les employés seront motivés à mettre en œuvre les pratiques.' En partant, je ne suis pas certain de ça, parce que ça dépend. Comment on récompense? C'est comme le concept d'augmenter le salaire en pensant que personne ne va faire une meilleure job. Non. Ça dure deux mois, ça dure deux semaines. Mais c'est l'inverse. Ils vont mettre quelque chose de plus, ils vont appliquer les pratiques sécuritaires puis, si on récompense le respect, je ne suis pas certain que ça va avoir un impact à moyen terme ou long terme. » *(à propos de la proposition « Récompenses »)* • « Puis si on sanctionne vraiment le non-respect : là, je pense qu'on va tomber dans le règne de la terreur, où les gens vont se rabattre sur la politique en place et vont agir comme des robots. Toutes les politiques, si leur but est juste de les appliquer sans se poser de questions, c'est impossible d'être dans un environnement flexible, agile et qui va s'adapter aux nouvelles réalités. […] Donc, pour celle-là, je suis plus ou moins d'accord. » *(à propos de la proposition « Sanctions »)*
Participant #13	7	7	• « C'est vrai. »
Participant #14	1	1	• Il est d'accord avec la proposition « Récompenses ». • Il ne faut pas trop exagérer avec les sanctions, surtout si on veut encourager la composante « Intelligence » de la variable dépendante. Pour changer un comportement, il faut communiquer, sensibiliser et vérifier l'effet de ces actions plutôt que de sanctionner.
	Score global =	**61 pts**	

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels présentés dans le tableau 4.52 permettent d'arriver aux fréquences présentées dans le tableau 4.53. Ce tableau montre que quatre participants ont placé cette caractéristique du climat dans le premier tiers du classement, cinq participants l'ont mise dans le tiers du milieu et deux autres l'ont fait dans le dernier tiers du classement.

Tableau 4.53 : Tableau des fréquences pour la caractéristique du climat #9

	Position	Fréquence	Total
Premier tiers	1	1	4
	2	1	
	3	2	
	4	-	
Tiers du milieu	5	2	5
	6	-	
	7	3	
Dernier tiers	8	-	2
	9	-	
	10	1	
	11	1	

- **Analyse des résultats obtenus pour la caractéristique du climat**

La majorité des participants a placé cette caractéristique du climat dans le premier tiers (#5, #7, #8 et #14) et le tiers du milieu du classement (#4, #6, #10, #11 et #13), ce qui lui a valu un score global relativement faible, soit 61 points (pour un score global possible variant entre 11 et 132 points). Les commentaires des participants, à l'image de ce classement, étaient pour la plupart positifs. Certains participants (#5, #6, #10, #13 et #14) ont dit que cette caractéristique du climat pourrait influencer la variable dépendante alors que d'autres (#4, #8, #9 et #12) ont nuancé leurs propos. Les participants #4, #8, #9 et #12 ont effectivement déclaré que les récompenses et les sanctions étaient des moyens inefficaces pour motiver les employés à mettre en œuvre des pratiques sécuritaires de manière significative. Les participants #8 et #12 ont également ajouté qu'elles n'avaient de l'effet qu'à court terme. Le participant #8 donne d'ailleurs l'exemple d'un employé de son organisation, qui, malgré s'être fait sanctionné à de multiples reprises, n'a pas respecté les pratiques sécuritaires et a récidivé plusieurs fois. Selon les participants #4 et #9, les sanctions en sécurité de l'information ne sont pas assez sévères (par exemple, des notes dans le dossier, des avertissements par le gestionnaire, etc.) pour avoir un impact significatif sur les employés. Toutefois, ces critiques semblaient sans conséquence car elles se fondaient plutôt sur l'incapacité de leur organisation respective à mettre en œuvre des récompenses ou des sanctions significatives et non pas sur le manque d'influence de cette

caractéristique du climat sur la mise en œuvre de pratiques sécuritaires par les employés. Au final, si on analyse les propos tenus, la plupart affirmaient que cela serait efficace, mais qu'elles ne sont pas systématiquement appliquées. On peut donc affirmer que cette caractéristique semble influencer la variable dépendante.

Le participant #5, quant à lui, a stipulé que cette caractéristique du climat était étroitement liée à la caractéristique du climat #8 (« Communication des problèmes/erreurs »). Selon lui, elles vont de pair puisque l'on ne peut préconiser l'ouverture et la communication si l'on sanctionne ensuite les employés. Les participants #7 et #9, pour leur part, ont fait remarquer qu'à l'instar de la caractéristique du climat #1 (« Soutien projeté par les gestionnaires »), cette caractéristique du climat découlait de la caractéristique du climat #11 (« Importance réelle accordée à la sécurité de l'information »). D'après le participant #9, l'importance accordée à la sécurité de l'information teinte les gestes des gestionnaires, définit et justifie les récompenses et les sanctions aux employés. Ce participant a d'ailleurs ajouté que cette caractéristique était plus importante que la caractéristique du climat #10 (« Façon dont le monitorage du respect des pratiques se fait ») car elle semble plus influente sur la variable dépendante. En effet, pour encourager la mise en œuvre de pratiques sécuritaires, il faut de la confiance, additionnée de mesures de contrôles. En ce qui concernait le participant #10, il a déclaré que cette caractéristique du climat était proche de la caractéristique du climat #8 (« Communication des problèmes/erreurs »). Il n'a pas été davantage explicite à ce sujet, mais on pourrait penser que récompenser ou sanctionner est l'étape suivant la communication de problèmes ou d'erreurs. Ces caractéristiques du climat pourraient donc être indissociables dans certaines organisations. Enfin, le participant #11 a mentionné que l'imputabilité était nécessaire pour savoir qui récompenser ou sanctionner. Ainsi, la valeur #10 (« Imputabilité ») et cette caractéristique du climat sont à niveau égal. En résumé, ces liens ont permis de reconnaître que les récompenses et les sanctions sont susceptibles d'influencer la variable dépendante surtout si elles sont complémentées des autres caractéristiques du climat énumérées ci-dessus.

Avec un classement et des propos globalement positifs quant à l'importance de cette caractéristique, on peut conclure qu'elle semble influencer la variable dépendante. Les commentaires des participants indiquent également que l'influence de cette caractéristique du climat est renforcée si elle est couplée avec certaines autres caractéristiques du climat. De ce fait, elle peut être retenue pour la sélection finale.

4.3.1.10 Caractéristique du climat #10 : Façon dont le monitorage du respect des pratiques de sécurité se fait

CARACTÉRISTIQUE DU CLIMAT #10

Cette caractéristique du climat organisationnel réfère à la façon (confiance et/ou contrôle) privilégiée par l'organisation pour s'assurer du respect des pratiques de sécurité.

Plus l'organisation fait confiance aux employés qu'ils feront tout en leur pouvoir pour protéger l'information, plus ils seront engagés dans la protection de l'information et mettront en œuvre des pratiques sécuritaires. À l'opposé, plus l'organisation fait le monitorage continu du respect des pratiques, moins les employés se sentent responsabilisés et auront plutôt tendance à faire fi des pratiques de sécurité.

- **Résultats**

Par l'entremise des classements réalisés par les participants, cette caractéristique du climat a obtenu entre trois et 11 points de la part des participants. De plus, aucun participant n'a écarté cette caractéristique du climat de son classement. Des commentaires sur cette caractéristique du climat ont été colligés pour chacun des participants, sauf pour les participants #7 (dans ce cas-ci, l'absence de commentaires peut s'expliquer par une prise de notes incomplète ou par le silence du participant) et #12 (dans ce dernier cas, l'absence de commentaires est due au silence du participant). Les classements, les points attribués et les commentaires émis relatifs à cette caractéristique du climat figurent dans le tableau 4.54.

Tableau 4.54 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #10

Participant	Classement de la caract. (sur 11)	Points attribués	Commentaires sur cette caractéristique du climat
Participant #4	8	8	• « Bonne question. Je ne le sais pas. […] En fait, oui, je pense que ça peut avoir un gros impact d'abord. Parce que si c'est fait négativement, surveillance, avec un non-respect, je pense que oui, ça peut avoir un effet sur les pratiques. Ça n'encourage pas d'avoir des pratiques sécuritaires. » • « On est en train de mettre en place des pratiques de surveillance où il va y avoir une forme d'alerte, Les gens vont être au courant. Je suis d'avis que la surveillance pourrait, au contraire, bien faite, véhiculer le bon message. Si on dit aux gens 'On a vu que tu es allé là, fais pas ça', c'est sûr que ça peut avoir une perception négative. Mais si on dit aux gens 'en passant, on a vu ton compte, tu t'es connecté de la France. Es-tu en France?'. Un peu comme Mastercard [et] Visa qui le font quand… Moi, je pense que c'est une belle valorisation, la sécurité, et voir ce qu'on est capable de voir parce qu'on le fait pour le bien-être de la personne et pour le bien-être de l'organisation. Ce n'est pas 'On ne veut pas que tu fasses ça, on ne veut pas que tu te connectes de là, on ne veut pas que tu aies tel comportement'. On voit [ce qu'est] un comportement à risque. » *(à propos de la proposition « Monitorage »)*
Participant #5	11	11	• « Ça… Je ne suis pas trop sûr que ça ait une grosse influence. En fait, c'est un couteau à double tranchant. Si tu mets en place des directives des politiques de sécurité, puis en fait, tu n'as rien pour monitorer, pour avoir des métriques, pour faire le suivi, pour t'assurer que c'est appliqué, ça peut avoir un effet inverse. Dans le fond, les personnes vont dire 'Okay, c'est bien beau toutes ces belles paroles-là dans les politiques, mais vous faites aucun suivi'. Des fois, c'est bien de se faire suivre et dire 'Oh, tu as oublié tel élément'. Donc, là, ça montre un sérieux. Donc, c'est pour ça que je dis que c'est à double tranchant. C'est parce que là, on dit 'Plus l'organisation fait confiance aux employés…', donc en fait, des fois, cette confiance-là, qui implique selon la question peut-être moins de contrôle, peut avoir un effet inverse. » *(à propos de la proposition « Monitorage »)* • « C'est sûr que quand il y a un sentiment de confiance, c'est bien. Mais du contrôle, ça ne veut pas dire qu'on ne fait pas confiance. » *(à propos de la proposition « Confiance »)* • « Je vais le mettre à la fin parce que je pense pas que c'est une question de confiance. Des fois, c'est des obligations qui nous amènent à faire des suivis, justement pour voir si on est conforme, parce que des suivis, du monitoring, ça permet de démontrer notre conformité et aussi permet de voir si notre cadre normatif, nos politiques sont bien en adéquation avec la réalité. Parce que si avec le monitoring, on se rend compte que la majorité du monde ne suit pas les politiques, c'est peut-être qu'il y a un problème dans nos politiques, pas nécessairement au niveau des employés. »
Participant #6	4	4	• « Oui. […] Ça, c'est comme… Justement est-ce qu'on contrôle comme des enfants ou on fait confiance? »
Participant #7	11	11	• *(Aucun commentaire)*

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.54 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #10 (suite)

Participant	Classement de la caract. (sur 11)	Points attribués	Commentaires sur cette caractéristique du climat
Participant #8	9	9	• « Ça revient un peu à ce que je disais tantôt. Il faut que tu les surveilles, mais pas trop. Il faut que tu leur fasses confiance, mais pas trop. C'est une question d'équilibre. »
Participant #9	11	11	• « La [caractéristique] #10, je vais la mettre en bas pour l'instant… » • « On ne peut pas faire une confiance aveugle. Si on informe, on forme, on sensibilise les gens, on va s'attendre à ce qu'ils utilisent de meilleures pratiques sécuritaires, mais on ne peut pas prendre pour acquis que ça va être le cas. Donc, il faut faire du monitoring. » *(à propos de la proposition « Confiance »)* • « Du monitoring, ce n'est pas jouer à la police et essayer de prendre les gens en défaut. C'est de s'assurer que les politiques et les façons de faire sécuritaires sont appropriées. Alors c'est sûr que si le monitoring est vu par les employés comme étant la police, Big Brother, c'est une erreur. Avant de mettre du monitoring, il faut que tu expliques, faut que tu informes, faut que tu sensibilises et que les gens comprennent pourquoi on est là. » *(à propos de la proposition « Monitorage »)* • « Pourquoi j'ai mis [la caractéristique] #9 avant [la caractéristique] #10? C'est que, pour moi, on doit avoir une confiance contrôlée de nos employés. » *(lien avec la caractéristique du climat #9)*
Participant #10	11	11	• « Tu n'as pas le choix d'avoir les mesures de contrôle. Tu peux faire confiance à tes employés, mais tu as quand même des contrôles en arrière. Puis, ce n'est pas nécessairement pour surveiller tes employés… Peut-être que quelqu'un a mis la main sur tes identifiants, puis accède aux ressources de la compagnie. Si je fais de la surveillance sur ton identifiant, ce n'est pas parce que je ne te fais pas confiance, mais c'est parce qu'on n'est pas à toute épreuve. Il ne faut pas que les gens se sentent directement affectés par cette surveillance. On fait de la surveillance qui n'est pas dirigée vers quelqu'un en particulier. On le fait parce qu'il faut le faire. Ce n'est pas incompatible avec la notion de confiance faite aux employés. Dans quelques cas, on ne fait pas confiance aux employés du tout et on fait de la surveillance parce qu'on veut les surveiller, c'est clair. » • « Je mettrais cette caractéristique en dernier. Parce que les gens savent qu'on ne les surveille pas eux, mais l'utilisation des ressources, dans le contexte de sécurité. »
Participant #11	3	3	• « Ça, oui… Confiance [de la part de] l'organisation pour s'assurer du respect des pratiques de sécurité. Mais avant ça, il y a une imputabilité : 'Je sais qu'il y a des conséquences si je le fais pas'. Est-ce que l'entreprise me reconnaît pour utiliser des pratiques sécuritaires? S'il y a un climat qui fait en sorte qu'on te dit 'Hey Good Job… Tu l'as envoyé comme il faut…', tu vas être amené justement à opérer de cette façon-là. » *(lien avec la caractéristique du climat #9 et la valeur #10)*
Participant #12	7	7	• *(Aucun commentaire)*
Participant #13	8	8	• « C'est vrai. »

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.54 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #10 (suite et fin)

Participant	Classement de la caract. (sur 11)	Points attribués	Commentaires sur cette caractéristique du climat
Participant #14	7	7	• Il n'est pas d'accord avec les propositions. • Même raisonnement que pour la croyance #7 (« Le maillon faible en sécurité de l'information »). Le monitoring amène plus de responsabilisation. Si les gens savent qu'ils sont monitorés, ils sont plus responsables et sensibles à avoir un comportement sécuritaire. Par ailleurs, le monitoring ne signifie pas qu'on ne leur fait pas confiance. On leur fait confiance, mais pas à l'aveugle. Il y aura toujours un certain niveau de monitoring, peu importe la confiance qu'on leur fait. *(lien avec la croyance #7, à propos de la proposition « Monitorage »)*
	Score global =	**90 pts**	

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels présentés dans le tableau 4.54 permettent d'arriver aux fréquences présentées dans le tableau 4.55. Ce tableau montre que deux participants ont placé cette caractéristique du climat dans le premier tiers du classement, deux participants l'ont mise dans le tiers du milieu et sept autres l'ont fait dans le dernier tiers du classement.

Tableau 4.55 : Tableau des fréquences pour la caractéristique du climat #10

	Position	Fréquence	Total
Premier tiers	1	-	2
	2	-	
	3	1	
	4	1	
Tiers du milieu	5	-	2
	6	-	
	7	2	
Dernier tiers	8	2	7
	9	1	
	10	-	
	11	4	

- **Analyse des résultats obtenus pour cette caractéristique du climat**

La majorité des participants a placé cette caractéristique du climat dans le dernier tiers (#4, #5, #7, #8, #9, #10, #13) et dans le tiers du milieu (#12 et #14) du classement, ce qui lui a valu un score global relativement élevé de 90 points (pour un score global possible variant de 11 à 132 points). Pour ce qui est des participants #7 et #12, leur classement laissait présager qu'elle était d'importance moindre puisqu'ils l'ont classée dans le tiers du milieu et dans le dernier tiers.

La plupart des critiques des participants étaient en désaccord avec la prémisse de base de cette caractéristique du climat. En outre, leurs critiques visaient principalement les propositions de cette caractéristique du climat : « Plus l'organisation fait confiance aux employés qu'ils feront tout en leur pouvoir pour protéger l'information, plus ils seront engagés dans la protection de l'information et mettront en œuvre des pratiques sécuritaires. À l'opposé, plus l'organisation fait le monitorage continu du respect des pratiques, moins les employés se sentent responsabilisés et auront plutôt tendance à faire fi des pratiques de sécurité. ». En effet, les participants #5, #8, #9 et #10 ont fait remarquer que faire confiance aveuglément aux employés ou les monitorer de manière continu n'avaient pas d'influence sur la mise en œuvre de pratiques sécuritaires. Selon eux, il est nécessaire d'instaurer un équilibre entre ces deux manières de faire si l'on veut influencer les employés. Étant donné que ces propositions n'aient pas d'impact, cela disqualifierait cette caractéristique du climat. Cela pourrait expliquer la raison

pour laquelle ces participants ont principalement placé cette caractéristique dans le dernier tiers du classement.

Des liens avec d'autres caractéristiques ont aussi été identifiés par les participants. Tout d'abord, le participant #9 a mentionné que cette caractéristique du climat était moins importante que la caractéristique du climat #9 (« Récompenses/sanctions »). Selon lui, il est nécessaire de mettre en place des mesures de contrôle, mais ce sont les récompenses ou les sanctions qui auraient une influence significative sur la variable dépendante. Pour le participant #11, pour que cette caractéristique du climat influence la variable dépendante de manière significative, la valeur #10 (« Imputabilité ») et la caractéristique du climat #9 (« Récompenses/sanctions ») doivent au préalable exister dans l'organisation. Enfin, le participant #14 a déclaré que cette caractéristique du climat suivait le même raisonnement que la croyance #7 (« Le maillon faible en sécurité de l'information »). Pour rappel, cette croyance avait trait au rôle que jouait l'être humain dans la sécurité de l'information. En outre, plus on croit que l'humain est le maillon faible en sécurité de l'information, plus les employés seront motivés à mettre en œuvre des pratiques sécuritaires. Ainsi, selon le participant #14, si les employés ont conscience qu'ils sont surveillés par l'organisation, alors ils seraient plus enclins à mettre en œuvre des pratiques sécuritaires. Donc, ce participant était d'accord avec le concept de monitorage, et non avec les propositions formulées. En somme, il semblerait que, dans sa formulation actuelle, cette caractéristique n'a pas de lien avec la variable dépendante. Il est nécessaire que d'autres caractéristiques ou valeurs (telles un système de récompenses et de sanctions ou encore l'imputabilité) soient présentes dans l'organisation pour qu'elle exerce une influence potentielle.

Cette caractéristique du climat semble être d'importance moindre puisque les participants l'ont majoritairement placée dans le dernier du classement et parce que ses propositions se sont avérées être non influentes sur la variable dépendante. Cette influence limitée est d'autant plus notable dans le fait qu'elle ne peut avoir un impact sur la variable dépendante à elle seule. Ainsi, cette caractéristique du climat n'est pas retenue pour la sélection finale.

4.3.1.11 Caractéristique du climat #11 : Importance réelle accordée à la sécurité de l'information

CARACTÉRISTIQUE DU CLIMAT #11

Cette caractéristique du climat organisationnel réfère à l'importance qui est accordée au quotidien à la sécurité de l'information dans l'environnement de travail.

Dans un environnement de travail donné, plus on accorde de l'importance à la sécurité de l'information, plus les employés seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, moins on accorde d'importance à la sécurité de l'information, moins élevées sont les chances que les employés mettent en œuvre des pratiques sécuritaires.

- **Résultats**

Par l'entremise des classements réalisés par les participants, cette caractéristique du climat a obtenu entre un et dix points de la part des participants. De plus, aucun participant n'a écarté cette caractéristique du climat de son classement. Des commentaires sur cette caractéristique du climat ont été colligés pour chacun des participants, sauf pour le participant #14 (dans ce dernier cas, l'absence de commentaires peut s'expliquer par une prise de notes incomplète ou par le silence du participant). Les classements, les points attribués et les commentaires émis relatifs à cette caractéristique du climat figurent dans le tableau 4.56.

Tableau 4.56 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #11

Participant	Classement de la caract. (sur 11)	Points attribués	Commentaires sur cette caractéristique du climat
Participant #4	10	10	• « Je ne suis pas sûr que je le vois tout un ou tout l'autre. » • « On peut avoir trop d'une bonne chose. Plus on accorde de l'importance, on peut en accorder trop aussi. On peut désabuser les gens ou les rendre blasés sur une thématique, si on le fait trop. Il faut trouver la bonne quantité d'informations à donner, la capacité d'absorption. Combien de fois qu'on répète le même message? Est-ce qu'on le complexifie parce qu'il y a plusieurs thématiques à adresser en même temps? Comme ils disent en anglais 'You can't have too much of a good thing'. Donc, c'est un piège. [Il faut] trouver le juste milieu. Pour moi, on pourrait parler de trop de sécurité. Des fois, je pense qu'on le fait aussi. Ça ne nous permet pas d'atteindre nos objectifs pour la culture. Je pense que ça peut avoir l'effet contraire. » *(à propos de la proposition « Importance de la sécurité »)*
Participant #5	7	7	• « Oui, je suis d'accord qu'il faut montrer que c'est important, ça, c'est clair. » • « Dans le fond, pour ce qui est de l'importance dans l'environnement de travail, ça vient rejoindre [les caractéristiques] #1 et #6. Ces deux autres éléments montrent qu'on accorde de l'importance à la sécurité. J'ai comme l'impression que [la caractéristique] #11 est incluse partiellement dans les caractéristiques #1 et #6. C'est pour ça que j'ai de la misère à le positionner. » *(lien avec les caractéristiques du climat #1 et #6)*
Participant #6	2	2	• « Je trouve que c'est important. »
Participant #7	1	1	• C'est la base à partir de laquelle les caractéristiques #1 et #9 découlent. *(lien avec les caractéristiques du climat #1 et #9)*
Participant #8	2	2	• « Oui…»

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Tableau 4.56 : Résultats (classements, points et commentaires) obtenus pour la caractéristique du climat #11 (suite et fin)

Participant	Classement de la caract. (sur 11)	Points attribués	Commentaires sur cette caractéristique du climat
Participant #9	1	1	• « Oui, effectivement. » • « Les caractéristiques du climat #11 et #2… Si l'organisation démontre par ses agissements que la sécurité est importante, même si on n'explique pas tout, on n'explique pas pourquoi, mais si les gens voient que c'est important, ils vont quand même avoir une attitude [sécuritaire]. Si on leur explique pourquoi, ils vont comprendre pourquoi c'est important pour l'entreprise. » *(lien avec la caractéristique du climat #2)* • « [Comparée à la caractéristique] #7, en comprenant pourquoi c'est important pour l'entreprise, ils ont un sentiment d'appartenance, ils vont agir en fonction du bien-être de l'entreprise. Dans une municipalité, tu vas avoir la police qui va être présente pour voir à la sécurité. On ne connaît pas nécessairement les renseignements... Tous les règlements municipaux, mais on voit que les policiers sont là pour les faire respecter. Et là, on les explique lors d'un conseil municipal.» *(lien avec la caractéristique du climat #7)* • Alors, si je n'ai pas de culture d'entreprise en sécurité et un climat organisationnel qui reflète l'importance [de la sécurité], l'employé peut me dire 'Mais moi, j'ai aucune espèce de connaissance que c'est important pour toi.' Si je n'ai jamais dit ce qu'il fallait faire, si j'ai les départements qui [sont hostiles] entre eux et disent que la sécurité, c'est de la foutaise et que bon, etc. Alors, je ne peux pas seulement punir ou récompenser. Si je n'explique pas mes attentes [pour les pratiques sécuritaires]… On dit toujours qu'on doit prêcher par l'exemple. Alors c'est pour ça que pour moi, [la caractéristique] #11 était plus importante. » *(lien avec les caractéristiques #1 et #9)*
Participant #10	4	4	• « Oui, aussi [ndlr : fort importante]. »
Participant #11	7	7	• « Si dans mon environnement de travail, l'importance de la sécurité dans ce que je fais n'est pas caractérisée, puis que je suis laissé à mes propres moyens pour définir les pratiques qui sont plus sécuritaires que d'autres, alors on n'y arrivera pas. Il y a quelqu'un qui s'y connaît plus et qui est capable de dire 'Fais pas ça là, fais ça comme ça'. Mais s'il n'y a personne pour te dire 'Fais ça comme ça', ça devient tough. »
Participant #12	3	3	• « Des fois, il y en a certains qui sont redondants. Je pense au climat, avec la caractéristique #11, on peut déduire [les caractéristiques] #5 et #6. La caractéristique #11 est bien cernée, bien ciblée, [les caractéristiques] #5 et #6 le sont moins, ils ne sont pas aussi pertinents. » *(lien avec les caractéristiques du climat #5 et #6)*
Participant #13	1	1	• « C'est l'une des plus vraies. »
Participant #14	5	5	• *(Aucun commentaire)*
	Score global =	**43 pts**	

Légende : « Citation tirée de la transcription de l'entrevue »; [précision à la citation]; […] : passage omis; *(analyse de la chercheure);* le texte seul indique un passage tiré des notes d'entrevue.

Les classements individuels présentés dans le tableau 4.56 permettent d'arriver aux fréquences présentées dans le tableau 4.57. Ce tableau montre que sept participants ont placé cette caractéristique du climat dans le premier tiers du classement, trois participants l'ont mise dans le tiers du milieu et un autre l'a fait dans le dernier tiers du classement.

Tableau 4.57 : Tableau des fréquences pour la caractéristique du climat #11

	Position	Fréquence	Total
Premier tiers	1	3	7
	2	2	
	3	1	
	4	1	
Tiers du milieu	5	1	3
	6	-	
	7	2	
Dernier tiers	8	-	1
	9	-	
	10	1	
	11	-	

- **Analyse des résultats obtenus pour la caractéristique du climat**

La majorité des participants (#6, #7, #8, #9, #10, #12 et #13) a placé cette caractéristique du climat dans le premier tiers du classement, ce qui lui a valu un score global relativement faible de 43 points (pour un score global variant entre 11 et 132 points). Hormis le participant #4, les participants étaient en général positifs quant à l'influence de cette caractéristique du climat sur la variable dépendante. Quant au participant #14, son classement laissait présumer qu'elle lui était plus au moins importante, puisqu'il l'a placée dans le tiers du milieu de son classement.

Le participant #4 était le seul à avoir critiqué cette caractéristique. Il a apporté une nuance à la proposition suivante : « Dans un environnement de travail donné, plus on accorde de l'importance à la sécurité de l'information, plus les employés seront motivés à mettre en œuvre des pratiques sécuritaires. ». Selon lui, accorder trop d'importance à la sécurité de l'information pourrait avoir un effet néfaste. Son commentaire semblait sans conséquence pour cette analyse car, malgré tout, il ne remettait pas en question l'influence (qu'elle soit positive ou négative) que pourrait exercer cette caractéristique sur la variable dépendante.

D'après les participants #5, #7, #9, et #12, cette caractéristique du climat s'avère être à la base de certaines autres caractéristiques du climat. Et pour cause, les analyses individuelles précédentes ont fait référence à cette caractéristique à plusieurs reprises (lorsque les participants soulevaient les liens entre les caractéristiques). Pour rappel, le participant #5 a

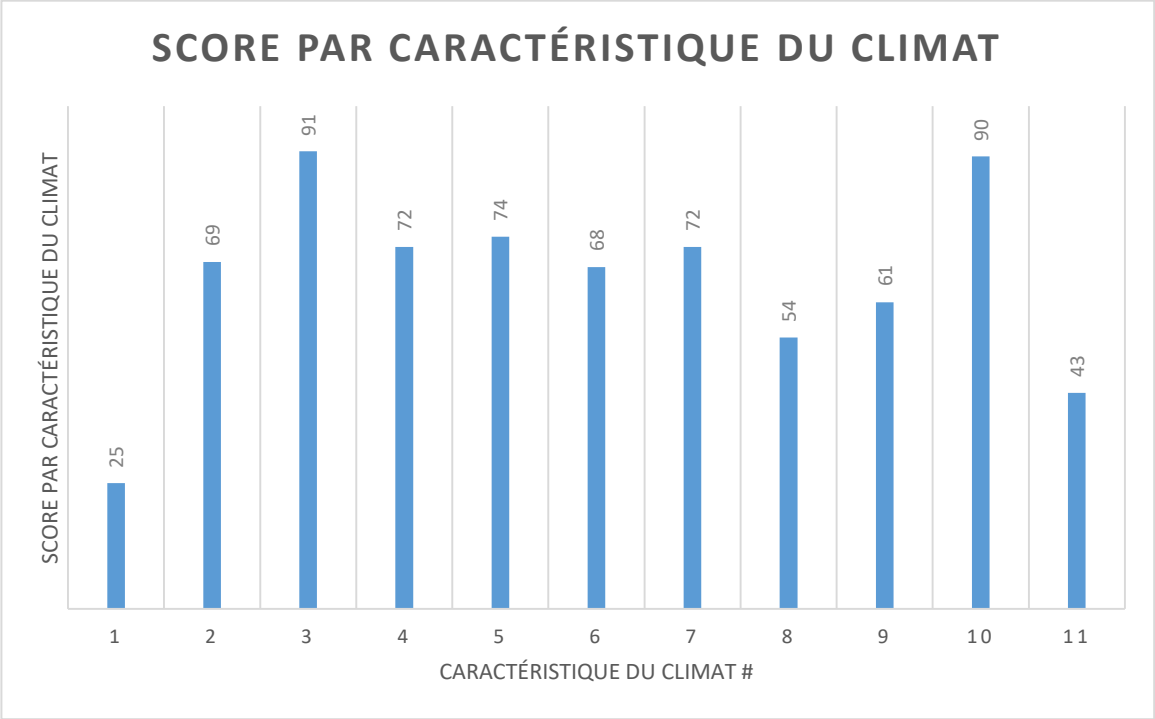
souligné le fait que les caractéristiques du climat #1 (« Soutien projeté par les gestionnaires ») et #6 (« Adéquation aux tâches ») découlaient de cette caractéristique du climat. Les participants #7 et #9 ont, pour leur part, fait remarquer que les caractéristiques du climat #1 (« Soutien projeté par les gestionnaires ») et #9 (« Récompenses/sanctions ») en découlaient. Le participant #9 a notamment déclaré que l'importance accordée à la sécurité de l'information teintait les gestes des gestionnaires et justifiait les récompenses ou les sanctions aux employés. Ce participant a aussi relevé le fait que la caractéristique du climat #2 (« Communication organisationnelle ») était importante pour préciser la position de l'organisation vis-à-vis la sécurité de l'information et, de ce fait, pour influencer la mise en œuvre de pratiques sécuritaires par les employés. Il a également fait le lien entre cette caractéristique du climat et la caractéristique du climat #7 (« Engagement organisationnel »). Selon lui, si les employés comprennent pourquoi la sécurité de l'information est critique pour l'organisation, alors ils se sentiront davantage impliqués dans la mise en œuvre de pratiques sécuritaires, et ce, pour le bien-être de l'organisation. Enfin, le participant #12 a indiqué que les caractéristiques du climat #5 (« Adéquation au contexte organisationnel ») et #6 (« Adéquation aux tâches ») découlaient de cette caractéristique du climat. Tous ces liens ne font que tendre vers la démonstration que l'importance réelle accordée à la sécurité de l'information est une caractéristique-clé du climat, puisqu'elle influencerait tant les autres caractéristiques que la variable dépendante.

En considérant le classement et les commentaires des participants, on constate que l'importance réelle accordée à la sécurité de l'information est une caractéristique primordiale en sécurité de l'information. D'après les participants, elle influence tant la variable dépendante que certaines des autres caractéristiques du climat. Ainsi, elle est retenue pour la sélection finale.

4.3.2 Caractéristiques du climat : Analyse globale et décisions

L'analyse individuelle de chacune des caractéristiques du climat a permis de prendre une décision d'inclusion ou de rejet dans le cas de plusieurs caractéristiques, mais certains résultats plus mitigés nous amènent à conduire une analyse comparative élargie pour voir si les résultats globaux pourraient alimenter notre réflexion. Pour cela, les analyses individuelles de la sous-section précédente ainsi que le score global attribué à chacune des caractéristiques du climat (voir la figure 4.3.) sont utilisés. Il est nécessaire de rappeler que plus le score global d'une caractéristique est faible, plus celle-ci est susceptible d'influencer la variable dépendante d'après les participants.

Figure 4.3 : Score obtenu pour chacune des caractéristiques du climat suite à l'ensemble des classements



Pour rappel, l'analyse individuelle des caractéristiques du climat a permis de retenir les caractéristiques du climat #1 (« Soutien projeté par les gestionnaires »), #2 (« Communication organisationnelle »), #9 (« Récompenses/sanctions ») et #11 (« Importance réelle accordée à la sécurité de l'information »), mais aussi de ne pas conserver les caractéristiques du climat #3 (« Soutien à l'apprentissage »), #4 (« Implication des employés »), #7 (« Engagement organisationnel ») et #10 (« Façon dont le monitorage du respect des pratiques de sécurité se fait »). En conséquence, les caractéristiques du climat (#5, #6, #8) doivent être soumises à un examen global.

La caractéristique du climat #5 (« Adéquation au contexte organisationnel ») a été critiquée car elle n'était pas assez précise pour pouvoir influencer la variable dépendante de manière significative. Elle a néanmoins été confrontée à la caractéristique du climat #6 (« Adéquation aux tâches ») à plusieurs reprises. Selon plusieurs participants, il existerait un lien très étroit entre ces deux caractéristiques du climat. Certains sont même allés jusqu'à suggérer de les fusionner. Puisque l'on vise la parcimonie, il s'avère donc pertinent de suivre cette recommandation étant donné que la formulation des caractéristiques du climat #5 et #6 sont sensiblement les mêmes. Et pour cause, ces caractéristiques s'adressent principalement à l'adaptation des pratiques de sécurité de l'information aux pratiques d'affaires de l'organisation. Ainsi, pour les fusionner, il suffit d'ajouter l'idée principale de la caractéristique

#6 au titre et aux propositions de la caractéristique du climat #5. La nouvelle caractéristique du climat est ainsi présentée dans le tableau 4.58. Cette nouvelle caractéristique du climat fusionnée fera partie de la sélection finale.

Tableau 4.58 : Fusion des caractéristiques du climat #5 et #6

Caractéristiques du climat initiales	Caractéristique du climat fusionnée
Caractéristique du climat #5 : Adéquation au contexte organisationnel **Cette caractéristique du climat organisationnel réfère à l'adéquation (le « fit ») entre les pratiques de sécurité de l'information dans l'organisation et les caractéristiques du contexte organisationnel.** *Plus les pratiques de sécurité de l'information définies sont en adéquation avec les caractéristiques du contexte organisationnel comme la culture et les pratiques d'affaires, plus les employés seront enclins à mettre en œuvre ces pratiques sécuritaires. À l'opposé, s'il y a un « misfit » entre les pratiques de sécurité de l'information et les caractéristiques du contexte organisationnel, plus élevées sont les chances que les pratiques sécuritaires ne seront pas mises en œuvre.*	**<u>Caractéristique du climat A : Adéquation au contexte organisationnel et aux tâches</u>** **Cette caractéristique du climat organisationnel réfère à l'adéquation (le « fit ») entre les pratiques de sécurité de l'information dans l'organisation et les caractéristiques du contexte organisationnel <u>ainsi que les tâches à réaliser.</u>** *Plus les pratiques de sécurité de l'information définies sont en adéquation avec les caractéristiques du contexte organisationnel (la culture et les pratiques d'affaires) <u>et la tâche (effort minimal, impact marginal sur le rendement, etc.)</u>, plus les employés seront enclins à mettre en œuvre ces pratiques sécuritaires. À l'opposé, s'il y a un « misfit » entre les pratiques de sécurité de l'information et les caractéristiques du contexte organisationnel <u>et que les tâches sont alourdies</u>, plus élevées sont les chances que les pratiques sécuritaires ne seront pas mises en œuvre.*
Caractéristique du climat #6 : Adéquation aux tâches **Cette caractéristique du climat organisationnel réfère à l'adéquation (le « fit ») entre les pratiques de sécurité de l'information dans l'organisation et les tâches à réaliser.** *Plus les pratiques de sécurité de l'information définies sont en adéquation avec la tâche (effort minimal, impact marginal sur le rendement, etc.), plus les employés seront enclins à mettre ces pratiques sécuritaires en œuvre. À l'opposé, si les pratiques ajoutent une lourdeur au travail quotidien, plus les chances sont élevées que les pratiques sécuritaires ne seront pas mises en œuvre.*	

Légende : le texte souligné indique ce qui a été modifié dans le texte de nouvelle croyance.

Finalement, l'analyse individuelle de la caractéristique du climat #8 (« Communication des problèmes/erreurs ») s'est également conclue par la nécessité de conduire une analyse globale. Malgré un classement mitigé, les participants ont prononcé des commentaires globalement positifs quant à l'influence de cette caractéristique du climat sur la variable dépendante. En effet, les participants ont avancé l'importance de l'ouverture et de la communication pour signaler les problèmes ou les erreurs en sécurité de l'information. Et pour cause, cela permettrait de prévenir ou de corriger rapidement les potentiels incidents en sécurité de l'information qui pourraient être causés en raison de ces-dits problèmes et erreurs. Toutefois,

les liens soulevés par les participants laissent entendre qu'elle est d'importance moindre par rapport aux autres caractéristiques du climat ou des valeurs (telles que la communication organisationnelle ou l'importance accordée au développement des ressources humaines). Même si elle a obtenu le troisième score global le plus faible parmi toutes les caractéristiques du climat, elle ne peut être conservée pour la sélection finale étant donné que son influence sur la variable dépendante serait moindre et ce, surtout si l'on vise la parcimonie.

En conclusion, à l'issue des résultats et des analyses de ces caractéristiques du climat, les décisions suivantes ont été prises :

- Quatre caractéristiques du climat ont été retenues et seront incluses telles quelles dans la sélection finale :
    - Caractéristique du climat #1 : Soutien projeté par les gestionnaires
    - Caractéristique du climat #2 : Communication organisationnelle
    - Caractéristique du climat #9 : Récompenses/sanctions
    - Caractéristique du climat #11 : Importance réelle accordée à la sécurité de l'information
- Deux caractéristiques du climat ont été fusionnées et la caractéristique du climat qui en résulte sera incluse dans la sélection finale :
    - Caractéristique du climat #5 : Adéquation au contexte organisationnel (non retenue pour la sélection finale)
    - Caractéristique du climat #6 : Adéquation aux tâches (non retenue pour la sélection finale)
    - Leur esprit est fusionné dans la nouvelle caractéristique du climat #A : Adéquation au contexte organisationnel et aux tâches
- Cinq caractéristiques du climat ne sont pas retenues pour la sélection finale :
    - Caractéristique du climat #3 : Soutien à l'apprentissage
    - Caractéristique du climat #4 : Implication des employés
    - Caractéristique du climat #7 : Engagement organisationnel
    - Caractéristique du climat #8 : Communication des problèmes/erreurs
    - Caractéristique du climat #10 : Façon dont le monitorage du respect des pratiques de sécurité se fait

4.4 Résultat final de l'analyse des données

Pour rappel, ce chapitre avait pour objectif d'identifier les croyances, les valeurs ainsi que les caractéristiques du climat les plus susceptibles d'influencer la mise en œuvre de pratiques sécuritaires. À la fin de chacune des sections de ce chapitre, des décisions ont été prises afin de déterminer quels étaient les éléments à retenir, à omettre et à modifier pour la sélection finale d'éléments susceptibles d'influencer la variable dépendante. Ainsi, cette section a pour optique d'offrir un sommaire des décisions qui ont été prises à l'issue des analyses individuelles et globales des croyances, des valeurs et des caractéristiques du climat.

Premièrement, à l'issue des analyses des données individuelles et globales, les décisions suivantes ont affecté la liste initiale de croyance :

- Une croyance a été retenue et sera incluse telle quelle dans la sélection finale :
    - Croyance #3 : Importance générale qu'a la sécurité de l'information dans l'organisation
- Deux croyances ont été fusionnées et la croyance qui en résulte sera incluse dans la sélection finale :
    - Croyance #1 : Responsabilité quant à la sécurité de l'information (non retenue pour la sélection finale)
    - Croyance #2 : Vision de l'organisation quant à la nature des défis en termes de sécurité de l'information (non retenue pour la sélection finale)
    - Leur esprit est fusionné dans la nouvelle croyance #A : Vision de l'organisation quant à la nature des défis et la gestion de la sécurité de l'information
- Quatre croyances n'ont pas été retenues pour la sélection finale :
    - Croyance #4 : Auto-efficacité organisationnelle face aux menaces
    - Croyance #5 : Responsabilité morale de protéger l'information
    - Croyance #6 : Nature générale de l'être humain
    - Croyance #7 : Le maillon faible en sécurité de l'information

Pour ce qui est des valeurs, les décisions suivantes ont été prises suite aux analyses individuelles et globales :

- Six valeurs ont été retenues et seront incluses telles quelles dans la sélection finale :
    - Valeur #2 : Horizon temporel de la planification dans l'organisation
    - Valeur #3 : Prédispositions éthiques de l'organisation

- Valeur #4 : Attitude des employés envers la conformité
- Valeur #5 : Importance accordée au développement des ressources humaines
- Valeur #6 : Attitude générale des employés face au changement
- Valeur #10 : Imputabilité

- Quatre valeurs n'ont pas été retenues pour la sélection finale :
  - Valeur #1 : Bases générales sur lesquelles sont prises les décisions dans l'organisation
  - Valeur #7 : Force du réseau au sein de l'organisation
  - Valeur #8 : Réaction habituelle de l'organisation face aux problèmes
  - Valeur #9 : Réponse habituelle de l'organisation face aux pressions externes

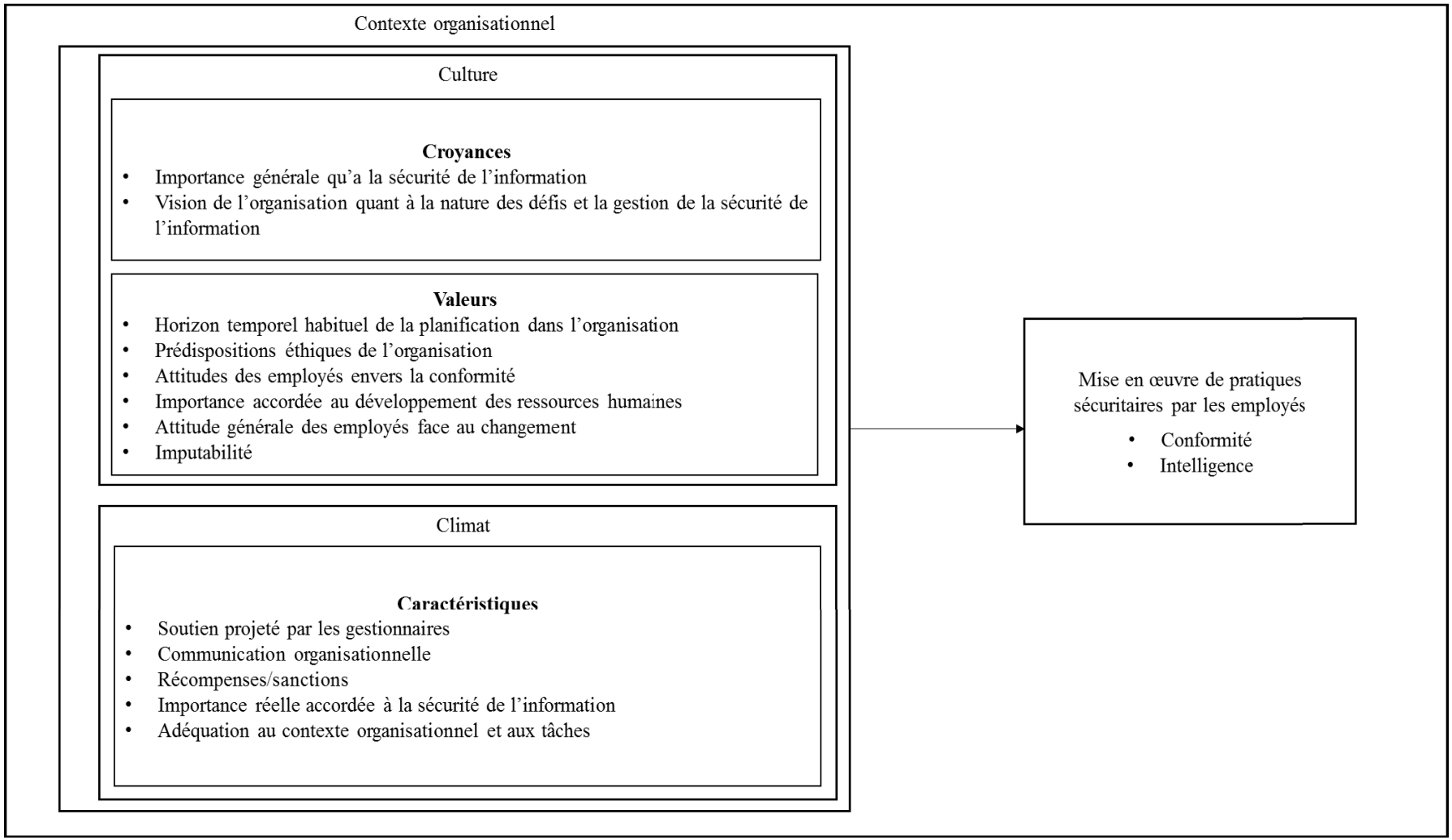
Enfin, les décisions affectant la liste de caractéristiques du climat initiale qui ont été appliquées suite aux analyses individuelles et globales des participants sont les suivantes :

- Quatre caractéristiques du climat ont été retenues et seront incluses telles quelles dans la sélection finale :
  - Caractéristique du climat #1 : Soutien projeté par les gestionnaires
  - Caractéristique du climat #2 : Communication organisationnelle
  - Caractéristique du climat #9 : Récompenses/sanctions
  - Caractéristique du climat #11 : Importance réelle accordée à la sécurité de l'information
- Deux caractéristiques du climat ont été fusionnées et la caractéristique du climat qui en résulte sera incluse dans la sélection finale :
  - Caractéristique du climat #5 : Adéquation au contexte organisationnel (non retenue pour la sélection finale)
  - Caractéristique du climat #6 : Adéquation aux tâches (non retenue pour la sélection finale)
  - Leur esprit est fusionné dans la nouvelle caractéristique du climat #A : Adéquation au contexte organisationnel et aux tâches
- Cinq caractéristiques du climat ne sont pas retenues pour la sélection finale :
  - Caractéristique du climat #3 : Soutien à l'apprentissage
  - Caractéristique du climat #4 : Implication des employés
  - Caractéristique du climat #7 : Engagement organisationnel
  - Caractéristique du climat #8 : Communication des problèmes/erreurs

- Caractéristique du climat #10 : Façon dont le monitorage du respect des pratiques de sécurité se fait

Au final, les propos des 11 participants ont permis de cibler les croyances, les valeurs et les caractéristiques du climat les plus susceptibles d'influencer la variable dépendante, à savoir deux croyances, six valeurs ainsi que cinq caractéristiques du climat. Par conséquent, 13 éléments du contexte organisationnel en sécurité de l'information ont été retenus sur les 27 éléments initiaux. Les décisions prises à l'issue de ces analyses ont conduit au remaniement du modèle représentant les sources d'influence de la mise en œuvre de pratiques sécuritaires par les employés, qui avait été introduit dans le chapitre 2. En outre, la figure 4.4 représente une mise à jour du modèle initial et la sélection finale des croyances, des valeurs et des caractéristiques du climat les plus susceptibles d'influencer la variable dépendante.

Figure 4.4 : Les principales sources d'influence du contexte organisationnel sur la mise en œuvre de pratiques sécuritaires – modèle final



Chapitre 5 : Discussion

Cette étude a été conduite afin d'approfondir la compréhension des construits de la culture et du climat de la sécurité de l'information, qui, malgré la criticité de la sécurité de l'information dans les organisations à l'heure actuelle, ne sont pas encore maîtrisés. En recueillant et en analysant les propos de 11 professionnels en sécurité de l'information, il a été possible de répondre aux deux questions de recherche au cœur de ce mémoire. Elles visaient notamment à déterminer, avec complétude et parcimonie, les éléments de la culture et du climat organisationnels qui sont les plus susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés dans l'organisation.

Ce chapitre a pour but, grâce aux résultats de l'étude, de présenter des pistes de réflexion afin d'enrichir les connaissances sur les construits de la culture et du climat de la sécurité de l'information. Il vise à mieux comprendre la culture et le climat de la sécurité de l'information en présentant, dans un premier temps, les éléments ayant été retenus dans le modèle final de l'étude, et ensuite, les éléments qui n'ont pas été conservés. Il a également pour but de comparer les résultats obtenus au chapitre 4 avec ce qui a été énoncé dans la littérature et recensé au chapitre 2. En somme, le présent chapitre offre des pistes de réflexion permettant d'enrichir la connaissance des construits de la culture et de climat de la sécurité de l'information.

5.1 Vers une meilleure compréhension de la culture et du climat de la sécurité de l'information

Lors des entrevues individuelles, les participants ont pu prendre connaissance des croyances, des valeurs et des caractéristiques du climat de la sécurité de l'information présentées dans la littérature. Bien que les participants étaient d'accord avec plusieurs d'entre elles, ils en ont aussi contesté d'autres car, de leur point de vue, ce qui a été dit dans la littérature n'était pas en adéquation avec la pratique. Cette section met en relief les similarités ou les différences entre la littérature et les résultats des entrevues.

5.1.1 Éléments de la culture et du climat organisationnels retenus

Cette sous-section a pour objectif de comparer les éléments conservés et figurant dans le modèle final de l'étude.

- **Croyances**

Parmi toutes les croyances tirées de la littérature, les résultats ont permis de cibler les deux croyances les plus susceptibles d'expliquer l'influence du contexte organisationnel sur la mise

en œuvre de pratiques sécuritaires par les employés : « Importance générale qu'a la sécurité de l'information dans l'organisation » et « Vision de l'organisation quant à la nature des défis en termes de sécurité de l'information ». Ici, il s'avère intéressant de mettre en lumière les commentaires des participants, car ils appuient ce qui est énoncé dans la littérature.

La première croyance qui a été retenue pour la sélection finale, « Importance générale qu'a la sécurité de l'information », est considérée comme (1) étant la croyance de base par les participants et (2) une source d'influence significative pour la mise en œuvre des pratiques sécuritaires par les employés d'une organisation. Ces deux idées rappellent d'ailleurs ce qu'ont stipulé Ross (2011) et Ruighaver et al. (2007) dans leur étude respective. Pour ces auteurs, il est crucial que les employés d'une organisation croient que la sécurité de l'information est importante pour comprendre la raison d'être de leurs actions et pour les inciter à agir de manière sécuritaire. Il incombe donc aux responsables de la sécurité de l'information de faire valoir, au sein de l'organisation, l'importance de la sécurité de l'information. En effet, ils sont les premiers ambassadeurs de l'organisation dans le domaine et se doivent d'agir comme leaders en ce sens afin d'inculquer aux employés la croyance de l'importance de la sécurité de l'information et de les inciter à mettre en œuvre des pratiques sécuritaires. D'ailleurs, plusieurs participants lors des entrevues ont spécifié la manière dont doit être véhiculée l'importance de la sécurité de l'information au sein d'une organisation. Ces commentaires concordent également avec ce qui a été déclaré par les auteurs dans la littérature. Selon Knapp & Ferrante (2014), Schlienger & Teufel (2002) ainsi que Ruighaver et al. (2007) et certains des participants à l'étude, l'importance accordée à la sécurité de l'information doit provenir de la haute direction et doit être communiquée à l'aide de messages à l'ensemble de l'organisation ou par l'entremise de gestes posés par l'organisation et les gestionnaires qui la représentent. Ainsi, les propos émis par ces auteurs et ces participants laissent entendre que cette croyance exercerait une influence majeure sur la mise en œuvre de pratiques sécuritaires par les employés, mais aussi sur d'autres éléments du contexte organisationnel puisque la communication et le soutien offerts par les gestionnaires sont des caractéristiques du climat en sécurité de l'information.

En ce qui concerne la deuxième croyance ayant été conservée pour la sélection finale, « Vision de l'organisation quant à la nature des défis et à la gestion de la sécurité de l'information », elle est le fruit d'une fusion entre les croyances « Responsabilité d'assurer la sécurité de l'information » et « Vision de l'organisation quant à la nature des défis en termes de sécurité de l'information ». La grande majorité des participants a observé que, dans leur organisation respective, la sécurité de l'information était perçue tel un enjeu holistique, qui ne concerne plus uniquement le département informatique, mais tous les employés de l'organisation. Cela rejoint

ce qui a été dit dans la littérature puisque Alhogail (2015), Dhillon et al. (2006), Flores & Ekstedt (2016) et Mishra (2015) stipulent que la sécurité de l'information doit être une responsabilité collective et doit être considérée comme étant à la fois un problème humain et technique afin de se prémunir contre les menaces du domaine. Cela démontre que les organisations, comme l'explique la littérature, ont réussi à évoluer de concert avec le profil des menaces, qui vise désormais en priorité les humains. Il demeure cependant des exceptions où certaines organisations perçoivent encore la sécurité de l'information comme un enjeu technique qui est exclusivement confié au département informatique. Toutefois, pour les participants, cette croyance était une source d'influence très importante sur la mise en œuvre de pratiques sécuritaires par les employés. C'est pourquoi certains d'entre eux ont admis le besoin de changer le paradigme dans lequel se trouvait leur organisation respective. Les professionnels en sécurité de l'information sont conscients de l'évolution des menaces, mais cette croyance est encore ancrée dans les directions d'un certain nombre d'organisations qui persistent à croire que la sécurité de l'information est un enjeu purement technique.

- **Valeurs**

À l'instar des croyances, l'analyse du chapitre 4 a permis de sélectionner les valeurs qui étaient les plus susceptibles d'expliquer l'influence du contexte organisationnel sur la mise en œuvre de pratiques sécuritaires par les employés, la variable dépendante au cœur de ce mémoire. Ainsi, les valeurs « Horizon temporel de la planification dans l'organisation », « Prédispositions éthiques de l'organisation », « Attitudes des employés envers la conformité », « Importance accordée au développement des ressources humaines », « Attitude générale des employés face au changement » et « Imputabilité » sont celles qui ont été retenues. Comme dans la section précédente, les propos tenus par les participants seront rapportés ici afin de souligner leur concordance avec la littérature.

Premièrement, ce que les participants ont mentionné par rapport à la valeur « Horizon temporel de la planification dans l'organisation » s'accordait avec ce qui a été exposé dans la littérature. En effet, tout comme le dénotent Chang & Lin (2007), les participants ont rapporté l'importance de planifier dans un horizon à court et à long termes en sécurité de l'information. La littérature offre différentes perspectives par rapport à ce sujet et ces perspectives ont évolué dans le temps. D'une part, la planification à long terme permet d'assurer un environnement organisationnel respectant un seuil minimal de sécurité de l'information, car elle laisse le temps aux organisations de mettre en place les moyens adéquats qui pourraient encourager les employés à mettre en œuvre des pratiques sécuritaires (Thomson & Von Solms, 2005). D'autre part, dans les premiers écrits sur la sécurité de l'information, la planification à court terme était

perçue de manière négative (Chia et al., 2002), car elle était signe de laxisme et de budgets limités alloués à la gestion de la sécurité de l'information. Néanmoins, dans la pratique, il semblerait que la planification à court terme soit désormais considérée comme étant vitale en sécurité de l'information puisqu'elle permet de répondre aux éléments perturbateurs en sécurité de l'information (par exemple, une brèche de données ou une indisponibilité de services momentanée, etc.). Ainsi, pour mener à bien la gestion de la sécurité de l'information et pour encourager les employés à mettre en œuvre des pratiques sécuritaires, les professionnels du domaine doivent veiller à conduire des analyses dans un horizon à long et à court termes.

Deuxièmement, le constat est le même pour la valeur « Prédispositions éthiques de l'organisation » étant donné que les propos des participants ont soutenu le contenu de la littérature. En effet, dans l'étude de Dhillon & Torkzadeh (2006), il a été montré que l'éthique ne pourrait qu'avoir une influence positive sur les comportements des employés. Les participants ont appuyé les dires de ces auteurs sur ce dernier point et ont même ajouté que l'éthique était un pilier en sécurité de l'information et qu'elle permettait de rehausser les gestes des employés afin qu'ils mettent en œuvre des pratiques sécuritaires. Par conséquent, il relève de la responsabilité des gestionnaires en sécurité de l'information de s'assurer que les employés de leur organisation comprennent le code d'éthique et de déontologie en vigueur dans l'organisation et y adhèrent pour qu'ils soient plus enclins à mettre en œuvre des pratiques sécuritaires.

La valeur « Attitudes des employés envers la conformité » a également fait consensus entre les participants et la littérature. Selon Williams et al. (2014), la conformité des employés aux règles et aux politiques de sécurité de l'information est cruciale pour un environnement sécuritaire. Les propos des participants concordaient avec ce dernier point puisque pour eux, la conformité était un pilier en sécurité de l'information. Sans cette valeur, les autres valeurs influençant la sécurité de l'information n'auraient aucune utilité. D'ailleurs, Lim et al. (2010) ont relevé le fait que les employés adhéraient aux politiques de sécurité de l'information si la haute direction considérait que la sécurité de l'information était importante. Cette idée a également été exprimée par les participants, mais il est important de tisser un lien avec l'une des croyances qui ont été retenues pour la sélection finale : « Importance générale accordée à la sécurité de l'information ». Ainsi, si les employés croient que la sécurité de l'information est importante et qu'ils ont un rôle à jouer, alors ils auront davantage tendance à respecter les politiques de sécurité de l'organisation et, par conséquent, à mettre en œuvre des pratiques sécuritaires. Les professionnels de la sécurité de l'information pourraient donc véhiculer la croyance que la

sécurité de l'information est importante pour inciter les employés à mettre en œuvre des pratiques sécuritaires.

Ensuite, les résultats liés à la valeur « Importance accordée au développement des ressources humaines » appuient également ce qui a été dit dans la littérature. En effet, certains auteurs ont remis en question l'efficience des programmes de sensibilisation ou de formation, car les employés sont encore la principale source des incidents de sécurité de l'information malgré l'offre de nombreux programmes du genre dans les organisations (Da Veiga & Martins, 2015; Van Loenen, 2015). Généralement, ces programmes ne couvrent que les rudiments de la sécurité de l'information (par exemple, créer un mot de passe qui soit fort, verrouiller son ordinateur quand on quitte son poste de travail, etc.). Ils ne permettent pas d'outiller suffisamment les employés dans leur mise en œuvre de pratiques sécuritaires. D'après certains participants, il est nécessaire d'offrir aux employés des programmes de formation plus spécialisés, qui ciblent des problèmes de sécurité en particulier (par exemple, la correction de vulnérabilités de Windows 10, les failles de sécurité des services infonuagiques, etc.). Toutefois, ces programmes se rapportent plutôt à l'aspect technique de la sécurité de l'information et ne répondent ni à tous les besoins des employés en termes de sécurité de l'information et ne respectent pas non plus les habiletés de chacun à s'approprier des concepts parfois relativement techniques. Par exemple, un employé du département de marketing ne possèderait ni les connaissances ni le jargon nécessaires pour comprendre les concepts techniques exposés dans ces programmes de formation. Il serait donc plus judicieux d'adresser ces programmes de formation plus techniques aux employés de l'équipe de sécurité de l'information et d'en créer de plus conviviaux et accessibles pour les autres employés. De plus, ces programmes de formation contribueraient davantage à la deuxième composante de la variable dépendante, à savoir l'intelligence. En effet, ils visent à enrichir les connaissances, permettant aux employés de développer des réflexes et d'agir de manière éclairée en sécurité de l'information.

Pour ce qui est de la valeur « Attitude face au changement », les participants ont assuré qu'elle était très importante, car la sécurité de l'information est un domaine qui évolue perpétuellement. Il est donc nécessaire que l'organisation adapte ses nouvelles façons de faire et ses politiques de sécurité de l'information afin de se protéger face aux menaces émergentes en sécurité de l'information. Selon les participants, cela faciliterait la mise en œuvre de pratiques sécuritaires. D'ailleurs, ces observations vont directement dans le sens de celles mentionnées par Chia et al. (2003), Da Veiga et al. (2013) ainsi que par Rantos et al. (2012).

Ces auteurs affirment que l'ouverture au changement permet à l'organisation de bénéficier d'une plus grande marge de manœuvre afin de se protéger contre les menaces.

Enfin, la dernière valeur, qui a été conservée pour la sélection finale « Imputabilité », montre également l'accord entre les propos des participants et ce qui a été relevé de la littérature. D'après les participants, Mishra et al. (2015) ainsi que Tang et al. (2016), l'imputabilité exerce une influence considérable sur les employés dans leur mise en œuvre de pratiques sécuritaires. Puisque les participants ont perçu cette valeur comme étant un pilier dans le contexte organisationnel, il s'avère important que les professionnels en sécurité de l'information y prêtent une grande attention à cette valeur. En effet, l'organisation doit faire comprendre à ses employés qu'ils ont une part de responsabilité en sécurité de l'information et qu'ils doivent être conscients des conséquences possibles d'un manquement aux politiques de sécurité de l'organisation.

- **Caractéristiques du climat**

Enfin, les caractéristiques du climat les plus susceptibles d'influencer la mise en œuvre de pratiques sécuritaires ont été identifiées à l'issue du chapitre précédent. Ces caractéristiques du climat sont les suivantes: « Soutien projeté par les gestionnaires », « Communication organisationnelle », « Récompenses/sanctions », « Importance réelle accordée à la sécurité de l'information », « Adéquation au contexte organisationnel et aux tâches ». Dans cette sous-section, il sera également question de mettre en lumière les propos des participants et de les confronter à la littérature.

La première caractéristique du climat ayant été conservée pour la sélection finale est « Soutien projeté par les gestionnaires ». Ici, les propos des participants étaient en concordance avec ce qui a été exprimé dans la littérature. En effet, si les gestionnaires ont tendance à montrer leur appui à la sécurité de l'information, alors les employés seraient plus susceptibles de mettre en œuvre des pratiques sécuritaires puisqu'ils comprendront l'importance qu'a la sécurité de l'information dans leur organisation (Chan et al., 2005; Gaunt, 2000; Hu et al., 2012; Da Veiga et al., 2015). Les propos concordaient avec l'affirmation précédente, mais ont toutefois permis d'apporter plus de précisions quant à cette caractéristique du climat. En effet, d'après les participants, le gestionnaire est un acteur-clé en sécurité de l'information, car il est le lien entre la haute direction et les employés. Par ses gestes, ses paroles, et ses décisions, il illustre au quotidien l'importance accordée à la sécurité de l'information et communique le « walk the talk » de la haute direction.

La caractéristique du climat « Communication organisationnelle » constituait également un point de concordance entre les propos des participants et ce qui est démontré dans la littérature. Nombreux sont les auteurs à avoir évoqué la criticité de la communication organisationnelle lorsque la haute direction exprime ses attentes envers la sécurité de l'information (par exemple, Alhogail, 2015; Bulgurcu et al., 2011; Chen et al., 2015; D'arcy & Green, 2014; Ngo et al., 2005; Tang et al., 2016). Pour l'ensemble des participants, il va de soi qu'une communication organisationnelle claire est extrêmement importante en sécurité de l'information, puisqu'elle permet de diffuser un message précis décrivant les attentes de la direction, les croyances, les valeurs ainsi que les objectifs que l'organisation doit atteindre dans ce domaine. D'ailleurs, la croyance de l'importance accordée à la sécurité de l'information peut être inculquée aux employés via une communication organisationnelle. Celle-ci pourrait ainsi favoriser la mise en œuvre de pratiques sécuritaires par les employés.

Parmi ces caractéristiques du climat qui ont été retenues, « Récompenses/sanctions » en est une sur laquelle les participants ont élaboré et dont les propos permettent d'enrichir la connaissance existante. En effet, dans la littérature, les récompenses et les sanctions sont considérées comme étant des moyens efficaces pour influencer les employés à mettre en œuvre des pratiques sécuritaires (Flores & Ekstedt, 2016; Knapp et al., 2006; Parsons et al., 2015). Néanmoins, aucun de ces auteurs ne spécifie la nature des récompenses et des sanctions en sécurité de l'information. Lors des entrevues, les participants ont pour la plupart donné des exemples de sanctions (par exemple, des notes dans le dossier de l'employé, une rencontre avec le gestionnaire, un licenciement, etc.), car, dans leur organisation respective, les employés étaient rarement récompensés pour avoir respecté les politiques de sécurité. De plus, malgré l'existence de ces sanctions, elles ne sont pas toujours appliquées. Comme l'indiquent Bulgurcu et al. (2010), ces sanctions n'auraient qu'un effet à court terme sur les employés. Par ailleurs, certains participants ont observé l'apparition de nouvelles sanctions : celles imposées par les pairs (par exemple, un employé oubliant de verrouiller son ordinateur lorsqu'il quitte son bureau devra offrir un café à chacun de ses collègues). La littérature existante ne mentionne pas ce type de sanction. On pourrait donc se demander si elles auraient réellement un impact sur les employés.

De plus, la caractéristique du climat « Importance réelle accordée à la sécurité de l'information » est également marquée par la concordance entre ce qui a été mentionné par une grande majorité des participants et la littérature. Pour une grande partie des chercheurs en sécurité de l'information et des participants, l'importance réelle accordée à la sécurité de l'information est vitale pour la mise en œuvre de pratiques sécuritaires par les employés (Chan

et al., 2005; D'Arcy & Green, 2014; Bakari et al., 2007; Martins & Eloff, 2002). Néanmoins, les participants ont soulevé un point très intéressant : l'importance accordée à la sécurité de l'information pourrait avoir un effet à double tranchant. En effet, si l'organisation semble accorder trop d'importance à la sécurité de l'information et le répète constamment aux employés, cela peut les ennuyer au point de les rendre imperméables aux enjeux de sécurité de l'information. À un certain point, une trop grande quantité d'information finit par être ignorée. Selon les participants, il s'avère donc judicieux que l'organisation dose les communications aux employés concernant l'importance qu'elle accorde à la sécurité de l'information pour éviter de complexifier le message que veut communiquer la haute direction et de désengager les employés.

Enfin, pour ce qui est de la caractéristique du climat « Adéquation au contexte organisationnel et aux tâches », les connaissances à en retirer sont minimes puisque les propos des participants étaient parfaitement en accord avec ce qui a été stipulé par les auteurs dans la littérature. Pour Chang et al. (2007), Flores & Ekstedt (2016), Helokunnas & Kuusisto (2003) ou encore Mishra (2015) ainsi que pour les participants, la sécurité de l'information doit être adaptée au contexte organisationnel et incorporée dans les tâches de façon à être en adéquation avec les processus d'affaires de l'organisation. De plus, les participants ont précisé que l'organisation doit porter son attention sur l'adéquation au contexte organisationnel et aux tâches, car cela éviterait aux employés de déployer des efforts supplémentaires dans la réalisation de leurs activités.

5.1.2 Éléments de la culture et du climat organisationnels non retenus

À l'issue du chapitre 4, des éléments du contexte organisationnel ont été retenus pour la sélection finale, mais d'autres ont aussi été rejetés. Par conséquent, cette sous-section a pour but de présenter certains de ces éléments.

- **Croyances contestées par les participants**

Le chapitre 4 a permis d'aboutir au rejet de la sélection finale des croyances suivantes : « Auto-efficacité organisationnelle face aux menaces », « Responsabilité morale de protéger l'information », « Nature générale de l'être humain », « Le maillon faible en sécurité de l'information ». De ce groupe de croyances, « Responsabilité morale de protéger l'information » et « Le maillon faible en sécurité de l'information » représentent des cas particulièrement intéressants, car lorsqu'était venu le temps de les commenter, les participants ont tenu un discours contraire à la littérature. C'est pour cette raison que seules ces deux dernières croyances sont présentées dans les lignes suivantes.

La croyance « Responsabilité morale de protéger l'information » a été omise de la sélection finale, car selon certains participants, elle n'existerait pas en pratique. La responsabilité morale en sécurité de l'information serait apparente lorsque les employés sont conscients de la responsabilité organisationnelle d'assurer la sécurité et lorsqu'ils sont sensibilisés à la sécurité de l'information (Faily & Fléchais, 2010). Toutefois, les propos des participants contestaient les affirmations de Faily & Fléchais (2010) puisque certains d'entre eux ont observé que, dans leur organisation, l'information ne serait pas protégée par acquit de conscience. Elle le serait parce que leur organisation doit respecter des normes ou des lois, qui exigent que les données liées aux clients soient protégées. Personne ne peut être contre la vertu, mais les participants affirment que la responsabilité morale est un concept trop abstrait et n'est pas le moteur par lequel passe la protection de l'information dans les contextes organisationnels où ils évoluent. D'autre part, l'un des participants a remarqué que cette croyance relevait davantage de la perspective individuelle qu'organisationnelle. En effet, la responsabilité morale dépendrait plutôt de l'individu. C'est ce dernier qui serait maître de déterminer s'il souhaite aller au-delà de ses responsabilités organisationnelles afin de protéger l'information de son organisation.

De plus, la croyance « Le maillon faible en sécurité de l'information » a également été omise du modèle final. Plusieurs études affirment clairement que les humains sont le maillon fort en sécurité de l'information (Chen et al., 2015; Da Veiga & Eloff, 2007; Vroom & Von Solms, 2004). D'autant plus qu'avec l'augmentation des cyber-attaques ciblant les humains, ces derniers sont perçus comme étant la meilleure ligne de défense face à ces menaces. Pourtant, plusieurs participants ont affirmé que les employés demeureraient toujours le maillon faible de l'organisation en matière de sécurité de l'information. En effet, peu importe le montant alloué aux formations ou aux technologies protégeant l'information, il suffit d'un moment d'inattention pour que les employés commettent une erreur pouvant causer un incident de sécurité de l'information. Par exemple, des employés peuvent cliquer sur un lien malveillant par inadvertance et se faire voler leurs informations personnelles. Ainsi, on peut considérer que l'humain est le maillon faillible de l'organisation en sécurité de l'information, mais qu'il soit faillible ou non, il reste que cela n'a pas d'influence directe sur la variable dépendante d'intérêt.

- **Valeurs contestées par les participants**

Certaines valeurs ont également été omises de la sélection finale suite aux décisions prises à l'issue du chapitre 4. De ce fait, les valeurs « Bases générales sur lesquelles sont prises les décisions dans l'organisation », « Force du réseau au sein de l'organisation », « Réaction habituelle de l'organisation face aux problèmes » et « Réponse habituelle de l'organisation face aux pressions externes » n'ont pas été retenues. À l'instar des croyances, certaines valeurs

trouvaient tant ancrage dans la littérature que dans la pratique, mais elles ont été principalement omises par souci de parcimonie. Ainsi, seules les valeurs « Bases générales sur lesquelles sont prises les décisions dans l'organisation » et « Force du réseau au sein de l'organisation » sont évoquées dans cette section, car les propos des participants qui leur sont rattachés ont permis de mettre en exergue des connaissances additionnelles.

Premièrement, la valeur « Bases générales sur lesquelles sont prises les décisions dans l'organisation » est l'une des valeurs ayant suscité le plus de contestation de la part des professionnels de la sécurité de l'information rencontrés. Pour asseoir des décisions en sécurité de l'information sur des fondements solides, Mishra (2015) préconise l'analyse quantitative plutôt que l'analyse qualitative. Or, les participants ont révélé qu'en sécurité de l'information, l'organisation avait souvent de la difficulté à obtenir de l'information qui soit concrète et assez rigoureuse pour prendre des décisions éclairées. Trop souvent, les mesures et les chiffres qui sont disponibles se limitent au nombre de virus détectés pour une période ou encore au nombre de clics sur des liens malveillants. Ces données sont relativement limitées et ne permettent pas d'appuyer la prise de décision. Ainsi, pour résoudre ce problème, les participants ont déclaré que l'organisation doit allier analyse quantitative et qualitative pour prendre des décisions en sécurité de l'information. En outre, si elle attendait d'avoir accès à des données quantitatives, aucune décision ne serait jamais prise en sécurité de l'information, compte tenu de l'effort considérable à déployer pour les obtenir.

Deuxièmement, la valeur « Force du réseau au sein de l'organisation » a également fait l'objet de contestation parmi les participants. D'un côté, Chia et al. (2003) et Mishra (2015) ont déclaré que la collaboration au sein d'une organisation était nécessaire pour assurer un environnement sécuritaire de l'information. Néanmoins, cette valeur ne serait valide qu'en théorie. En effet, certains participants ont affirmé qu'ils n'avaient jamais observé d'employés qui collaboraient ou discutaient de sujets liés à la sécurité de l'information et donc, qu'il n'y avait aucune chance que le réseau influence la mise en œuvre de pratiques sécuritaires. On peut expliquer le tout par le fait que les employés doivent être formés et sensibilisés à la sécurité de l'information à un niveau avancé pour qu'ils puissent collaborer. C'est pour cela qu'un des participants a fait remarquer que cette valeur ne pourrait être partagée dans l'organisation, en théorie, à cause du niveau de connaissances requis, qu'aux professionnels de la sécurité de l'information eux-mêmes. À la lumière des propos des participants, il semblerait que ce niveau de maturité des organisations (concernant le niveau de connaissances en sécurité de l'information des employés) en sécurité de l'information n'est pas assez élevé pour bénéficier de cette valeur. On pourrait attribuer ce problème à un fait qui a été mentionné un peu plus tôt soit que les

programmes de formation actuellement offerts aux employés sont trop génériques et ne permettent pas aux employés d'atteindre ce niveau de maturité. Ainsi, on pourrait affirmer que pour encourager la force du réseau au sein de l'organisation, il s'avère judicieux d'enrichir les programmes de formation en sécurité de l'information, et de les rendre accessibles pour tous les employés de l'organisation.

- **Caractéristiques du climat contestées par les participants**

Telles les croyances et les valeurs, certaines caractéristiques du climat ont également été omises de la sélection finale. Ces caractéristiques du climat sont les suivantes : « Soutien à l'apprentissage », « Implication des employés », « Engagement organisationnel », « Communication des problèmes/erreurs » ainsi que « Façon dont le monitorage du respect des pratiques de sécurité se fait ». Parmi ces caractéristiques du climat, plusieurs d'entre elles ont été approuvées par les participants et les propos de ces derniers sont venus appuyer ce qui a été énoncé par les auteurs dans la littérature. Cependant, les caractéristiques du climat « Implication des employés » et « Façon dont le monitorage du respect des pratiques de sécurité se fait » sont particulièrement intéressantes, car elles ont fait l'objet de contestations importantes de la part des participants. C'est la raison pour laquelle elles seront traitées dans cette sous-section puisqu'elles permettent d'enrichir la compréhension que l'on a de ces caractéristiques du climat.

D'une part, la caractéristique du climat « Implication des employés » a été rejetée par les participants parce que la majorité d'entre eux l'ont contestée. Pour mieux arrimer la réalité des employés aux pratiques de sécurité, Chen et al. (2015) ou encore Safa et al. (2016) suggèrent d'impliquer tous les employés d'une organisation dans la conception de pratiques sécuritaires ou de programmes de sensibilisation. Néanmoins, les participants ont souligné la difficulté d'impliquer les employés de l'organisation dans l'élaboration et l'évolution des pratiques de sécurité de l'information, surtout dans les grandes organisations. En réalité, selon eux, les employés montrent peu d'intérêt à s'engager et comme cette responsabilité est du ressort du département de la sécurité de l'information, ils peuvent percevoir cette implication comme étant une charge de travail supplémentaire. Certains d'entre eux préféreraient tout simplement ne pas être consultés. Cette caractéristique du climat pourrait avoir été rejetée par les participants parce que leur organisation respective n'adopterait pas la bonne approche pour impliquer les employés en sécurité de l'information. En outre, pour ne pas représenter une charge de travail substantielle, l'implication des employés devrait être volontaire. L'organisation pourrait mettre en place des dispositifs afin de faciliter leur implication. Par exemple, les employés dont la sécurité nuit à leur travail peuvent signaler cet irritant à une

adresse courriel mise à leur disposition à cet effet ou bien une « boîte à idées » pourrait être installée afin de recueillir toute recommandation pouvant faciliter l'intégration entre la sécurité de l'information et les activités des employés.

Enfin, la caractéristique du climat « Façon dont le monitorage du respect des pratiques de sécurité se fait » a été omise de la sélection finale. Dans la littérature, il a été observé que cette caractéristique du climat divisait les auteurs. D'un côté, certains auteurs stipulent que faire confiance aux employés influencerait la mise en œuvre de pratiques sécuritaires par les employés (Batteau, 2011; Lacey, 2010; Mishra 2015). De l'autre côté, d'autres auteurs déclarent simplement qu'en sécurité de l'information, il est nécessaire de contrôler les employés d'une organisation (Alhogail, 2015; Myyry et al., 2009; D'Arcy & Green, 2014). Pour ces derniers, l'organisation doit surveiller ses employés de manière constante afin de les encourager à mettre en œuvre des pratiques sécuritaires. À l'image des auteurs, les participants sont aussi partagés quant au rôle que peut jouer le monitorage au sein d'une organisation. Il a été rapporté que la confiance accordée aux employés en sécurité de l'information pouvait être un « couteau à double tranchant ». En effet, accorder une confiance aveugle sans mettre en place des moyens de contrôle pourrait avoir l'effet inverse. Au vu de l'absence de monitorage, les employés peuvent devenir laxistes dans leur mise en œuvre de pratiques sécuritaires. Au final, il s'avère que l'idéal pour influencer les employés serait l'atteinte d'un juste équilibre entre monitorage et confiance.

En bref, cette section a montré les points concordants et discordants entre les croyances, les valeurs et les caractéristiques de la culture et du climat de la sécurité de l'information relevées dans la littérature et les résultats tirés des données collectées auprès des participants.

Chapitre 6 : Conclusion

Ce mémoire avait pour but d'identifier les éléments du contexte organisationnel susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés. L'atteinte de cet objectif a été rencontrée par l'intermédiaire d'une revue de la littérature et par la rencontre de professionnels en sécurité de l'information expérimentés. Ce chapitre fait office de conclusion en dressant un portrait des résultats obtenus et des contributions. Il offre, en premier lieu, une mise en contexte du mémoire par un bref rappel des questions de recherche, de la démarche méthodologique adoptée ainsi que des principaux résultats. Ensuite, il présente les apprentissages réalisés, desquels découlent plusieurs contributions sur le plan pratique et théorique. Afin de préserver un regard critique quant aux résultats de ce mémoire, les limites de l'approche scientifique adoptée sont exposées. Enfin, ce chapitre se clôt par une discussion des futures perspectives de recherche.

6.1 Rappel des questions de recherche

En exploitant au maximum la connaissance reliée à la culture et au climat de la sécurité de l'information, la revue de la littérature a permis d'enrichir les connaissances du contexte organisationnel en sécurité de l'information. Observant les principes de complétude et de parcimonie, cette conceptualisation, qui inclut les éléments composant une culture et un climat de la sécurité de l'information, a permis de répondre aux questions de recherche suivantes :

1. ***Quels sont les éléments de la culture organisationnelle les plus susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés dans l'organisation?***

2. ***Quelles sont les caractéristiques du climat organisationnel qui sont les plus susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés dans l'organisation?***

6.2 Rappel de la démarche méthodologique adoptée

Pour répondre à ces questions de recherche, la méthodologie employée dans ce mémoire s'est articulée en plusieurs étapes. Premièrement, une revue de la littérature existante a permis d'obtenir un premier regard et de poser les fondements des conceptualisations de culture et de climat de la sécurité de l'information. Cette étape a notamment permis d'élaborer une liste exhaustive de croyances, de valeurs et de caractéristiques du climat de la sécurité de l'information telles que discutées dans la littérature. Deuxièmement, un groupe de discussion auprès de trois professionnels de la sécurité de l'information a été conduit afin de tester et de

s'approprier le protocole avant l'étape de cueillette de données suivante, mais aussi d'apporter un premier éclairage externe sur ces croyances, ces valeurs et ces caractéristiques du climat. Troisièmement, des rencontres individuelles auprès d'un échantillon de 11 professionnels de la sécurité de l'information a permis de confronter leur expérience aux connaissances recueillies dans la littérature. Enfin, l'analyse, à la fois quantitative et qualitative, des résultats de la collecte de données a permis de sélectionner les croyances, les valeurs et les caractéristiques du climat de la sécurité de l'information les plus susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés.

6.3 Synthèse des principaux résultats

Contrairement à ce qu'il a été dit dans la littérature, il n'existe pas de « culture de la sécurité de l'information » ou de « climat de la sécurité de l'information » en tant que tels, mais plutôt une culture organisationnelle et un climat organisationnel qui contribuent ou qui nuisent à la sécurité de l'information. Toutefois, ces termes sont utilisés dans ce mémoire afin d'en alléger la lecture, mais aussi parce qu'ils sont largement utilisés dans la littérature.

Bien que les construits de la culture et du climat de la sécurité de l'information soient considérés comme étant importants par les chercheurs, ils souffrent de l'absence d'une définition claire. Dans ce mémoire, la culture de la sécurité de l'information a été définie comme étant un ensemble de manifestations visibles et invisibles partagées par les membres d'une organisation. Ces manifestations incluent les croyances, les valeurs, les hypothèses, les artefacts et les pratiques formelles et informelles qui influencent les décisions et les comportements des employés quant à la protection de l'information.

Une définition du climat de la sécurité de l'information a également été développée dans le cadre de ce mémoire. Ainsi, le climat de la sécurité de l'information correspond aux perceptions partagées au sein d'une organisation sur les politiques organisationnelles, les règles, les normes et les pratiques, formelles et informelles. Le climat représente les perceptions partagées par les employés à propos de « comment les choses se passent chez nous ».

L'objectif des organisations en matière de sécurité de l'information a également été défini. Ainsi, la variable dépendante au cœur de ce mémoire, soit la mise en œuvre de pratiques sécuritaires par les employés, concerne l'application des mesures permettant de protéger l'information d'une organisation. Elle est composée de la conformité, qui est le respect des pratiques de sécurité de l'information définies par une organisation, ainsi que de l'intelligence, soit le réflexe d'assurer la protection de l'information en jugeant de manière éclairée les activités du quotidien et en prenant, au besoin, les mesures appropriées.

Une conceptualisation de la culture et du climat en sécurité de l'information a également été développée dans le cadre dans ce mémoire. En effet, il était question d'identifier les éléments du contexte organisationnel les plus susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés. Bien qu'une liste exhaustive de croyances, de valeurs et de caractéristiques du climat de la sécurité de l'information ait été réalisée dans ce mémoire, il s'est avéré pertinent de déterminer quelles étaient celles qui étaient les plus susceptibles d'influencer la variable dépendante. En effet, cela constitue un premier pas vers le développement d'un instrument de mesure de la culture et du climat de la sécurité de l'information. Par conséquent, l'analyse des résultats a permis de mettre à jour le premier modèle bâti sur la littérature et ayant subi une première validation par des professionnels en sécurité de l'information et à mettre en exergue les deux croyances, les six valeurs et les cinq caractéristiques du climat les plus susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés.

6.4 Contributions pratiques et théoriques du mémoire

Cette section a pour objectif de présenter les contributions qu'apporte ce mémoire tant à la théorie qu'à la pratique.

6.4.1 Contributions théoriques

Bien que ce sujet ait été abondamment étudié dans la littérature, les écrits s'avèrent anecdotiques et souffrent d'un manque de validation empirique rigoureuse. La contribution première de ce mémoire est donc d'enrichir les connaissances sur la culture et le climat de la sécurité de l'information, sur la base de la littérature existante et des propos des participants.

Les conceptualisations de la culture et du climat de la sécurité de l'information qui figurent dans les écrits scientifiques recensés ne couvrent pas les construits dans leur intégralité et celles-ci sont rarement soumises à un processus de validation. Par conséquent, la conceptualisation de ce mémoire fait l'objet d'un processus de validation rigoureux et aspire à englober les aspects humains, organisationnels et techniques de la culture et du climat de la sécurité de l'information. C'est pourquoi cette étude s'avère être la première à établir une liste exhaustive des éléments du contexte organisationnel (croyances, valeurs et caractéristiques du climat) susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés. À cela s'ajoute le fait qu'elle présente également une liste à la fois complète et parcimonieuse de ces éléments du contexte organisationnel. Au final, ce mémoire représente un premier pas permettant d'alimenter de futures recherches, dont le but sera de développer un instrument de mesure de la culture et du climat de la sécurité de l'information et ensuite, de mesurer

empiriquement l'influence de ces éléments sur la mise en œuvre de pratiques sécuritaires au sein des organisations.

6.4.2 Contributions pratiques

Faute d'instrument de mesure de la culture ou du climat de la sécurité de l'information, les praticiens ont souvent recours à des outils de maturité ou d'évaluation de la sensibilisation, bien que cela ne réponde pas parfaitement à leurs besoins. De ce fait, le modèle conceptuel final peut informer ces professionnels en sécurité de l'information des éléments du contexte organisationnel à prendre en compte et qui sont susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés. De plus, tout en considérant le fait qu'il doit encore franchir plusieurs étapes de validation, ce modèle peut servir aux gestionnaires qui souhaitent avoir une première évaluation de la culture et du climat de la sécurité de l'information de leur organisation. En d'autres termes, elle permet de s'assurer de l'existence d'une croyance, d'une valeur ou bien d'une caractéristique du climat donnée. Ce premier diagnostic pourrait alimenter la réflexion des gestionnaires quant aux éléments du contexte organisationnel dans lesquels ils évoluent et pourrait les assister dans leur mise en place d'un plan d'action visant à développer un contexte organisationnel mieux aligné sur leurs objectifs en matière de sécurité de l'information. Quoique la littérature montre que les changements à la culture ou au climat de la sécurité de l'information sont des projets de longue haleine.

6.5 Limites de la recherche

Ce mémoire possède certaines limites qu'il convient de mentionner afin que le lecteur puisse disposer d'un regard critique sur l'étude en question. En limitant la cueillette de données à 11 participants, la taille de l'échantillon est l'une des principales limites de ce mémoire. On a toutefois bénéficié d'une grande représentativité puisque les participants rencontrés étaient très expérimentés et provenaient de contextes organisationnels forts variés (tant du secteur privé que du secteur public). Malgré la taille modeste de l'échantillon, les propos des participants rencontrés se démarquent par leur grande richesse.

La deuxième limite de ce mémoire concerne la cueillette de données sur le terrain. Chacun des exercices de priorisation n'a pas bénéficié du même soin. Le temps imparti aux rencontres est l'une des raisons de cette limite. Bien que certains des participants aient eu la générosité d'accorder du temps supplémentaire pour leur entrevue, quelques-uns d'entre eux, pressés par le temps, ont réalisé le dernier exercice de priorisation, sans prendre le temps de systématiquement commenter verbalement leurs décisions. Certains des participants ont d'ailleurs avoué que la réalisation de ces exercices était longue. Toutefois, tous les participants

ont pu réaliser les trois exercices de priorisation et les données par elles-mêmes se sont avérées riches compte tenu de leur grande expérience dans le domaine de la sécurité de l'information. Étant donné la longueur de l'entrevue, il va de soi que les propos pris en considération par la prise de notes sont limités, dans les cas où les participants ont refusé de se faire enregistrer.

6.6 Pistes de recherche future

Ce mémoire, qui porte sur l'identification des éléments du contexte organisationnel susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés, contribue à la littérature en sécurité de l'information et laisse envisager plusieurs possibilités de recherches futures.

Les résultats de ce mémoire peuvent être utilisés pour poursuivre le but initial de ce mémoire, qui était le développement d'un instrument permettant d'évaluer l'influence du contexte organisationnel sur la mise en œuvre de pratiques sécuritaires par les employés. En outre, les croyances, les valeurs et les caractéristiques du climat les plus susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés (qui ont été identifiées à l'issue du chapitre 4), pourraient servir de base à cet instrument de mesure. En d'autres termes, on obtiendrait donc un instrument de mesure de la culture et du climat de la sécurité de l'information qui pourrait évaluer ces construits avec complétude et parcimonie.

L'examen des liens entre les éléments du contexte organisationnel pourrait également faire l'objet de recherches futures. En effet, l'analyse conduite au chapitre 4 a permis de mettre en exergue l'existence de plusieurs liens entre les différents éléments de la culture et du climat de la sécurité de l'information. Selon les participants, certains éléments s'influenceraient mutuellement tandis que d'autres pouvaient en influencer plusieurs à la fois. D'autre part, il pourrait aussi s'avérer intéressant d'examiner plus en profondeur l'influence des éléments du contexte organisationnel sur la variable dépendante. En effet, les résultats montrent que les éléments du contexte organisationnel pouvaient influencer soit l'une, soit les deux composantes (conformité et intelligence) de la variable dépendante.

Par ailleurs, ce mémoire s'est principalement concentré sur les croyances et les valeurs, manifestations-clé de la culture organisationnelle, car, selon la littérature, elles exerceraient les influences les plus significatives sur les individus. Il peut dès lors s'avérer pertinent d'étudier l'influence des autres manifestations de la culture (telles que les artefacts, les histoires, etc.) dans le but de comprendre comment elles pourraient influencer la mise en œuvre de pratiques sécuritaires par les employés. Par exemple, les organisations font régulièrement usage d'artefacts (qui se présentent sous la forme de posters, de fournitures de bureau ou encore de

sites Web) afin d'influencer la mise en œuvre de pratiques sécuritaires par les employés. Néanmoins, les organisations demeurent dépourvues d'outils mesurant l'influence réelle de ces artefacts sur la mise en œuvre de pratiques sécuritaires par les employés.

BIBLIOGRAPHIE

Albrechtsen, E. & Hovden, J. (2010). « Improving Information Security Awareness and Behaviour Throuh Dialogue, Participation and Collective Reflection. An Intervention Study », *Computers & Security*, vol. 29, p. 432-445.

Alhogail, A. (2015). « Design and Validation of Information Security Culture Framework », *Computers in Human Behavior*, vol. 49, p. 567-575.

Alnatheer, M., Chan, T. & Nelson, K. (2012). « Understanding and Measuring Information Security Culture », *PACIS 2012 Proceedings*.

Alvesson, M. & Sveningsson, S. (2016). *Changing Organizational Culture: Cultural Change Work in Progress*, vol. 209, Routledge.

Ashkanasy, N., Wilderom, C. & Peterson, M. (2011). *The Handbook of Organizational Culture and Climate*, SAGE Publications, 650 p.

Astakhova, L.V. (2014). « The Concept of the Information Security Culture », *Scientific and Technical Information Processing*, vol. 41, no 1, p. 22-28.

Batteau, A. (2011). « Creating a Culture of Enterprise Cybersecurity », *International Journal of Business Anthropology*, vol. 2, no 2, p. 37-47.

Bauer, S., Bernroider, E. & Chudzikowski, K. (2017). « Prevention Is Better Than Cure! Designing Information Security Awareness Programs to Overcome Users' Non-Compliance with Information Security Policies in Banks », *Computers & Security*, vol. 68, p. 145-159.

Bernard, R. (2007). « Information Lifecycle Security Risk Assessment: A Tool for Closing Security Gaps », *Computers & Security*, vol. 26, no 1, p. 26-30.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). « Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness », *MIS Quarterly*, vol. 34, no 3, p. 523-548.

Campbell, N.R. (1920). Physics: the Elements, London: Cambridge University Press.

Campbell, J.P., Dunette, M.D., Lawler, E.E. & Weick, K.E. (1970). *Managerial Behavior, Performance, and Effectiveness*, McGraw-Hill, 546 p.

Chan, M., Woon, I. & Kankanhalli, A. (2005). « Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior », *Journal of Information Privacy & Security*, vol. 1, no 3, p. 18-41.

Chang, S. & Lin, C. (2007). « Exploring Organizational Culture for Information Security Management », *Industrial Management & Data Systems*, vol. 107, no 3, p. 438-458.

Chen, Y., Ramamurthy, K. & Wen, K.W. (2015). « Impacts of Comprehensive Information Security Programs on Information Security Culture », *The Journal of Computer Information Systems*, vol. 55, no 3, p. 11-19.

Chia, P., Ruighaver, A. B. & Maynard, S. (2002). « Understanding Organizational Culture », *Sixth Pacific Asia Conference on Information Systems Proceedings*.

Dang-Pham, D., Pittayachawan, S. & Bruno, V. (2015). « Investigating the Formation of Information Security Climate Perceptions with a Social Network Analyss: A Research Tool », *Proceedings of the 2015 Pacific Asia Conference on Information Systems (PACIS 2015)*.

Da Veiga, A. & Eloff, J.H.P. (2007). « An Information Security Governance Framework », *Information Systems Management*, vol. 24, no 4, p. 361-372.

Da Veiga, A. & Eloff, J.H.P. (2010). « A Framework and Assessment Instrument for Information Security Culture », *Computers & Security*, vol. 29, p. 196-207.

Da Veiga, A. & Martins, N. (2015). « Improving the Information Security Culture through Monitoring and Implementation Actions Illustrated through a Case Study », *Computers & Security*, vol. 49, p. 162.

Da Veiga, A. & Martins, N. (2015). « Information Security Culture and Information Protection Culture: A Validated Assessment Instrument », *Computer Law & Security Review*, vol. 31, p. 243-256.

Da Veiga, A., Martins, N. & Eloff, J.H.P. (2007). « Information Security Culture - Validation of an Assessment Instrument », *South Africa Business Review*, vol. 11, no 1, p. 147-166.

D'Arcy, J. & Greene, G. (2014). « Security Culture and the Employment Relationship as Drivers of Employees' Security Compliance », *Information Management & Computer Security*, vol. 22, no 5, p. 474-489.

Denison, D.R. (1996). « What Is the Difference between Organizational Culture and Organizational Climate? A Native's Point of View on a Decade of Paradigm Wars. », *Academy of Management* vol. 21, p. 619-654.

Delbecq, A., Van De Ven, A. & Gustafson, D. (1986). *Group Techniques for Program Planning: A Guide to Nominal Group and Delphi Processes*, Green Briar Pr.

Dhillon, G. (1997). *Managing Information System Security*, 1e éd., Macmillan Press, 519 p.

Dhillon, G. & Torkzadeh, G. (2006). « Value-Focused Assessment of Information System Security in Organizations », *Information Systems Journal*, vol. 16, p. 293-314.

Dojkovski, S., Lichtenstein, S. & Warren, M. (2010). « Enabling Information Security Culture: Influences and Challenges for Australian Smes », *21st Australasian Conference on Information Systems Proceedings*.

Drevin, L., Kruger, H.A. & Steyn, T. (2007). « Value-Focused Assessment of Ict Security Awareness in an Academic Environment », *Computers & Security*, vol. 26, p. 36-43.

Dubé, L. & Robey, D. (1999). « Software Stories: Three Cultural Perspectives on the Organizational Practices of Software Development », *Accounting, Management and Information Technologies*, vol. 9, no 4, p. 223-259.

Dzazali, S. & Zolait, A.H. (2012). « Assessment of Information Security Maturity: An Exploration Study of Malaysian Public Service Organizations », *Journal of Systems and Information Technology*, vol. 14, no 1, p. 23-57.

Ericsson, K. & Simon, H. (1980). « Verbal Reports as Data », *Psychological Review*, vol. 87, no 3, p. 215.

Erlich, Z. & Zviran, M. (2010). « Goals and Practices in Maintaining Information Systems Security », *International Journal of Information Security and Privacy (IJISP)*, vol. 4, no 3, p. 40-50.

Faily, S. & Fléchais, I. (2010). « Designing and Aligning E-Science Security Culture with Design », *Information Management & Computer Security*, vol. 18, no 5, p. 339-349.

Fishbein, M. & Azjen, I. (1975). *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*, Addison-Wesley Pub. Co., 578 p.

Flores, W.R. & Ekstedt, M. (2016). « Shaping Intention to Resist Social Engineering through Transformational Leadership, Information Security Culture and Awareness », *Computers & Security*, vol. 59, p. 26-44.

Forehand, G.A. & Von Haller, B. (1964). « Environmental Variation in Studies of Organizational Behavior », *psychological Bulletin*, vol. 62, no 6.

Forrester (2015). *Assess Your Security Program with Forrester's Information Security Maturity Model*, Forrester, 12 p. Consulté le 23 juillet 2016 de https://www.forrester.com/report/Assess+Your+Security+Program+With+Forresters+Information+Security+Maturity+Model/-/E-RES56671

Gartner (2017). « Predicts 2017: Information Security Management ». Gartner. Consulté le 8 mai 2017 de https://www.gartner.com/document/3512935?ref=solrAll&refval=189070760&qid=d4fffb5824e392b33b39586df4e18335

Gaunt, N. (2000). « Practical Approaches to Creating a Security Culture », *International Journal of Medical Informatics*, vol. 60, no 2, p. 151-157.

Ge, X., Yuan, Y. & Lu, L. (2011). « An Information Security Maturity Evaluation Mode », *2011 International Conference on Advances in Engineering Proceedings*.

Goo, J., Yim, M.-S. & Kim, D.J. (2013). « A Path Way to Successful Management of Individual Intention to Security Compliance: A Role of Organizational Security Climate », *Proceedings of the 46th Hawaii International Conference on System Sciences*.

Hänsch, N. & Benenson, Z. (2014). « Specifying It Security Awareness », *Proceedings of 25th International Workshop on Database and Expert Systems Applications*.

Helokunnas, T. & Kuusisto, R. (2003). « Information Security Culture in a Value Net », *IEMC '03 Proceedings*.

Herath, T. & Rao, H. (2009). « Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations », *European Journal of Information Systems*, vol. 18, no 2, p. 106-125.

Holmberg, R. & Sundstrom, M. (2012). « Leadership and the Psychology of Awareness: Three Theoretical Approaches to Information Security Management », *Organization Management Journal*, vol. 9, p. 64-77.

Hu, Q., Dinev, T., Hart, P. & Cooke, D. (2012). « Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture », *Decision Sciences Journal*, vol. 43, no 4, p. 615-659.

Karlsson, F., Astrom, J. & Karlsson, M. (2013). « Information Security Culture – State-of-the-Art Review between 2000 and 2013 », *Information & Computer Security*, vol. 23, no 3, p. 246-285.

Lacey, D. (2010). « Understanding and Transforming Organizational Security Culture », *Information Management & Computer Security*, vol. 18, no 1, p. 4-13.

Litwin, G.H. & Stringer, R.A. (1968). *Motivation and Organizational Climate*, Harvard Business School.

ISACA (2012). *Cobit 5 for Information Security*. Consulté le 20 juillet 2016 de https://www.isaca.org/bookstore/Pages/Product-Detail.aspx?Product_code=WCB5IS

ISECOM (2004). *ISM3 1.0.: Information Security Management Maturity Model*, 72 p. Consulté le 23 juillet 2016 de https://www.lean.org/FuseTalk/Forum/Attachments/ISM3_v2.00-HandBook.pdf

ISO/CEI 27002 (2013). *Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information,* Genève, Organisation internationale de normalisation/Commission électrotechnique internationale, 80p.

Jaafar, N. & Ajis, A. (2013). « Organizational Climate and Individual Factors Effects on Information Security Compliance Behaviour », *International Journal of Business and Social Science*, vol. 4, no 10.

Jalal-Karim, A. (2013). « Evaluating the Impact of Information Security on Enhancing the Business Decision-Making Process », *World Journal of Entrepreneurship, Management and Sustainable Development*, vol. 9, no 1, p. 55-64.

James, L.R. & Jones, A.P. (1974). « Organizational Climate: A Review of Theory and Research », *Psychological Bulletin*, vol. 81, no 12, p. 1096-1112.

Kappos, A. & Rivard, S. (2008). « A Three-Perspective Model of Culture, Information Systems, and Their Development and Use », *MIS Quarterly*, vol. 32, no 3, p. 601-634.

Karokola, G., Kowalski, G. & L., Yngström. (2011). « Secure E-Government Services: Towards a Framework for Integrating It Security Services into E-Government Maturity Models », *ISSA 2011 Proceedings*.

Knapp, K. & Ferrante, C. (2014). « Information Security Program Effectiveness in Organizations: The Moderating Role of Task Interdependence », *Journal of Organizational and End User Computing*, vol. 26, no 1, p. 27-46.

Knapp, K., Marshall, T., Rainer, R. & Ford, F. (2006). « Information Security: Management's Effect on Culture and Policy », *Information and Computer Security*, vol. 14, no 1, p. 24-36.

Koh, K., Ruighaver, A. B., Maynard, S. & Ahmad, A. (2005). « Security Governance: Its Impact on Security Culture », *Proceedings of 3rd Australian Information Security Management Conference*, p. 47-57.

Köne, H. & Eloff, J.H.P. (2002). « Information Security Policy—What Do International Information Security Standards Say? », *Computers & Security*, vol. 21, no 5, p. 401-409.

Kortjan, N. & Von Solms, R. (2014). « A Conceptual Framework for Cyber-Security Awareness and Education in Sa », *South African Computer Journal*, vol. 52, p. 29-41.

Kruger, H.A., Drevin, L. & Steyn, T. (2010). « A Vocabulary Test to Assess Information Security Awareness », *Information Management & Computer Security*, vol. 18, no 5, p. 316-327.

Kruger, H.A. & Kearney, W.D. (2006). « A Prototype for Assessing Information Security », *Computers & Security*, vol. 25, p. 289-296.

Lacey, D. (2010). « Understanding and Transforming Organizational Security Culture », *Information Management & Computer Security*, vol. 18, no 1, p. 4-13.

Larousse (2017). *Le Petit Larousse*, coll. Le Petit Larousse, 2044 p.

Lebek, B., Uffen, J., Neumann, M., Hohler, B. & Breitner, M. (2014). « Information Security Awareness and Behavior: A Theory-Based Literature Review », *Management Research Review*, vol. 37, no 12, p. 1049-1092.

Leidner, D. & Kayworth, T. (2006). « Review: A Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict », *MIS Quarterly*, vol. 30, no 2, p. 357-399.

Lim, J., Ahmad, A., Chang, S. & Maynard, S. (2010). « Embedding Information Security Culture Emerging Concerns and Challenges », *PACIS 2010 Proceedings*.

Lim, J., Chang, S., Maynard, S. & Ahmad, A. (2009). « Exploring the Relationship between Organizational Culture and Information Security Culture », *Australian Information Security Management Conference*.

Lim, J., Maynard, S., Ahmad, A. & Chang, S. (2012). « Information Security Culture: Towards an Instrument for Assessing Security Management Practices », *International Journal of Cyber Warfare and Terrorism*, vol. 5, no 2, p. 31-52.

Lyu, H. & Zhang, Z. (2015). « Job Quitters, Information Security Awareness, and Knowledge Management Strategies », *Journal of Information Privacy and Security*, vol. 11, p. 189-210.

Mackenzie, S.B., Podsakoff, P. & Podsakoff, N. (2011). « Construct Measurement and Validation Procedures in Mis and Behavioral Research: Integrating New and Existing Techniques », *MIS Quarterly*, vol. 35, no 2.

Maeyer, D. (2007). « Setting up an Effective Information Security Awareness Programme », *Proceedings of ISSE/SECURE 2007*, p. 49-58.

Martin, J. (1992). *Cultures in Organization: Three Perspectives*, Oxford University Press.

Martins, N. & Eloff, J.H.P. (2002). « Information Security Culture », *SEC2000 Proceedings*, p. 203-214.

Mellado, D., Blanco, C., Sanchez, L.E. & Fernandez-Medina, E. (2010). « A Systematic Review of Security Requirements Engineering », *Comput Stand Interfaces*, vol. 32, p. 153-165.

Mishra, S. (2015). « Organizational Objectives for Information Security Governance: A Value Focused Assessment », *Information & Computer Security*, vol. 23, no 2, p. 122-144.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T. & Vance, A. (2009). « What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study », *European Journal of Information Systems*, vol. 18, no 2, p. 126-139.

Ng, B-Y., Kankanhalli, A. & Xu, Y. (2009). « Studying Users' Computer Security Behavior: A Health Belief Perspective », *Decision Support Systems*, vol. 46, no 4, p. 815-825.

Ngo, L., Zhou, W. & Warren, M. (2005). « Understanding Transition Towards Information Security Culture Change », *3rd Australian Computer, Network & Information Forensics Conference Proceedings*, p. 67-73.

Nosworthy, J. (2000). « Implementing Information Security in the 21st Century — Do You Have the Balancing Factors? », *Computers & Security*, vol. 19, no 4, p. 337-347.

OCRCVM (2015). *Cadre De Cybersécurité Volontaire De L'organisme Canadien De Réglementation Du Commerce Des Valeurs Mobilières (Ocrcvm)*, Organisme Canadien de Réglementation du Commerce des Valeurs Mobilières, 59 p.

Ott, S. (1989). *The Organizational Culture Perspective*, Brooks/Cole, 231 p.

Padayachee, K. (2012). « Taxonomy of Compliant Information Security Behavior », *Computers & Security*, vol. 31.

Parsons, K., McCormac, A., Butavicius, M. & Ferguson, L. (2010). *Human Factors and Information Security: Individual, Culture and Security Environment*, Defence Science and Technology Organisation.

Parsons, K., Young, E., Butavicius, M., McCormac, A., Pattinson, M. & Jerram, C. (2015). « The Influence of Organizational Information Security Culture on Information Security Decision Making », *Journal of Cognitive Engineering and Decision Making*, vol. 9, no 2, p. 117-129.

Pentland, B. (1995). « Information Systems and Organizational Learning: The Social Epistemology of Organizational Knowledge Systems », *Accounting, Management and Information Technologies*, vol. 5, no 1, p. 1-21.

Pliskin, N., Romm, T., Lee, A.S. & Weber, Y. (1993). « Presumed Versus Actual Organizational Culture: Managerial Implications for Implementation of Information Systems », *The Computer Journal*, vol. 36, no 2.

Podsakoff, P. & Organ, D. (1986). « Self-Reports in Organizational Research: Problems and Prospects », *Journal of Management*, vol. 12, no 4, p. 531-544.

Ponemon (2016). « Ponemon Institute Cost of a Data Breach Study ». Ponemon. Consulté le 1 juin 2017 de https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN

Potosky, D. & Ramakrishna, H.V. (2002). « The Moderating Role of Updating Climate Perceptions in the Relationship between Goal Orientation, Self-Efficacy, and Job Performance », *Human Performance*, vol. 15, no 3.

PricewaterhouseCoopers (2016). *Global State of Information Security Survey 2017*, PricewaterhouseCoopers. Consulté le 1 juin 2017 de https://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

Rantos, K., Fysarakis, K. & Manifavas, C. (2012). « How Effective Is Your Security Awareness Program? An Evaluation Methodology », *Information Security Journal: A Global Perspective*, vol. 21, p. 328-345.

Rastogi, R. & Von Solms, R. (2012). « Information Security Service Culture - Information Security for End-Users », *Journal of Universal Computer Science*, vol. 18, no 12, p. 1628-1642.

Reichers, A.E. & Schneider, B. (1990). « Climate and Culture: An Evolution of Constructs », dans *Organizational Climate and Culture*, Jossey-Bass, p. 5-39.

Rhee, H.S., Kim, C. & Ryu, Y. (2009). « Self-Efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior », *Computers & Security*, vol. 28, p. 816-826.

Robey, D., Ross, J. & Boudreau, M-C (2002). « Learning to Implement Enterprise Systems: An Exploratory Study of the Dialectics of Change », *Journal of Management Information Systems*, vol. 19, no 1, p. 17-46.

Romm, T., Pliskin, N., Weber, Y. & Lee, A.S. (1991). « Identifying Organizational Culture Clash in Mis Implementation », *Information & Management*, vol. 21.

Ross, J. (2011). *Creating a Culture of Security*, ISACA.

Ruighaver, A. B., Maynard, S. & Chang, S. (2006). « Organizational Security Culture: Extending the End-User Perspective », *Computers & Security*, vol. 26, no 1, p. 56-62.

Safa, N.S., Von Solms, R. & Furnell, S. (2016). « Information Security Policy Compliance Model in Organizations », *Computers & Security*, vol. 56, p. 70-82.

Saleh, M. (2011). « Information Security Maturity Model », *International Journal of Computer Science and Security*, vol. 5, no 3, p. 316-337.

Schein, E. (1985). *Organizational Culture and Leadership*, Jossey-Bass.

Schlienger, T. & Teufel, S. (2002). « Information Security Culture - the Social-Cultural Dimension in Information Security Management », *17th International Conference on Information Security, Proceedings*.

Schneider, B. & Barbera, K.M. (2014). *The Oxford Handbook of Organizational Climate and Culture*, Oxford University Press, 730 p.

Siehl, C. & Martin, J. (1984). « The Role of Symbolic Management: How Can Managers Effectively Transmit Organizational Culture? », dans *Leaders and Managers: International Perspectives on Managerial Behavior and Leadership*, Pergamon, p. 227-269.

Siponen, M. (2000). « A Conceptual Foundation for Organizational Information Security Awareness », *Information Management & Computer Security*, vol. 8, no 1, p. 31.

Smircich, L. (1983). « Concepts of Culture and Organizational Analysis », *Administrative Science Quarterly*, vol. 28, no 3.

Spears, J.L. & Barki, H. (2010). « User Participation in Information Systems Security Risk Management », *MIS Quarterly*, vol. 34, no 3, p. 503-522.

Tang, M., Li, M. & Zhang, T. (2015). « The Impacts of Organizational Culture on Information Security Culture: A Case Study », *Information Technology and Management*, vol. 16, no 57, p. 1-8.

TechTarget (2017). *Framework: Definition*., TechTarget Inc. Consulté le 5 mai 2017 de http://whatis.techtarget.com/definition/framework

Thomson, M.E. & Von solms, R. (1998). « Information Security Awareness: Educating Your Users Effectively », *Information Management & Computer Security*, vol. 6, no 4, p. 167-173.

Trice, H.M. & Beyer, J.M. (1993). *The Cultures of Work Organizations*, Prentice-Hall.

Tsohou, A., Karyda, M. & Kokolakis, S. (2012). « Analyzing Trajectories of Information Security Awareness », *Information Technology & People*, vol. 25, no 3, p. 327-352.

Van Loenen, J. (2015). « Information Security Awareness », *Research World*, vol. 54, no 53.

Van Niekerk, J. F. & Von Solms, R. (2010). « Information Security Culture: A Management Perspective », *Computers & Security*, vol. 29, p. 476-486.

Von Solms, B. (2000). « Information Security Culture: A Management Perspective », *Computers & Security*, vol. 19, no 7, p. 615-620.

Von Solms, S.H. & Von Solms, R. (2006). « Information Security Governance: Due Care », *Computers & Security*, vol. 25, no 7, p. 494-497.

Vroom, C. & Von Solms, R. (2004). « Towards Information Security Compliance », *Computers & Security*, vol. 23, no 3, p. 191-198.

Williams, C.K., Wynn, D., Madupalli, R., Karahanna, E. & Duncan, B. (2014). « Explaining Users' Security Behaviors with the Security Belief Model », *Journal of Organizational and End User Computing*, vol. 26, no 3, p. 23-46.

Wolf, M., Haworth, D. & Pietron, L. (2011). « Measuring an Information Security Program », *Review of Business Information Systems*, vol. 15, no 3, p. 9-21.

ANNEXES

Annexe 1 : Examen des autres concepts du domaine de la sécurité de l'information

Cette annexe présente l'examen des concepts connexes qui a permis d'exploiter au maximum la littérature existante, mais surtout de s'assurer qu'aucunes croyances, valeurs ou caractéristiques du climat de la sécurité de l'information aient été omises. Pour ce faire, les instruments de mesure et les cadre de référence de chacun des concepts connexes ont été soumis à une analyse. Ainsi, cette annexe inclut l'examen des instruments de mesure et des cadres de référence de la culture de la sécurité de l'information, de la maturité de la sécurité de l'information et de la sensibilisation à la sécurité de l'information.

1.1 Les instruments de mesure de la culture de la sécurité de l'information

Cette section de l'annexe 1 a pour principal objectif de présenter comment les instruments présents dans la littérature qui ont pour but de mesurer la culture de la sécurité de l'information pourraient aider à identifier des dimensions en lien avec les croyances, les valeurs et les caractéristiques du climat de la sécurité de l'information susceptibles d'influencer la mise en œuvre de pratiques sécuritaires par les employés.

Le tableau A1 présente les instruments de mesure inventoriés. Il expose leurs dimensions, leur description, leurs forces et faiblesses ainsi qu'une analyse concernant leur lien potentiel avec les croyances, les valeurs et les caractéristiques du climat en sécurité de l'information.

Tableau A1 : Les instruments de la culture de la sécurité de l'information

Nom de l'instrument	Auteur(s)	Dimensions	Description	Forces/faiblesses	Analyse
-	Alnatheer et al. (2012)	1. Implication de la haute direction en sécurité de l'information 2. Application des politiques en sécurité 3. Formation en sécurité 4. Sensibilisation en sécurité 5. Imputabilité de la responsabilité en sécurité	• Questionnaire • 19 items • Validé auprès des gestionnaires et des experts en sécurité (nombre de participants inconnu)	**Force(s)**: • Validé auprès de différents types d'organisations (public, semi-public, privé) et de différentes tailles (100 à 3000) **Faiblesse(s)** : • Présence de biais culturels (testé uniquement avec des organisations d'Arabie Saoudite) • Touche principalement les pratiques formelles de la sécurité de l'information • Échelle de mesure utilisée non spécifiée	Bien que cet instrument de mesure se focalise sur les pratiques formelles de la sécurité de l'information, il réfère à la croyance « Responsabilité morale de protéger l'information », la valeur « Importance accordée au développement des ressources humaines » et la caractéristique du climat « Soutien projeté par les gestionnaires ».
Information Security Culture Assessment	Da Veiga & Martins (2014 ; 2015) Da Veiga & Eloff (2007 ; 2010) Da Veiga, Martins & Eloff (2007)	1. Gestion des actifs informationnels 2. Gestion de la sécurité de l'information 3. Gestion du changement 4. Gestion de l'utilisateur 5. Politiques de sécurité de l'information 6. Programme de sécurité de l'information 7. Confiance 8. Gouvernance en sécurité de l'information	• Questionnaire • 55 items • Validé auprès de tous les employés d'une organisation (2320 participants en 2010 et de 2159 en 2013)	**Force(s)** : • Est actuellement l'instrument de mesure de la culture de la sécurité de l'information le plus raffiné (est en développement depuis 2007) **Faiblesse(s)**: • Relève de la vision individuelle de la sécurité de l'information (alors que ce mémoire traite de la vision organisationnelle) • N'est pas intégralement rendu public (seules les dimensions et leur définition le sont) • Ne traite pas de la culture de la sécurité de l'information mais plutôt des pratiques formelles de la sécurité de l'information	Cet instrument de mesure s'attarde aux perceptions des employés quant aux pratiques formelles de la sécurité de l'information. De ce fait, il évoque de manière implicite les valeurs « Attitude générale des employés face au changement » et « Importance accordée au développement des ressources humaines ») ainsi que les caractéristiques du climat « Soutien projeté par les gestionnaires » et « Communication organisationnelle ».

Tableau A1 : Les instruments de la culture de la sécurité de l'information (suite et fin)

Nom de l'instrument	Auteur(s)	Dimensions	Description	Forces/faiblesses	Analyse
Information Protection Culture Assessment	Da Veiga & Martins (2015)	1. Engagement quant à la sécurité de l'information 2. Participation de la direction 3. Nécessité et importance de la sécurité de l'information 4. Efficacité des politiques de sécurité de l'information 5. Imputabilité de la sécurité de l'information 6. Perception de l'usage de l'information	• Questionnaire • Nombre d'items inconnu (car l'instrument n'est pas rendu public)	**Force(s) :** • Premier instrument de la mesure de la vie privée et de la protection de l'information personnelle **Faiblesse(s)** : • L'intégralité de l'instrument de mesure n'est pas rendu public (seules les dimensions et leur définition le sont) • Ne traite pas de la culture de la sécurité de l'information mais plutôt des pratiques formelles de la sécurité de l'information	Cet instrument de mesure se concentre essentiellement sur les pratiques formelles de la sécurité de l'information et fait référence les valeurs « Attitude générale des employés face au changement » et « Importance accordée au développement des ressources humaines » et les caractéristiques du climat « Soutien projeté par les gestionnaires », « Communication organisationnelle » et « Engagement organisationnel ».
-	Lim et al. (2012)	1. Implication de la haute direction en sécurité 2. Impartition des responsabilités en sécurité 3. Gestion de risque en sécurité 4. Instauration des politiques de sécurité 5. Application des politiques de sécurité 6. Éducation, formation et sensibilisation en sécurité 7. *Benchmarking* et certification des pratiques en sécurité 8. Communications en sécurité et mécanismes de *reporting* 9. Contrôle de la sécurité	• Questionnaire • 35 items • Validation des items auprès de 46 praticiens	**Force(s)** : • Se base sur la littérature de la culture organisationnelle **Faiblesse(s)** : • Ne traite pas de la culture de la sécurité de l'information mais plutôt des pratiques formelles de la sécurité de l'information	Cet instrument de mesure concerne uniquement les pratiques formelles liées à la sécurité de l'information. Les dimensions de cet instrument de mesure évoquent la valeur « Importance accordée au développement des ressources humaines » et les caractéristiques du climat « Bases générales sur lesquelles sont prises les décisions », « Soutien projeté par les gestionnaires », « Adéquation au contexte organisationnel », « Récompenses/sanctions » et « Réponses face aux pressions externes ».

Dans le tableau A1, le premier instrument de mesure est celui d'Alnatheer et al. (2012). Bien que les auteurs stipulent que leur instrument de mesure évalue la culture de la sécurité de l'information, l'examen de ses dimensions et items (présentés dans le tableau A1.1) révèle que l'accent est mis sur les pratiques formelles liées à la sécurité de l'information (par exemple, l'instrument comprend les dimensions *information security policy enforcements, information security training,* etc.). De plus, les auteurs ne précisent pas l'échelle de mesure choisie dans leur étude et l'instrument peut faire état d'un biais culturel puisqu'il a uniquement été testé en Arabie Saoudite. Toutefois, cet instrument de mesure se démarque par le fait qu'il ait été validé auprès des organisations de différentes tailles et peut donc être adapté pour chacune d'entre elles. Il fait également la distinction entre les dimensions qui constituent la culture de la sécurité de l'information et celles qui l'influencent. L'analyse des dimensions et des items démontre que cet instrument de mesure inclut la croyance « Responsabilité morale de protéger l'information », la valeur « Importance accordée au développement des ressources humaines » et la caractéristique du climat « Soutien projeté par les gestionnaires ».

Tableau A1.1 : Instrument de mesure d'Alnatheer et al. (2012)

Dimensions	Items
Top Management Involvement in Information Security	1. Top management considers information security an important organisational priority. 2. Senior management gives strong and consistent support to the security program. 3. Senior management is always involved in key information security activities. 4. Management ensures that appropriate individuals are made responsible for specific aspects of information security 5. Management ensures that everyone who takes information security actions, and makes information security decisions and are held accountable for their decisions and actions
Information Security Policy Enforcement	1. Information security practices and procedures are continually monitored to ensure compliance with security policy 2. Information security practices and procedures are externally audited 3. Information security violations are reported to the proper authority 4. Actions against violations are always taken
Information Security Training	1. I receive adequate information security training 2. Information security policy is communicated well 3. I am always educated or trained about new security policies
Information Security Awareness	1. I am aware of my information security roles and responsibilities 2. I am aware of the risk of not following the information security policy 3. I am familiar with the information security policy 4. I am aware of the procedures for reporting security policy violations
Information Security Ownerships	1. It is my responsibility to protect the information of my organisation 2. I take ownership of the outcomes of my information security decisions and actions 3. Protecting information security is an important part of my job
Échelle de mesure: *Yes/No*	

Le deuxième instrument de mesure du tableau s'intitule *Information Security Culture Assessment* (Da Veiga & Martins, 2014; 2015; Da Veiga & Eloff, 2007,2010; Da Veiga, Martins & Eloff, 2007). Comme son nom l'indique, ses auteurs ont développé un outil qui évalue la culture de la sécurité de l'information. Il est d'ailleurs l'instrument de mesure de la culture de la sécurité de l'information le plus raffiné qui existe dans la littérature puisqu'il est développé et mis à jour depuis 2007. Malgré cette prémisse, il s'avère que cet instrument ne mesure que les perceptions des employés quant aux pratiques formelles liées à la sécurité de l'information (qui figurent dans le tableau A1.2) et n'évalue donc qu'une portion de la culture de la sécurité de l'information. De plus, cet instrument de mesure a été développé à des fins de consultation. Il n'est donc pas intégralement rendu public (seules les dimensions et leur définition le sont). En analysant les dimensions de cet instrument de mesure, on peut affirmer que ce dernier démontre l'importance des valeurs « Attitude générale des employés face au changement » et « Importance accordée au développement des ressources humaines » ainsi que les caractéristiques du climat « Soutien projeté par les gestionnaires » et « Communication organisationnelle ».

Tableau A1.2 : *Information Security Culture Assessment* (Da Veiga & Martins, 2014; 2015; Da Veiga & Eloff, 2007;2010; Da Veiga, Martins & Eloff, 2007)

Dimensions	Explications
1. Information asset management	Assesses users' perceptions of the protection of information assets
2. Information security management	Assesses management's perceptions of information security management
3. Change management	Assesses the perceptions about change and the willingness of users to change in order to protect information
4. User management	Assesses user awareness and training with regard to the requirements to protect information
5. Information security policies	Assesses whether users understand the information security policy and whether communication thereof was successful
6. Information security programme	Assesses the effectiveness of investing in information security resources
7. Trust	Assesses the perceptions of users regarding the safekeeping of private information and their trust in the communications of the organisation
8. Information security leadership	Assesses users' perceptions of information security governance (e.g. monitoring) to minimise risks to information
Échelle de mesure: échelle de Likert (*strongly disagree, disagree, unsure, agree, strongly agree)* et *Yes/No*	

Le troisième instrument de mesure du tableau, *Information Protection Culture Assessment* (présenté dans le tableau A1.3), a été créé par Da Veiga & Martins (2015) et est un complément à *Information Security Culture Assessment* (Da Veiga & Martins, 2014; 2015; Da Veiga &

Eloff, 2007; 2010; Da Veiga, Martins & Eloff, 2007) puisqu'il considère la vie privée et la protection de l'information personnelle comme des composantes de la culture de la sécurité de l'information. Comme son antécédent, cet instrument de mesure ne se focalise que sur les pratiques formelles de la sécurité de l'information et n'est pas entièrement rendu public (seules les dimensions et leur définitions le sont) puisqu'il est réservé à des fins de consultation. Une analyse de cet instrument de mesure a permis de constater qu'il faisait référence aux mêmes valeurs (« Attitude générale des employés face au changement » et « Importance accordée au développement des ressources humaines ») et les mêmes caractéristiques du climat (« Soutien projeté par les gestionnaires » et « Communication organisationnelle ») que son antécédent. À cela s'ajoute la caractéristique du climat « Engagement organisationnel », qui est également considéré par cet instrument de mesure.

Tableau A1.3 : *Information Protection Culture Assessment* par Da Veiga Martins (2015)

Dimensions	**Explications**
Information security commitment	The perception on the commitment from an organisational, divisional and employee perspective regarding the protection of information and implementation of information security controls.
Management buy-in	The perception on management buy-in towards information security and the importance attached to the concept by senior managers and executives. The concept of management adherence to the information security policy is also established.
Information security necessity and importance	Information security necessity is established by focussing on specific concepts such as people, time, money and the impact of changes.
Information security policy effectiveness	The effectiveness of the information security policy and the communication thereof is established.
Information security accountability	Individual accountability to compliance and the requirements for information security training.
Information usage perception	The perception on information security and privacy usage requirements.
Échelle de mesure: Non spécifiée	

Finalement, le dernier instrument figurant dans le tableau A1 est celui de Lim et al. (2012) (présenté dans le tableau A1.4). Ces derniers proposent un instrument de mesure de la culture de la sécurité de l'information qui se base sur la littérature de la culture organisationnelle en empruntant le cadre de Detert (2000). Bien que les auteurs souhaitent mesurer la culture de la sécurité de l'information, leur instrument de mesure met l'accent sur les pratiques formelles en la matière. En analysant cet instrument de mesure, on remarque que ses dimensions vont dans la même direction que la valeur « Importance accordée au développement des ressources humaines » ainsi que les caractéristiques du climat « Bases générales sur lesquelles sont prises les décisions », « Soutien projeté par les gestionnaires », « Adéquation au contexte

organisationnel », « Récompenses/sanctions » ainsi que de« Réponses face aux pressions externes ».

Tableau A1.4 : Instrument de mesure de Lim et al. (2012)

Dimensions	Explications
1. Top Management Involvement	• Top management makes key decisions on information security matters • Top management participates in information security matters e.g. attending SETA programs • Top management leads by example in implementing security matters. • Top management provides sufficient resources for information security activities • Top management responds immediately to internal and external requirements relating to information security
2. Assignment of security responsibili-ties	• There is a clear assignment of information security roles and responsibilities for every employee. • There is representation and participation across organizational departments on the steering committee responsible for information security management • Information security is a joint responsibility of the organization's functional units and IT department
3. Security Risk Management	• Security risks are identified and assessed periodically or if significant changes to information resources or the threat environment occurs • Risk management methodologies applied in the organization comply with best-practice standards • Selection of managerial and technical controls for risk response is based on the outcomes of risk assessments
4. Security policy development and implementa-tion	• The information security policy is reviewed at planned intervals or if significant changes occur to ensure its continuing suitability and effectiveness • The information security policy is written in a clear and understandable manner • Employees are aware of the existence of the organization's information security policies • The information security policy is aligned with the organization's goals
5. Security policy enforcement	• There are consequences of non-compliance of the information security policy • Information security violations result in prompt response from top management • Employees caught violating security policies would be dealt with consistently. • Employees who repeatedly violate the information security policy may be considered for disciplinary action
6. Security education, training and awareness (SETA)	• SETA programs are compulsory for every employee • There is a continuous SETA program to increase employees' awareness towards information security • Employees receive sufficient information security training prior to gaining access to the network
7. Security benchmarking and certification	• Information security is measured on a continuous basis • Information security measures in place are as good if not better than in other similar organizations. • Information security measures comply with international standards
8. Security communica-tions and reporting mechanisms	• There are reminders and briefings on appropriate and inappropriate behaviors in regards to information security practices • There are notices and posters used to promote security awareness • Information security plans and details are communicated to heads of departments across the organization • There is a reporting mechanism for employees to provide feedback to enhance information security

9. Security controls implementa-tion and monitoring	• Employees are aware that there are daily routine checks of information system logs • There are sufficient physical controls in place to protect organizational information • There are sufficient logical controls in place to protect access to the information systems • There are sufficient legal controls to protect organizational information • There is a regular audit on information security compliance by internal auditors • There is a regular audit on information security compliance by external auditors
Échelle de mesure: Non spécifiée	

En conclusion, l'examen de ces instruments de mesure a permis de constater qu'ils étaient très limités puisqu'aucun ne mesure la culture et le climat de la sécurité de l'information de manière conjointe. Tels qu'ils ont été définis dans le chapitre 2. En effet, ils évaluent plutôt les pratiques formelles liées à la sécurité de l'information. Ces instruments de mesure n'ont pas permis d'enrichir la liste de croyances, de valeurs et de caractéristiques du climat de la sécurité de l'information, mais ont néanmoins permis de démontrer la pertinence d'inclure certaines d'entre elles sur la liste finale de croyances, de valeurs et de caractéristiques du climat de la sécurité de l'information.

1.2 Les cadres de référence en sécurité de l'information

Un cadre de référence en sécurité de l'information est un document regroupant des processus détaillés, permettant de définir les politiques et les procédures qui encadrent la mise en place et la gestion de la sécurité de l'information dans une organisation. Au même titre que les instruments de mesure, les cadres de référence de la culture de la sécurité de l'information constituent également des sources pertinentes pour vérifier l'exhaustivité de la liste de croyances, de valeurs et des caractéristiques du climat réalisée précédemment. De ce fait, l'examen conduit dans la section précédente est répliqué ici.

Cette sous-section a, dans un premier temps, pour objectif de présenter les cadres de référence de la culture de la sécurité de l'information. Ensuite, ces derniers seront soumis au même examen que ceux des instruments de mesure de la culture de la sécurité de l'information car les dimensions les composant faisant l'objet d'une analyse.

Les cadres de référence sont synthétisés dans le tableau A2. Ils sont présentés en exposant leurs dimensions, une description ainsi que leurs forces et faiblesses. Ces cadres de référence seront également analysés afin d'en déterminer les liens avec les valeurs, croyances et les caractéristiques du climat de la sécurité de l'information.

Tableau A2 : Cadres de référence de la culture de la sécurité de l'information

Cadre	Auteur(s)	Dimensions	Description	Forces et faiblesses	Analyse
Information Security Culture Framework	Alhogail (2015)	1. Stratégie 2. Technologie 3. Organisation 4. Employés 5. Environnement	• Cadre de référence • Validé auprès de 9 experts en sécurité de l'information	**Force(s) :** • Prend en compte la dimension macro de la sécurité de l'information **Faiblesse(s) :** • Seules les dimensions et leur description sont rendus publics • S'intéresse principalement aux pratiques formelles de la sécurité de l'information	La dimension « Organisation » pourrait s'avérer être une source intéressante d'information car d'après sa description, elle énonce les croyances, les valeurs, les hypothèses, les normes (etc.) liées à la sécurité de l'information. Malheureusement, l'instrument n'est pas accessible au public, ce qui empêche d'en savoir davantage sur cette dimension.
Information Security Culture Framework	Da Veiga & Eloff (2010)	1. Direction et gouvernance 2. Gestion de la sécurité et des opérations 3. Politiques de sécurité 4. Gestion du programme de sécurité 5. Gestion de la sécurité utilisateur 6. Protection et opérations de la technologie 7. Changement	• Cadre de référence • A servi de fondation pour l'instrument *Information Security Culture Assessment* de Da Veiga & Eloff (2007; 2015) • Validé auprès d'une entreprise Sud-africaine (nombre de participants inconnu)	**Force(s) :** • Évalue les pratiques de la sécurité de l'information de manière exhaustive **Faiblesse(s) :** • Omet les autres manifestations de la culture de la sécurité de l'information	Ce cadre évalue les pratiques formelles liées à la sécurité de l'information et touche donc des valeurs telles que « Réponse habituelle de l'organisation face aux pressions externes », « Attitude générale des employés face aux changements », ainsi que des caractéristiques du climat telles que « Soutien projeté par les gestionnaires », « Bases sur lesquelles sont prises les décisions », « Façon dont le monitorage du respect des pratiques de sécurité se fait ».

Le premier élément du tableau A2 est un cadre de référence de la sécurité de l'information développé par Alhogail (2015). Le cadre *Information Security Culture Framework* (2015) (dont le contenu peut être trouvé dans le tableau A2.1) adopte une vision macro de la sécurité de l'information en ayant pour dimensions la stratégie, la technologie, l'organisation, les employés et l'environnement dans lequel se situe l'organisation, ce qui en fait sa principale force. Il faut toutefois préciser que chacune de ces dimensions ne traitent que des pratiques formelles de l'organisation. La dimension « Organisation » pourrait s'avérer être une source intéressante pour valider ou enrichir la liste de croyances, de valeurs et de caractéristiques du climat de la sécurité de l'information car, d'après sa description, elle énonce les croyances, les valeurs, les hypothèses, les normes (etc.) liées à la sécurité de l'information. Malheureusement, seules les dimensions du cadre sont rendues publiques et il n'est donc pas possible de consulter les items afin d'en savoir davantage et d'enrichir la liste à élaborer.

Tableau A2.1 : Cadre de référence d'Alhogail (2015)

Dimensions	**Explications**
Strategy	Strategy in this context is concerned with the appropriate implementation of different information security strategies such as plans of actions, policies, objectives, best practices, standards, guidelines, and priorities that are designed to guide organization members to reach the goal of protecting information assets. (p.569)
Technology	The technology dimension in this context is concerned with security technologies such as hardware, software, services, appliances, and applications that are used within the organization to protect information assets. (p. 569)
Organisation	In this context, the organization dimension is concerned with the collection of information security-related beliefs, values, assumptions, symbols, norms, and knowledge that uniquely represent the organization. (p. 569)
People	The people dimension is concerned with the behavior of any person within the organization who is in direct contact with information assets. The information security culture aims to ensure that information security is everyone's responsibility. (p. 569)
Environment	In this framework context, the environment dimension is concerned with the identifiable external elements surrounding the organization that affect its structure and operations and in turn the security of the information assets and the information security culture. (p.569)
Échelle de mesure: échelle de 0 à 5 (n/a, *very low, low, average, high, very high)*	

Le deuxième et dernier cadre de référence du tableau A2*, Information Security Culture Framework* (dont l'intégralité peut être retrouvée dans le tableau A2.2) a été développé par Da Veiga & Eloff (2010). Il a notamment servi de fondation pour l'instrument de mesure *Information Security Culture Assessment* (Da Veiga & Martins, 2014; 2015; Da Veiga & Eloff, 2007; 2010; Da Veiga, Martins & Eloff, 2007). Les auteurs de ce cadre de référence affirment qu'il traite de la culture de la sécurité de l'information quand, en réalité, il met davantage l'accent sur les pratiques formelles de la sécurité de l'information et en présente une liste qui

se veut exhaustive. L'accent est également porté sur la technologie qui appuie ces pratiques. L'analyse des dimensions de ce cadre fait constater que ce cadre de référence démontre l'importance des valeurs « Réponse habituelle de l'organisation face aux pressions externes », « Attitude générale des employés face au changement » et les caractéristiques du climat « Soutien projeté par les gestionnaires », « Bases sur lesquelles sont prises les décisions » mais aussi « Façon dont le monitorage du respect des pratiques de sécurité se fait ».

Tableau A2.2 : *Information Security Culture Framework* de Da Veiga & Eloff (2010)

Dimensions	**Explications**
Leadership and Governance	Sponsorship, Strategy, IT Governance, Risk Assessment, ROI/Metrics/Measurement
Security Management and Organization	Program Organization, Legal & Regulatory
Security Policies	Policies, Procedures, Standards, Guidelines, Certification, Best practice
Security Management Program	Monitoring and Audit, Compliance
User Security Management Program	User Awareness, Education and Training, Ethical Conduct, Trust, Privacy
Technology Production and Operations	Asset Management, System Development Incident Management, Technical Operations, Physical and Environmental, Business Continuity
Change Management	-
Échelle de mesure: échelle de 1 à 5 (*strongly disagree, disagree, uncertain, agree strongly, agree disagree)*	

En conclusion, l'examen de ces cadres de référence atteste que ces outils demeurent limités puisque l'accent est porté sur les pratiques formelles de la sécurité de l'information bien qu'il y ait une volonté de traiter la culture de la sécurité de l'information de manière plus globale (en incluant ses aspects humains, organisationnels et technologiques). On notera notamment le cadre d'Alhogail (2015) qui inclut des valeurs et des croyances liées à la culture de la sécurité de l'information. Il aurait été pertinent de les comparer avec celles relevées dans ce mémoire mais, malheureusement, le détail des items de ce cadre de référence n'est pas rendu accessible au public. En bout de ligne, il est possible d'affirmer que ces cadres de référence évoquent certaines des valeurs et des caractéristiques du climat de la sécurité de l'information recensées dans ce chapitre, mais que la culture de la sécurité de l'information n'est pas traitée telle qu'elle a été définie dans le chapitre 2.

1.3 La maturité de la sécurité de l'information : un thème connexe à explorer

La culture de la sécurité de l'information et la maturité de la sécurité de l'information sont des construits étroitement liés (Dzazali & Zolait, 2012 ; Saleh, 2011). Au même titre que la culture de la sécurité de l'information, certains auteurs soulignent l'importance de la maturité de la sécurité de l'information mieux gérer les risques en sécurité informatique (par exemple, Dzazali & Zolait, 2012; Ge et al., 2011).

Selon Saleh (2011), la maturité de la sécurité de l'information traite de l'habileté des organisations à atteindre leurs objectifs de sécurité, de confidentialité, d'intégrité, et de disponibilité de l'information, tout en remplissant la mission de l'organisation en dépit des attaques et des incidents informatiques. Dans le rapport de l'*Institute for Security and Open Methodologies* (2004), la maturité de la sécurité de l'information est définie comme étant la gestion de processus de sécurité de l'information selon trois niveaux : stratégique, tactique et opérationnel.

Il s'agit donc, dans cette section, d'examiner les instruments et les cadres de référence de la maturité de la sécurité de l'information, afin de potentiellement s'assurer que toutes les croyances, les valeurs et les caractéristiques du climat liées à la sécurité de l'information aient été recensées dans les sections précédentes.

1.3.1 Les instruments de mesure de la maturité de la sécurité de l'information

Il existe dans les littératures scientifique et pratique des instruments de mesure de la maturité de la sécurité de l'information. Ces outils s'avèrent essentiels pour les organisations dans l'évaluation de leur programme de sécurité de l'information.

Les instruments de mesure de la maturité en sécurité de l'information sont présentés dans le tableau A3. À l'instar de la section précédente, ils feront l'objet d'une présentation et d'une analyse afin de pointer leurs potentiels liens avec la culture ou le climat de la sécurité de l'information.

Tableau A3 : Les instruments de mesure de la maturité de la sécurité de l'information

Nom de l'instr.	Auteur(s)	Description	Dimensions	Forces/faiblesses	Analyse
Forrester Information Security Maturity Assessment (2014)	Forrester	• Questionnaire • 128 items • Échelle de Likert (1 à 5)	1. Strategy 2. Governance and Program Management 3. Risk Management 4. Compliance 5. Audit and Assurance 6. Network 7. Databases 8. Systems 9. Endpoints 10. Application Infrastructures 11. Messaging, Content and Social Media 12. Data 13. Identity and access management 14. Threat and vulnerability management 15. Investigations and record management 16. Incident management 17. Third-party risk management 18. Information Asset Management 19. Applications/system development 20. Business continuity and disaster recovery 21. Security Services 22. Security advocacy, training, awareness 23. Security Organization 24. Business Relationship 25. Roles/responsibilities	**Force(s) :** • Fait la liste exhaustive des pratiques formelles liées à la sécurité de l'information **Faiblesse(s) :** • Est plutôt adapté pour une organisation de grande taille	Cet instrument de mesure expose les pratiques formelles liées à la gestion de la sécurité de l'information. La vision de la sécurité de l'information est principalement technologique puisque l'instrument évalue l'implantation et l'application de technologies qui en sécurité de l'information. Ainsi, cet instrument de mesure ne cherche pas à mesurer d'aucune façon un ou l'autre des aspects liés à la culture ou au climat.

Tableau A3 : Les instruments de mesure de la maturité de la sécurité de l'information (suite et fin)

Nom de l'instr.	Auteur(s)	Description	Dimensions	Forces/faiblesses	Analyse
Due care self-evaluation exercise	Von Solms & Von Solms (2006)	• Questionnaire • 11 items • Échelle de mesure *Yes/No*	N/A	**Force(s) :** • Simple et permet une évaluation rapide de la maturité **Faiblesse(s) :** • Trop limité • Besoin de sophistiquer l'échelle de mesure	Compte tenu de son format, cet outil s'apparente à une simple *checklist* des pratiques formelles de la sécurité de l'information. De ce fait, il est impossible d'en tirer quoi que ce soit en lien avec la culture ou le climat de la sécurité de l'information.

Le premier instrument de mesure du tableau A3, le *Forrester Information Security Maturity Assessment* (2014) est un instrument de mesure qui se base sur le cadre de maturité *Forrester Information Security Maturity* Model (2014) (figurant dans le tableau A3.1). Il a pour but d'aider les organisations à mesurer leur maturité de la sécurité de l'information et à les assister dans la gestion des processus de sécurité de l'information. L'instrument de mesure est un questionnaire qui fait la liste exhaustive des processus liés à la sécurité de l'information. Cependant, il est plutôt adapté pour les entreprises de grande taille compte tenu du nombre élevé de processus de sécurité de l'information qu'il évalue. Cet instrument a pour objectif d'évaluer la présence des pratiques formelles liées à la gestion de la sécurité de l'information. La vision de la sécurité de l'information est principalement technologique puisqu'elle évalue l'implantation et l'application de technologies qui opèrent la gestion de la sécurité de l'information. Par conséquent, cet outil n'évoque aucune des croyances, des valeurs et des caractéristiques du climat de la sécurité de l'information présentées dans ce chapitre.

Tableau A3.1: *Forrester Information Security Maturity Model & Assessment* de Forrester (2014)

Dimensions	Sous-dimensions	Explications
Oversight	Strategy	Ability of the security organization to consistently set objectives based on current conditions, available resources, and the needs of the business
	Governance and Program Management	A set of distinct processes by which the organization identifies, measures, controls, and reports on relevant risks and reports this information to all necessary stakeholders to support better-informed decisions
	Risk Management	A set of distinct processes by which the organization identifies, measures, controls, and reports on relevant risks and reports this information to all necessary stakeholders to support better-informed decisions
	Compliance	A function that supports the business by identifying all applicable laws, standards, and other requirements; translating those requirements into practical policies and controls; enforcing those policies and controls in a way that enables the business to operate; and measuring and reporting on the business' adherence to the requirements
	Audit and Assurance	The improvement of oversight through third-party assurance and effective response to audits, as well as the ability to demonstrate good governance to third parties
Technology	Network	Functions to maintain the confidentiality of communications and the availability of the network (wired, wireless, and software-defined), as well as the capability to protect devices attached to the network
	Databases	Capabilities to maintain the confidentiality, integrity, and availability of data stored within a database
	Systems	Capabilities to maintain the confidentiality, integrity, and availability of corporate servers and systems (both physical and virtual)

Dimensions	Sous-dimensions	Explications
	Endpoints	Capabilities to maintain the confidentiality, integrity, and availability of user endpoint devices (including desktops, laptops, mobile, SCADA endpoints, etc.)
	Application Infrastructures	Capabilities to maintain the confidentiality, integrity, and availability of application infrastructure components (including mobile applications)
	Messaging, Content and Social Media	Capabilities to protect the infrastructure from malicious content and to protect proprietary or confidential content from being mishandled
	Data	Capabilities to maintain the confidentiality and integrity of corporate data
Process	Identity and access management	Facility for defining, administering, and tracking privileges across corporate systems
	Threat and vulnerability management	Capabilities to assess and analyze threats, identify vulnerabilities, and take appropriate action to reduce relevant risks
	Investigations and record management	Processes to store, aggregate, synthesize, and report on historical IT and security data for legal, compliance, and risk management requirements
	Incident management	Capabilities for identifying potentially threatening security events that may negatively impact the organization, and responding appropriately to mitigate the risk
	Third-party risk management	Processes to set requirements and assess vendors, suppliers, outsources, service partners, cloud providers, and other partners to ensure they maintain desired levels of security
	Information Asset Management	Processes for identifying, classifying, and handling information assets as well as the physical platforms on which they reside or are processed
	Applications/system development	Policies and procedures in place during the development of applications (including internal and customer- facing mobile apps) and systems to ensure that proper controls are incorporated
	Business continuity and disaster recovery	Plans and processes to ensure that operations will be maintained and that the business will survive in the event of unexpected incidents and outages
People	Security Services	Capabilities for defining, communicating, tracking, and improving the services for which the security team is responsible
	Security advocacy, training, awareness	Ability of the security team to effectively communicate its role in supporting organizational objectives as well as to communicate and guide the role of individual employees to support security and risk management objectives
	Security Organization	Characteristics of the security organization that allow it to be effectively managed in support of changing business and risk management requirements
	Business Relationship	Ability of the security department to coordinate and collaborate with other functions across the organization
	Roles/responsibilities	Capabilities to define roles and responsibilities for information security within the immediate team as well as across relevant business and organizational functions
Échelle de mesure: échelle de 0 à 5 *(nonexistent, ad hoc, repeatable, defined, measured, optimized).*		

Le deuxième instrument de mesure du tableau s'intitule *Due care self-evaluation exercise* (présenté dans le tableau A3.2) et a été développé par Von Solms & Von Solms (2006). Il évalue si l'instauration des bonnes pratiques en matière de sécurité de l'information a été appliquée au sein d'une organisation. L'instrument de mesure permet d'obtenir un diagnostic rapide de la maturité de l'information de l'organisation. Néanmoins, le questionnaire est très limité et ne peut couvrir de manière exhaustive toutes les pratiques liées à la sécurité de l'information avec seulement 11 items. Par conséquent, il est impossible d'en tirer des conclusions en lien avec la culture ou le climat de la sécurité de l'information.

Tableau A3.2 : *Due care self-evaluation exercise* de Von Solms & Von Solms (2006)

No	Question
1	Do you accept that information is a critically important business asset to your organization?
2	Have you made an asserted effort to determine which the most critical risks are threatening the organization's information assets?
3	Did you create and express a clear vision to mitigate these risks to an acceptable level?
4	Did you ensure that the CISP was technically, operationally and managerially interpreted to be implemented in a practical manner?
5	Did you ensure that the required resources (budget, manpower, technology) were made available, as far as possible, to implement the company security standards?
6	Are you convinced that adequate procedures and guidelines were put in place to operationally enforce these company security policies and standards?
7	Are you convinced that the CISP and company security standards are effective?
8	Were all information workers in the company adequately educated on acceptable behavioral procedures and guidelines?
9	Is a definite process in place that ensures that the policies, company standards and procedures are updated with regular intervals?
10	Is a process in place to continuously monitor security controls to identify any exceptions or deviations?
11	Are all security related internal controls (including operational controls) audited for proper functioning?
Échelle de mesure: *Yes/No*	

Au final, ces instruments de mesure de la maturité de la sécurité de l'information ne permettent pas d'apporter de connaissances additionnelles quant à la liste de croyances, de valeurs et de caractéristiques du climat de la sécurité de l'information puisqu'ils ne s'intéressent qu'à l'aspect opérationnel de la sécurité de l'information. En effet, ces instruments de mesure concernent essentiellement les pratiques formelles et les technologies en la matière.

1.3.2 Les cadres de référence de la maturité de la sécurité de l'information

Pour avoir plus de contrôle sur leurs processus et pour atteindre l'excellence en gestion, les organisations s'appuient sur des modèles de maturité (Ge et al., 2011). Il va donc de soi que l'on retrouve de multiples modèles de maturité en sécurité de l'information dans la littérature scientifique et pratique. Communément appelés *Information Security Maturity Models (ISMMs)*, ils s'avèrent être une collection d'éléments de la sécurité de l'information qui

décrivent les différents niveaux de maturité dans une organisation. Ceux-ci ont pour but de décrire les différents niveaux de technologie et de sophistication de la sécurité ainsi que d'aider les organisations à identifier et à comprendre leurs vulnérabilités en matière de sécurité, à contrôler la progression de l'instauration de pratiques de sécurité de l'information, de politiques ainsi que de contrôler la gestion et les investissements en sécurité de l'information (Karakola et al., 2011; Ge et al., 2011). De plus, ces cadres de référence servent à guider les organisations lors de la priorisation des pratiques de sécurité de l'information à mettre en œuvre (Von Solms & Von Solms, 2006). D'autre part, ces cadres permettent d'évaluer les politiques et les procédures relatives à la sécurité de l'information et, en se basant sur les résultats de conformité à ces politiques et procédures, de déterminer si les objectifs en matière de sécurité sont atteints (Köne & Eloff, 2002). Tous ces facteurs offrent ainsi une meilleure compréhension des programmes de sécurité des organisations (Ge et al., 2011).

Les cadres de références recensés sont présentés dans le tableau A4 qui fournit une présentation de ces cadres de référence ainsi qu'une analyse des dimensions qui les composent. Ils seront également soumis à une analyse afin de relever leurs liens potentiels avec la culture ou le climat de la sécurité de l'information.

Tableau A4 : Les cadres de référence de la maturité de la sécurité de l'information

Nom du cadre	Auteur(s)	Description	Dimensions relatives à la maturité en sécurité de l'information	Force(s)/faiblesse(s)	Analyse
ISO 27002/CEI (2013)	ISO	• Norme internationale	1. Politiques de sécurité de l'information 2. Organisation de la sécurité de l'information 3. La sécurité des ressources humaines 4. Gestion des actifs 5. Contrôle d'accès 6. Cryptographie 7. Sécurité physique et environnementale 8. Sécurité liée à l'exploitation 9. Sécurité des communications 10. Acquisition, développement et maintenance des systèmes d'information 11. Relation avec les fournisseurs 12. Gestion des incidents liés à la sécurité de l'information 13. Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité 14. Conformité	**Force(s) :** • Présente les bonnes pratiques en gestion de la sécurité de l'information de manière exhaustive **Faiblesse(s) :** • Ne propose ni niveaux, ni méthodes d'évaluation de la maturité	Ce cadre de référence se concentre principalement sur les pratiques formelles liées à la sécurité de l'information et leurs technologies. Il ne constitue pas un apport quant au bassin de croyances, de valeurs et de caractéristiques de la sécurité de l'information**.**

Tableau A4 : Les cadres de référence de la maturité de la sécurité de l'information (suite)

Nom du cadre	Auteur(s)	Description	Dimensions relatives à la maturité en sécurité de l'information	Force(s)/faiblesse(s)	Analyse
Cadre de cyber sécurité volontaire de l'Organisme canadien de réglementation du commerce des valeurs mobilières (2015)	OCRCVM	• Guide de pratiques exemplaires en matière de cyber sécurité	1. Gouvernance et gestion des risques 2. Pratiques exemplaires recommandées: petites et moyennes sociétés membres 3. Enquête de sécurité sur le personnel et les menaces internes 4. Sécurité physique et environnementale 5. Sensibilisation à la cyber sécurité et formation 6. Évaluation des menaces et des vulnérabilités 7. Sécurité réseau 8. Protection des systèmes d'information 9. Gestion des comptes utilisateur et contrôle d'accès 10. Gestion des actifs 11. Intervention en cas d'incident 12. Partage de l'information et signalement d'une infraction 13. Cyber assurance 14. Gestion des risques de fournisseur 15. Politique de cyber sécurité	**Force(s) :** • Adapté à l'industrie financière **Faiblesse(s) :** • Ne propose ni niveaux, ni méthodes d'évaluation de la maturité	Ce cadre de référence concerne les pratiques formelles qui sont liées à la sécurité de l'information. Mais puisque ce cadre de référence a été développé pour des institutions financières, on peut affirmer que la valeur « Adéquation au contexte organisationnel » ressort de cet outil.

Tableau A4 : Les cadres de référence de la maturité de la sécurité de l'information (suite)

Nom du cadre	Auteur(s)	Description	Dimensions relatives à la maturité en sécurité de l'information	Force(s)/faiblesse(s)	Analyse
Forrester Information Security Model (2014)	Forrester	• Guide de pratiques	1. Oversight 2. Technology 3. Process 4. People	**Force(s) :** • Est accompagné d'un instrument de mesure de la maturité en sécurité de l'information **Faiblesse(s) :** • Ne propose pas de niveaux de la maturité en sécurité de l'information	Ce cadre de référence aborde toutes les facettes de la culture de la sécurité de l'information (humaines, organisationnelles et technologiques), mais il se focalise principalement sur les pratiques liées à la sécurité de l'information. De ce fait, il n'apporte pas de connaissances additionnelles à la liste de croyances, de valeurs et de caractéristiques du climat de la sécurité de l'information.
O-ISM 3 (2012)	Institute for Security and Open Methodolo-gies	• Cadre de référence	1. Security management – ISM3 Basics 2. Generic processes 3. Specific processes – strategic management 4. Specific processes – tactical management 5. Specific processes – operational management	**Force(s):** • Analyse les processus de sécurité selon 3 niveaux de gestion **Faiblesse(s) :** • Ne propose pas de bonnes pratiques	Ce cadre de référence évalue les pratiques formelles liées à la sécurité de l'information selon trois axes (stratégique, tactique et opérationnel). Le contexte organisationnel en étant absent, il est difficile d'y voir quoi que ce soit en lien avec la culture ou le climat de la sécurité de l'information.

Tableau A4 : Les cadres de référence de la maturité de la sécurité de l'information (suite et fin)

Nom du cadre	Auteur(s)	Description	Dimensions relatives à la maturité en sécurité de l'information	Force(s)/faiblesse(s)	Analyse
COBIT 5 for Information Security (2012)	ISACA	• Guide de pratiques • 6 niveaux de maturité	1. Principles, policies and frameworks 2. Processes 3. Organizational Structure 4. Culture, Ethics and Behaviour 5. Information 6. Services, Infrastructure, Applications 7. People, Skills and Competencies	**Force(s) :** • S'agit du seul cadre de la maturité en sécurité de l'information qui s'intéresse à la culture de la sécurité de l'information **Faiblesse(s) :** • Ne se concentre que sur les processus de la sécurité de l'information	Ce cadre de référence concerne majoritairement sur les pratiques formelles liées à la sécurité de l'information, mais il se penche aussi sur la question de la culture de la sécurité de l'information. Il inclut notamment l'éthique, ce qui valide la valeur « Prédispositions éthiques de l'organisation » relevée précédemment.

Le premier cadre de référence du tableau A4 est la norme internationale *ISO/CEI 27002* (2013). Elle est composée d'un ensemble de bonnes pratiques qui se rapporte à la sécurité de l'information et présente 113 mesures qui sont classées selon 14 dimensions de la sécurité de l'information (qui sont présentées dans le tableau A4.1). Néanmoins, elle ne fixe pas de niveaux de maturité et ne précise pas de méthodes permettant d'évaluer la maturité en sécurité de l'information. À cela s'ajoute le fait que cet outil ne s'attarde qu'aux pratiques formelles liées à la sécurité de l'information et sur les technologies qui les supportent. Il ne permet donc pas d'apporter des connaissances supplémentaires à la liste de croyances, de valeurs et de caractéristiques de la sécurité de l'information présentée dans ce chapitre.

Tableau A4.1 : *ISO/ CEI 27002* (2013)

Dimensions relatives à la maturité en sécurité de l'information	**Sous-dimensions**	**Sous-sous-dimensions**	**Objectif**
1. Politiques de sécurité de l'information	1.1. Orientations de la direction en matière de la sécurité de l'information	1.1.1. Politiques de sécurité de l'information	« Apporter à la sécurité de l'information une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur. » (p.2)
		1.1.2. Revue des politiques de sécurité de l'information	
2. Organisation de la sécurité de l'information	2.1. Organisation interne	2.1.1. Fonctions et responsabilités liées à la sécurité de l'information	« Établir un cadre de gestion pour engager, puis vérifier la mise en œuvre et le fonctionnement de la sécurité de l'information au sein de l'organisation. » (p. 4)
		2.1.2. Séparation des tâches	
		2.1.3. Relations avec les autorités	
		2.1.4. Relations avec des groupes de travail spécialisés	
		2.1.5. La sécurité de l'information dans la gestion de projet	
	2.2. Appareils mobiles et télétravail	2.2.1. Politiques en matière d'appareils mobiles	« Assurer la sécurité du télétravail et de l'utilisation d'appareils mobiles. » (p. 7)
		2.2.2. Télétravail	
3. La sécurité des ressources humaines	3.1. Avant l'embauche	3.1.1. Sélection des candidats	« S'assurer que les salariés et les contractants comprennent leurs responsabilités et qu'ils sont compétents pour remplir les fonctions que l'organisation envisage de leur confier. » (p.9)
		3.1.2. Termes et conditions de l'embauche	
	3.2. Pendant la durée du contrat	3.2.1. Responsabilités de la direction	"S'assurer que les salariés et les contractants sont conscients de leurs responsabilités en matière de sécurité de l'information et qu'ils assument ces responsabilités." (p.11)
		3.2.2. Sensibilisation, apprentissage et formation à la sécurité de l'information	
		3.2.3. Processus disciplinaire	
	3.3. Rupture, terme ou modification du contrat de travail	3.3.1. Réussite ou modification des responsabilités associées au contrat de travail	"Protéger les intérêts de l'organisation dans le cadre du processus de modification, de rupture ou de terme d'un contrat de travail." (p. 14)
4. Gestion des actifs	4.1. Responsabilités relatives aux actifs	4.1.1. Inventaire des actifs	"Identifier les actifs de l'organisation et définir les responsabilités appropriées en matière de protection." (p. 15)
		4.1.2. Propriété des actifs	
		4.1.3. Utilisation correcte des actifs	
		4.1.4. Restitution des actifs	
		4.2.1. Classification des informations	

Dimensions relatives à la maturité en sécurité de l'information	Sous-dimensions	Sous-sous-dimensions	Objectif
	4.2. Classification de l'information	4.2.2. Marquage des informations	"S'assurer que l'information bénéficie d'un niveau de protection approprié conforme à son importance pour l'organisation." (p. 16)
		4.2.3. Manipulation des informations	
	4.3. Manipulation des supports	4.3.1. Gestion des supports amovibles	"Empêcher la divulgation, la modification, le retrait ou la destruction non autorisé(e) de l'information de l'organisation stockée sur des supports." (p. 19)
		4.3.2. Mise au rebut des supports	
		4.3.3. Transfert physique des supports	
5. Contrôle d'accès	5.1. Exigences métier en matière de contrôle d'accès	5.1.1. Politiques de contrôle d'accès	"Limiter l'accès à l'information et aux moyens de traitement de l'information." (p. 21)
		5.1.2. Accès aux réseaux et aux services en réseau	
	5.2. Gestion de l'accès utilisateur	5.2.1. Enregistrement et désinscription des utilisateurs	"Maîtriser l'accès utilisateur par le biais d'autorisation et empêcher les accès non autorisés aux systèmes et services d'information." (p. 23)
		5.2.2. Maîtrise de la gestion des accès utilisateur	
		5.2.3. Gestion des privilèges d'accès	
		5.2.4. Gestion des informations secrètes d'authentification des utilisateurs	
		5.2.5. Revue des droits d'accès utilisateur	
		5.2.6. Suppression ou adaptation des droits d'accès	
	5.3. Responsabilités des utilisateurs	5.3.1. Utilisation d'informations secrètes d'authentification	"Rendre les utilisateurs responsables de la protection de leurs informations d'authentification." (p. 27)
	5.4. Contrôle de l'accès aux systèmes d'authentification	5.4.1. Restriction d'accès à l'information	"Empêcher les accès non autorisés aux systèmes et aux applications." (p. 28)
		5.4.2. Sécuriser les procédures de connexion	
		5.4.3. Système de gestion des mots de passe	
		5.4.5. Contrôle d'accès au code source des programmes	
6. Cryptographie	6.1. Mesures cryptographiques	6.1.1. Politique d'utilisation des mesures cryptographiques	"Garantir l'utilisation correcte et efficace de la cryptographie en vue de protéger la confidentialité, l'authenticité et/ou l'intégrité de l'information." (p.31)
		6.1.2. Gestion des clés	
7. Sécurité physique et environnementale	7.1. Zones sécurisées	7.1.1. Périmètre de sécurité physique	"Empêcher tout accès physique non autorisé, tout dommage ou intrusion portant sur l'information et les
		7.1.2. Contrôle physique des accès	

Dimensions relatives à la maturité en sécurité de l'information	Sous-dimensions	Sous-sous-dimensions	Objectif
		7.1.3. Sécurisation des bureaux, des salles et des équipements	moyens de traitement de l'information de l'organisation." (p.34)
		7.1.4. Protection contre les menaces extérieures et environnementales	
		7.1.5. Travail dans les zones sécurisées	
		7.1.6. Zones de livraison et de chargement	
	7.2. Matériels	7.2.1. Emplacement et protection du matériel	"Empêcher la perte, l'endommagement, le vol ou la comprission des actifs et l'interruption des activités de l'organisation." (p. 37)
		7.2.2. Services généraux	
		7.2.3. Sécurité du câblage	
		7.2.4. Maintenance du matériel	
		7.2.5. Sortie des actifs	
		7.2.6. Sécurité du matériel et des actifs hors des locaux	
		7.2.7. Mise au rebut ou recyclage sécurisé(e) du matériel	
		7.2.8. Matériel utilisateur laissé sans surveillance	
		7.2.9. Politique du bureau propre et de l'écran vide	
8. Sécurité liée à l'exploitation	8.1. Procédures et responsabilités liées à l'exploitation	8.1.1. Procédures d'exploitation documentées	"S'assurer de l'exploitation correcte et sécurisée des moyens de traitement de l'information." (p. 42)
		8.1.2. Gestion des changements	
		8.1.3. Dimensionnement	
		8.1.4. Séparation des environnements de développement, de test et d'exploitation	
	8.2. Protection contre les logiciels malveillants	8.2.1. Mesures contre les logiciels malveillants	"Garantir que l'information et les moyens de traitement de l'information sont protégés contre les logiciels malveillants." (p. 46)
	8.3. Sauvegarde	8.3.1. Sauvegarde des informations	"Se protéger de la perte de données." (p.47)
	8.4. Journalisation et surveillance	8.4.1. Journalisation des évènements	"Enregistrer les évènements et générer des preuves." (p. 48)
		8.4.2. Protection de l'information journalisée	
		8.4.3. Journaux administrateur et opérateur	

Dimensions relatives à la maturité en sécurité de l'information	Sous-dimensions	Sous-sous-dimensions	Objectif
		8.4.4. Synchronisation des horloges	
	8.5. Maîtrise des logiciels en exploitation	8.5.1. Installation des logiciels sur des systèmes en exploitation	"Garantir l'intégrité des systèmes en exploitation." (p. 50)
	8.6. Gestion des vulnérabilités techniques	8.6.1. Gestion des vulnérabilités techniques	"Empêcher toute exploitation des vulnérabilités techniques." (p. 51)
		8.6.2. Restrictions liées à l'installation de logiciels	
	8.7. Considérations sur l'audit du système d'information	8.7.1. Mesures relatives à l'audit des systèmes d'information	"Réduire au minimum l'incidence des activités d'audit sur les systèmes en exploitation." (p.53)
9. Sécurité des communications	9.1. Management de la sécurité des réseaux	9.1.1. Contrôle des réseaux	"Garantir la protection de l'information sur les réseaux et des moyens de traitement de l'information sur lesquels elle s'appuie." (p. 54)
		9.1.2. Sécurité des services de réseau	
		9.1.3. Cloisonnement des réseaux	
	9.2. Transfert de l'information	9.2.1. Politiques et procédures de transfert de l'information	"Maintenir la sécurité de l'information transférée au sein de l'organisation et vers une entité extérieure." (p. 56)
		9.2.2. Accords en matière de transfert de l'information	
		9.2.3. Messagerie électronique	
		9.2.4. Engagements de confidentialité ou de non-divulgation	
10. Acquisition, développement et maintenance des systèmes d'information	10.1. Exigences de sécurité applicables aux systèmes d'information	10.1.1. Analyse et spécification des exigences de sécurité de l'information	"Veiller à ce que la sécurité de l'information fasse partie intégrante des systèmes d'information tout au long de leur cycle de vie." (p. 61)
		10.1.2. Sécurisation des services d'application sur les réseaux publics	
		10.1.3. Protection des transactions liées aux services d'application	
	10.2. Sécurité des processus de développement et d'assistance technique	10.2.1. Politique de développement sécurisé	"S'assurer que les questions de sécurité de l'information sont étudiées et mises en œuvre dans le cadre du cycle de développement des systèmes d'information." (p.63)
		10.2.2. Procédures de contrôle des changements apportés au système	
		10.2.3. Revue technique des applications après changement apporté `la plateforme d'exploitation	
		10.2.4. Restrictions relatives aux changements apportés aux progiciels	

Dimensions relatives à la maturité en sécurité de l'information	Sous-dimensions	Sous-sous-dimensions	Objectif
		10.2.5. Principes d'ingénierie de la sécurité des systèmes	
		10.2.6. Environnement de développement sécurisé	
		10.2.7. Développement externalisé	
		10.2.8. Phase de test de la sécurité du système	
		10.2.9. Test de conformité du système	
	10.3. Données de test	10.3.1. Protection des données de test	"Garantir la protection des données utilisées pour les tests." (p. 68)
11. Relations avec les fournisseurs	11.1. Sécurité de l'information dans les relations avec les fournisseurs	11.1.1. Politique de sécurité de l'information dans les relations avec les fournisseurs	"Garantir la protection des actifs de l'organisation accessibles aux fournisseurs." (p.69)
		11.1.2. La sécurité dans les accords conclus avec les fournisseurs	
		11.1.3. Chaine d'approvisionnement informatique	
	11.2. Gestion de la prestation de service	11.2.1. Surveillance et revue des services des fournisseurs	"Maintenir un niveau convenu de sécurité de l'information et de prestation de services, conformément aux accords conclus avec les fournisseurs." (p. 72)
		11.2.2. Gestion des changements apportés dans les services fournisseurs	
12. Gestion des incidents liés à la sécurité de l'information	12.1. Gestion des incidents liés à la sécurité de l'information et des améliorations	12.1.1. Responsabilités et procédures	"Garantir une méthode cohérente et efficace de gestion des incidents liés à la sécurité de l'information, incluant la communication des évènements et des failles liées à la sécurité." (p. 74)
		12.1.2. Signalement des évènements liés à la sécurité de l'information	
		12.1.3. Signalement des failles liées à la sécurité de l'information	
		12.1.4. Appréciation des évènements liés à la sécurité de l'information et prise de décision	
		12.1.5. Réponse aux incidents liés à la sécurité de l'information	
		12.1.6. Tirer des enseignements des incidents liés à la sécurité de l'information	
		12.1.7. Recueil de preuves	

Dimensions relatives à la maturité en sécurité de l'information	Sous-dimensions	Sous-sous-dimensions	Objectif
13. Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité	13.1. Continuité de la sécurité de l'information	13.1.1. Organisation de la continuité de la sécurité de l'information	"Il convient que la continuité de la sécurité de l'information fasse partie intégrante des systèmes de gestion de la continuité de l'activité." (p.78)
		13.1.2. Mise en œuvre de la continuité de la sécurité de l'information	
		13.1.3. Vérifier, revoir et évaluer la continuité de la sécurité de l'information	
	13.2. Redondances	13.2.1. Disponibilité des moyens de traitement de l'information	"Garantir la disponibilité des moyens de traitement de l'information." (p.80)
14. Conformité	14.1. Conformité aux obligations légales et réglementaires	14.1.1. Identification de la législation et des exigences contractuelles applicables	"Éviter toute violation des obligations légales, statutaires, réglementaires ou contractuelles relatives à la sécurité de l'information, éviter toute violation des exigences de sécurité." (p. 81)
		14.1.2. Droits de propriété intellectuelle	
		14.1.3. Protection des enregistrements	
		14.1.4. Protection de la vie privée et protection des données à caractère personnel	
		14.1.5. Réglementation relative aux mesures cryptographiques	
	14.2. Revue de la sécurité de l'information	14.2.1. Revue indépendante de la sécurité de l'information	"Garantir que la sécurité de l'information est mise en œuvre et appliquée conformément aux politiques et procédures organisationnelles." (p. 84)
		14.2.2. Conformité avec les politiques et les normes de sécurité	
		14.2.3. Examen de la conformité technique	

Échelle de mesure : N/A

Le *cadre de cybersécurité volontaire de l'Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM)* (2006) est le deuxième élément du tableau A4. C'est un cadre qui propose un ensemble de normes et de bonnes pratiques en cybersécurité qui s'inscrit dans le domaine financier (qui sont présentées dans le tableau A4.2). Structuré autour de 25 dimensions relatives à la sécurité de l'information, il permet notamment aux courtiers de gérer les risques en matière de cybersécurité. La force de ce cadre provient du fait qu'il ait été développé sur mesure pour les besoins des organisations financières, en prenant en compte les exigences particulières de cette industrie. Cette dernière idée évoque la valeur « Adéquation au contexte organisationnel » puisque ce cadre de référence vise à mettre en place des pratiques sécuritaires qui sont en concordance avec des activités financières.

Tableau A4.2 : Cadre de cybersécurité volontaire de l'Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM) (2006)

Dimensions	Recommandations
1. Gouvernance et gestion des risques	• Mettre en place le cadre de gouvernance présenté. • Participation du conseil d'administration et de la haute direction.
2. Pratiques exemplaires recommandées : petites et moyennes sociétés membres	• Préciser les renseignements qui doivent être protégés, de même que toutes les menaces et les risques qui y sont rattachés. • Protéger les biens à l'aide de mesures de protection convenables. • Détecter les intrusions, les infractions à la sécurité et l'accès non autorisé. • Intervenir en cas d'événement de cybersécurité potentiel. • Se remettre d'un événement de cybersécurité en rétablissant les activités et services normaux.
3. Enquête de sécurité sur le personnel et les menaces internes	• Mettre sur pied une équipe pluridisciplinaire. • Enjeux organisationnels. • Examiner les processus de filtrage de sécurité préalable à l'embauche. • Élaborer des politiques et des processus. • Activités de formation et d'éducation. • Surveiller les comportements douteux ou perturbateurs dès le processus d'embauche et y appliquer des mesures d'intervention. • Anticiper et gérer les situations négatives en milieu de travail. • Établir une distinction entre les fonctions et les privilèges minimum.

Dimensions	Recommandations
4. Sécurité physique et environnementale	• Les employés devraient appliquer le principe du « bureau propre », c'est-à-dire que les employés devraient ranger les documents renfermant des renseignements de nature délicate avant de quitter leur zone de travail. En outre, un bureau propre évite que les renseignements de nature délicate se retrouvent entre les mains de personnes qui ne sont pas autorisées par la loi à les consulter. Le personnel des services d'entretien et les agents de sécurité font partie des employés qui n'ont pas « besoin de savoir ». • N'autorisez les employés à avoir accès à votre zone de travail que s'ils ont un besoin opérationnel légitime. • Limitez l'accès au contenu de votre ordinateur en verrouillant l'écran lorsque vous vous absentez de votre poste de travail. • Protégez votre système d'information contre les variations de l'alimentation électrique ou les pannes de courant, et assurez-vous que votre ordinateur est branché dans un système d'alimentation sans coupure. • Effectuez périodiquement des copies de vos renseignements pour être à l'abri des sinistres, tel un incendie ou une inondation. • Les organisations de petite et moyenne taille doivent mettre en place un plan d'intervention portant sur les problèmes de sécurité physique. L'ampleur des contrôles de sécurité physique mis en oeuvre doit être proportionnelle au niveau de sensibilité des renseignements protégés.
5. Sensibilisation à la cybersécurité et formation	• Mettre en oeuvre des politiques portant sur l'utilisation sûre et acceptable des systèmes informatiques. • Rendre obligatoire la formation et la sensibilisation à la cybersécurité pour tout le personnel. La formation peut se dérouler en classe, en ligne ou en séance vidéo, et elle doit être offerte sur une base annuelle. Les attaques par piratage (p. ex., l'hameçonnage par courriel) visent souvent les cadres supérieurs; il est donc important que ces personnes suivent également la formation en cybersécurité. • Veiller à ce que tous les membres du personnel comprennent bien leur rôle et leurs responsabilités au chapitre de la cybersécurité. • Les utilisateurs devraient être avisés de ne pas ouvrir de courriels douteux ni de cliquer sur des liens douteux, quelle qu'en soit la source. • Les utilisateurs devraient être avisés de ne pas brancher des dispositifs au réseau, à moins d'avoir un motif professionnel légitime de le faire ou d'utiliser des dispositifs approuvés. • Les utilisateurs devraient être avisés d'appliquer de saines pratiques en matière de mot de passe. • Les utilisateurs devraient comprendre les dangers et les usages sûrs de médias externes (clés USB et DC). • Les utilisateurs ne devraient pas télécharger ou installer des applications non autorisées parce leur contenu peut être malveillant. • Les utilisateurs devraient comprendre que des sanctions seront imposées aux membres du personnel qui ne se conforment pas aux principes de sensibilisation à la cybersécurité et aux politiques de sécurité. • Les méthodes de formation continue pour les cadres de direction peuvent comprendre des séances vidéo ou des webinaires qui ont pour but de sensibiliser les utilisateurs et de partager des renseignements visés par mandat.

Dimensions	Recommandations
6. Évaluation des menaces et des vulnérabilités	• Utiliser périodiquement un outil automatisé pour évaluer les vulnérabilités de tous les systèmes du réseau. Remettre des listes de priorité renfermant les vulnérabilités les plus pressantes à chaque administrateur de système. • S'abonner à un service de renseignement sur les vulnérabilités afin de demeurer au fait des nouvelles menaces et expositions au risque. • Veiller à ce que les outils d'évaluation de la vulnérabilité utilisés soient périodiquement mis à jour et renferment les renseignements les plus à jour sur les vulnérabilités. • Veiller à ce que les logiciels/applications informatiques soient mis à jour périodiquement à l'aide de correctifs de sécurité. • Soumettre les correctifs essentiels à des essais avant de les faire passer au mode de production.
7. Sécurité réseau	• Acheter un pare-feu de la prochaine génération. Les petites entreprises peuvent se procurer ce type de pare-feu pour moins de 1 000$. Ces pare-feu s'accompagnent des services de sécurité supplémentaires suivants : o Le filtrage des sites Web renfermant des éléments malveillants. o La protection contre les virus sur Internet et contre les programmes malveillants qui infiltrent le réseau. o La technologie de prévention des menaces qui examine le trafic réseau pour détecter et empêcher les vulnérabilités sur Internet d'infiltrer le réseau. • Exiger l'authentification à double facteur pour tout accès à distance, notamment par RVP. • Fractionner le réseau interne de l'organisation pour faire en sorte que les utilisateurs n'aient accès qu'aux services dont ils ont besoin à des fins professionnelles. • Mettre en oeuvre une solution de contrôle d'accès au réseau afin d'empêcher des systèmes informatiques inconnus de communiquer avec le réseau de l'organisation. • Établir un comportement minimal normal pour les dispositifs réseau.
8. Protection des systèmes d'information	• Mettre en oeuvre des processus de sauvegarde et de recouvrement et effectuer périodiquement des sauvegardes de vos systèmes. • Déployer une solution de blocage de logiciels malveillants qui surveille en permanence les postes de travail, les serveurs et les appareils mobiles à l'aide de logiciels antivirus et anti-espion et de pare-feu. • Déployer une solution de blocage de logiciels malveillants qui comprend une fonction IPS en mode hôte. • Mettre en oeuvre une politique pour contrôler tous les accès à des supports amovibles. • Limiter l'utilisation à des dispositifs internes, p. ex., des clés USB, aux personnes et groupes qui ont un besoin professionnel légitime. • Utiliser des pare-feu personnels intégrés à Windows et des systèmes UNIX. • Analyser tous les supports pour éliminer les programmes malveillants avant de les importer sur l'ordinateur de l'organisation. • Installer toutes les mises à jour de sécurité des applications et des systèmes d'exploitation, notamment ceux offerts par la fonction intégrée de mise à jour de Windows. • Surveiller l'utilisation et la tentative d'utilisation de dispositifs externes. • Les utilisateurs à distance devraient recourir aux ressources d'accès de l'organisation à l'aide d'un RPV protégé et ils devraient être approuvés par authentification à double facteur.

Dimensions	Recommandations
9. Gestion des comptes utilisateur et contrôle d'accès	• Mettre en oeuvre un processus de gestion des comptes. • Gérer centralement tous les comptes à l'aide d'un système de gestion des comptes, notamment Microsoft Active Directory. • Configurer les dispositifs de réseau et de sécurité pour utiliser le système centralisé d'authentification. • Limiter le nombre de comptes à privilèges à ceux qui répondent à un besoin professionnel légitime. • Contrôler l'accès aux journaux d'audit du système informatique. • Examiner tous les comptes de système et désactiver les comptes qui ne peuvent être associés à un processus opérationnel et à un responsable. • Veiller à ce qu'une date d'échéance soit associée à chaque compte. • Mettre en place un processus d'annulation immédiate de l'accès au système à la cessation de la relation avec un employé ou un sous-traitant. La désactivation plutôt que l'élimination du compte permet de conserver une piste de vérification si une enquête s'avère nécessaire, par exemple. • Obliger les utilisateurs à se brancher à nouveau après une période fixe d'inactivité. • Exiger que tous les comptes d'employés comportent des mots de passe forts, renfermant des lettres, des chiffres et des caractères spéciaux. Veiller à ce qu'ils soient modifiés aux 90 jours et que les 15 mots de passe les plus récents ne puissent pas être utilisés comme nouveau mot de passe. • Exiger l'authentification à double facteur pour les comptes à privilèges ou les comptes donnant accès à des données ou à des systèmes de nature délicate. L'authentification à double facteur peut être activée à l'aide de cartes à puces
10. Gestion des actifs	• Déployer et tenir à jour un outil automatisé de recherche des actifs, et l'utiliser pour mettre au point un relevé des systèmes branchés au réseau privé et public de l'organisation. • Se brancher au serveur au moyen du Dynamic Host Configuration Protocol (DHCP) afin d'améliorer le relevé des actifs et détecter les systèmes inconnus à l'aide des renseignements fournis par le protocole. • Veiller à ce que le système de relevé soit mis à jour lorsque de nouveaux appareils approuvés se raccordent au réseau. • Déployer le Network Access Control (NAC) et l'authentification réseau à l'aide du protocole 802.1x. Ces services de sécurité empêchent des dispositifs non autorisés de se brancher au réseau. • Utiliser les certificats des clients pour valider et authentifier les systèmes avant de les brancher à un réseau.
11. Intervention en cas d'incident	• Consigner la date et l'heure où l'infraction a été découverte. • Alerter et mobiliser tous les membres de l'équipe d'intervention pour qu'ils lancent le plan de préparation. • Sécuriser le périmètre du lieu où a eu lieu l'infraction à la sécurité des données afin de conserver les éléments de preuve. • Empêcher toute autre perte de données. Mettre tous les systèmes informatiques touchés hors tension. • Documenter tous les éléments connus au sujet de l'infraction. • Interviewer toutes les personnes visées par la découverte de l'infraction et celles qui pourraient posséder de l'information à ce sujet. • Examiner les protocoles touchant la dissémination de l'information au sujet de l'infraction pour toutes les personnes visées au tout début du processus. • Évaluer les priorités et les risques d'après ce que vous savez au sujet de l'infraction. • Informer les autorités compétentes, y compris votre organisme de réglementation. • Aviser les organismes d'application de la loi, le cas échéant, pour qu'une enquête approfondie soit ouverte.
12. Partage de l'information et	• Élaborer une stratégie de partage de l'information et de collaboration. • Concevoir en tenant compte de la protection des renseignements personnels.

Dimensions	Recommandations
signalement d'une infraction	• Établir un processus de gouvernance significatif. • Insister sur le partage des renseignements sur les menaces, les vulnérabilités et l'atténuation pouvant servir à la mise en place de mesures. • Bâtir des relations interpersonnelles. • Limiter le partage de l'information à des circonstances précises • Garantir le partage de l'information, en effectuant des analyses sur les tendances à long terme. • Encourager le partage des pratiques exemplaires. (Recommandations élaborées par Microsoft)
13. Cyberassurance	• Protection de première partie (Embauche d'un professionnel) • Protection en responsabilité civile
14. Gestion des risques de fournisseur	Pour être efficace, la gestion des risques de fournisseur devrait être intégrée au programme de gestion des risques de l'organisation et comporter des processus établis et répétitifs uniformes dans tous les services de l'organisation.
15. Politique de cybersécurité	Les principaux éléments d'une politique de sécurité comprennent : • La portée – tous les renseignements, les systèmes, les installations, les programmes, les réseaux de données, et tous les utilisateurs de la technologie au sein de l'organisation (à l'interne et à l'extérieur), sans exception • La classification de l'information – doit fournir des définitions axées sur le contenu plutôt que des définitions plus générales de type « confidentiel » ou « restreint » • Les objectifs de la direction au chapitre de la manutention protégée de l'information dans chacune des catégories de la classification • La place de la politique dans le contexte des autres directives et documents de la direction • Les renvois aux documents d'appui, notamment les normes et lignes directrices du secteur • Des instructions précises au sujet de mandats de sécurité à la grandeur de l'organisation (p. ex., aucun partage des mots de passe) • La désignation spécifique des rôles et responsabilités établis • Les conséquences de la non-conformité (p. ex., mesures pouvant aller jusqu'au congédiement ou à la résiliation du contrat)
Échelle de mesure : N/A	

Le troisième élément du tableau, le cadre de référence *Forrester Information Security Maturity Model* (2014) a été développé pour aider les professionnels de sécurité de l'information à identifier les failles de leur programme de sécurité, à évaluer la maturité des processus de leur organisation et à mieux gérer leur stratégie de sécurité. Le cadre s'articule autour de quatre principaux domaines de la sécurité (*oversight, technology, process, people*) ainsi que de 25 composantes de la sécurité de l'information (voir le tableau A3.1 pour plus de détails). Étant donné le fait que ce cadre se concentre exclusivement sur les pratiques formelles en sécurité de l'information, il est ardu d'apporter des connaissances additionnelles à la liste de croyances, de valeurs et de caractéristiques du climat de la sécurité de l'information.

Le quatrième élément du tableau, le cadre de référence *O-ISM 3* de l'*Institute for Security and Open Methodologies* (2012), évalue la maturité de la sécurité de l'information par trois niveaux de processus de sécurité de l'information: stratégique, tactique et opérationnel (pour plus de

détails, consulter le tableau A4.3). Ce cadre de référence concerne majoritairement les pratiques formelles liées à la sécurité de l'information. Aucun contenu n'est lié à la culture, ni au climat organisationnels. Il est donc impossible d'y puiser de plus amples connaissances permettant d'enrichir la liste de croyances, de valeurs et de caractéristiques du climat de la sécurité de l'information.

Tableau A4.3 : O-ISM 3 (2012)

1. Security management – ISM3 Basics	To manage something means to define and achieve goals, while optimizing the use of resources. Management activities normally include the requirements to plan, direct, control, and coordinate.
2. Generic processes	Generic Processes provide the essential infrastructure for the implementation, assessment, and improvement of ISMS processes.
3. Specific processes – strategic management	Strategic management is responsible for selecting and designing services to provide value within the cost and risk parameters of the organization. Strategic management is accountable to stakeholders for the use of resources through governance arrangements. The customers of strategic management are therefore external and possibly internal stakeholders.
4. Specific processes – tactical management	Strategic management is the customer of tactical management in respect of ISM processes. Tactical management is accountable to strategic management for the performance of the ISMS and for the use of resources.
5. Specific processes – operational management	Operational management reports to the Chief Information Officer and the Information Security Tactical Manager.
Échelle de mesure : N/A	

Enfin, le dernier élément du tableau A4 est le cadre de référence *COBIT 5 for Information Security* (2012). Ce cadre de référence donne des directives pour aligner les facilitateurs (*enablers*) sur les objectifs de sécurité de l'information de l'organisation (voir le tableau A4.4). Il fait office de guide de pratiques et est composé de sept dimensions et de six niveaux de maturité. Il est d'ailleurs le seul cadre de référence qui s'intéresse à la culture, à l'éthique et aux comportements à l'égard de la sécurité de l'information (cf. la dimension 6). D'ailleurs, le fait que ce cadre de référence traite de l'éthique démontre l'importance de la valeur « Prédispositions éthiques de l'organisation » relevée précédemment.

Tableau A4.4: *COBIT 5 for Information Security* (2012)

Principles, policies and frameworks	Principles, policies and frameworks are the vehicle to translate the desired behaviour into practical guidance for day-to-day management.
Processes	Processes describe an organised set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.
Organizational Structure	Organisational structures are the key decision-making entities in an enterprise.
Culture, Ethics and Behavior	Culture, ethics and behaviour of individuals and of the enterprise are very often underestimated as a success factor in governance and management activities.
Information	Information is pervasive throughout any organisation and includes all information produced and used by the enterprise. Information is required for keeping the organisation running and well governed, but at the operational level, information is very often the key product of the enterprise itself.
Services, Infrastructure, Applications	Services, infrastructure and applications include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.
People, Skills and Competencies	People, skills and competencies are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions.
Échelle de mesure: échelle de 0 à 5	

Les cadres de référence de la maturité de la sécurité de l'information ont permis de retrouver quelques-unes des valeurs et des caractéristiques du climat de la sécurité de l'information mais n'ont pas permis d'apporter pas de connaissances additionnelles au bassin de croyances, de valeurs et de caractéristiques du climat de la sécurité de l'information. En effet, ayant pour objectif l'évaluation de la maturité en sécurité de l'information, ces instruments se focalisent avant tout sur la présence et la sophistication des pratiques formelles liées à la sécurité de l'information au sein des organisations.

1.4 La sensibilisation à la sécurité de l'information: un dernier thème connexe à explorer

Étant un construit connexe à la culture de la sécurité de l'information, il a paru pertinent de dédier une section à la sensibilisation à la sécurité de l'information. En effet, dans les publications traitant de la culture de la sécurité de l'information, la sensibilisation est mentionnée de manière récurrente (par exemple, Chen et al., 2015; Lyu & Zhang, 2015; Rantos et al., 2012). Dans la littérature, nombreuses sont les publications qui utilisent le construit de la sensibilisation à la sécurité de l'information et traitent principalement de l'importance d'éduquer et de former les employés d'une organisation quant à la sécurité de l'information.

Malgré le fait que le construit soit grandement étudié, il n'empêche qu'il souffre d'une absence de définition concise et uniforme (Hänsch & Benenson, 2014; Wolf et al., 2011) et qu'il est

étudié selon plusieurs angles. D'une part, le construit est étudié comme étant le niveau de prise de conscience des employés quant à la sécurité de l'information (Hänsch & Benenson, 2014). D'autre part, il est perçu comme représentant les efforts déployés par l'organisation pour sensibiliser ses employés (Maeyer, 2007).

1.4.1 Les instruments de mesure de la sensibilisation à la sécurité de l'information

Bien qu'il soit essentiel d'évaluer la sensibilisation à la sécurité de l'information pour identifier et corriger les lacunes potentielles qu'elle possède (Drevin et al., 2007), il existe peu d'instruments de mesure qui évaluent le construit. Les quelques outils existants sont principalement des questionnaires ou des sondages destinés aux employés d'une organisation (Wolf et al., 2011) où les intentions, les attitudes, les motivations et la satisfaction sont mesurées selon les perceptions des employés (Podsakoff & Organ, 1986). Les résultats qui en découlent peuvent être biaisés dans la mesure où les réponses sont inconsistantes ou influencées par la désirabilité sociale (Podsakoff & Organ, 1986; Lebek et al., 2014). Dans la littérature, il n'existe pas d'instruments mesurant l'efficacité des mécanismes de contrôle de sécurité (hacking éthique, tests de *phishing*, etc.). Holmberg & Sundstrom (2012) soulignent notamment l'importance d'établir des mécanismes qui évaluent les comportements des employés vis-à-vis des incidents en sécurité de l'information. Les instruments de mesure recueillis dans la littérature sont présentés dans le tableau A5 qui regroupe une description et une analyse de ces instruments de mesure.

Tableau A5 : Instruments de mesure de la sensibilisation à la sécurité de l'information

Nom de l'instrument	Auteur(s)	Dimensions	Description	Forces/faiblesses	Analyse
-	Albrechtsen & Hovden (2010)	1. Responsibility 2. Motivation 3. Information security vs. functionality 4. Importance of specific information security measures 5. Importance of generic security and safety measures 6. Reporting 7. Perceived skills and knowledge 8. Locking the computer 9. Carrying ID-cards 10. Checking unfamiliar persons without ID-cards 11. Manual virus-check	• Questionnaire • 28 items • Échelle de Likert • Validé auprès d'une organisation	**Force(s):** • Évalue le niveau de connaissance des politiques de sécurité de l'information et le comportement des employés **Faiblesse(s):** • Omet les connaissances générales en matière de sécurité de l'information	La valeur qui transparait de cet instrument de mesure est « Importance accordée au développement des ressources humaines » car l'instrument de mesure a pour but de jauger les le niveau de connaissances des politiques de sécurité de l'information de l'organisation des employés.
-	Kruger & Kearney (2006)	1. Attitude 2. Connaissances 3. Comportement	• Questionnaire • 35 questions • Validé auprès d'une entreprise	**Force(s):** • Se base sur la littérature de la psychologie sociale **Faiblesse(s)** : • Besoin d'échelles de mesures plus sophistiquées • Nécessite un plus grand bassin de questions	La valeur « Importance accordée au développement des ressources humaines » est manifestée à travers cet instrument de mesure car l'instrument de mesure a pour but d'évaluer l'attitude, les connaissances et le comportement des employés suite à leur formation et leur sensibilisation à la sécurité de l'information.

Le premier instrument de mesure du tableau A5, développé par Albrechtsen & Hovden (2010) a pour but d'évaluer l'efficacité d'un programme de sensibilisation (plus de détails sont fournis dans le tableau A5.1). L'instrument repose sur la mesure du niveau de connaissances et des comportements des employés par rapport aux politiques et procédures de sécurité de l'organisation, mais les connaissances générales en sécurité de l'information n'y sont pas jaugées. Or, selon Flores & Eksted (2016), la sensibilisation à la sécurité de l'information est composée des connaissances générales en sécurité de l'information ainsi que des connaissances des politiques et de procédures de sécurité organisationnelles. En analysant cet outil, on constate que la valeur communiquée est « Importance accordée au développement des ressources humaines » car il a pour but de jauger et d'ensuite améliorer le niveau de connaissances des politiques de sécurité de l'information de l'organisation des employés.

Tableau A5.1 : Instrument de mesure de la sensibilisation de la sécurité de l'information d'Albrechtsen & Hovden (2010)

Dimensions	Items
1. Responsibility	1. I have a responsibility to create and maintain a satisfactory level of information security at the company. 2. I have a personal responsibility to prevent that my use of IT-systems create virus infections. 3. I believe that user friendly systems are more important than secure systems. 4. Maintaining information security is equally important to efficient work. 5. One must always comply with information security requirements irrespective of the working situation.
2. Motivation	1. Writing passwords down on a note is OK. 2. There is no need to lock my computer when I leave it for a short period of time. 3. It is no wonder that people write down their passwords since they are difficult to remember.
3. Information security vs functionality	1. I think information security is bothersome for my working situation. 2. A lot of information security requirements cannot be met if I'm going to work efficient. 3. Managing information security is first and foremost a technical challenge
4. Importance of specific information security measures	1. Safe use of e-mail is important. 2. Keeping passwords secret is important. 3. Anti-virus tools are important. 4. Locking the computer when absent from it is important. 5. Cautious use of the internet is important. 6. Non-disclosure agreement is important.
5. Importance of generic security and safety measures	1. Reporting incidents is important. 2. Keeping ID-cards visible is important. 3. Following ethical guidelines is important. 4. Occupational accident prevention is important 5. Fire protection is important.
6. Reporting	1. If I observe or suspect an information security incident, I will report this to the management.
7. Perceived skills and knowledge	1. I have the necessary information skills and knowledge to handle information security in my working situation.

Dimensions	Items
8. [Security practices]	Locking the computer Carrying ID-Cards Checking unfamiliar persons without ID-cards Manual virus check
Échelle de mesure: *Yes/No*	

Pour ce qui est du deuxième instrument du tableau A5, l'instrument de mesure de Kruger & Kearney (2006) (voir le tableau A5.2 pour l'intégralité de l'instrument de mesure), mesure ce que les employés savent (connaissances), ce qu'ils ressentent (attitude) et ce qu'ils font (comportement) vis-à-vis de la sensibilisation à la sécurité de l'information. En revanche, l'instrument est encore un prototype et doit être amélioré. Les auteurs mentionnent notamment le besoin de remplacer l'échelle de mesure existante (une échelle de Likert à 3 points) pour une autre qui soit davantage sophistiquée (une échelle de Likert à 7 points). Étant donné que le construit doit être mesuré à plusieurs reprises, les auteurs évoquent aussi le besoin de développer une plus grande banque de questions. Cela empêcherait les employés d'apprendre les réponses attendues et de fausser les résultats de l'instrument de mesure à long terme. L'analyse de cet instrument de mesure révèle que la valeur « Importance accordée au développement des ressources humaines » est manifestée à travers cet outil. En effet, il vise notamment à évaluer l'attitude, les connaissances et le comportement des employés suite à leur formation et leur sensibilisation à la sécurité de l'information, signe qu'il y a un souci d'évaluer les ressources humaines afin de les développer.

Tableau A5.2 : Instrument de mesure de la sensibilisation de la sécurité de l'information de Kruger & Kearney (2006)

Dimensions	Explications
1. Knowledge	What you know.
2. Attitude	What you think.
3. Behavior	What you do.
Principes du programme de sensibilisation de Kruger & Kearney (2006)	
1. Always adhere to security policies.	
2. Keep passwords and personal identification numbers (PINs) secret.	
Use e-mail and the Internet with care.	
Be careful when using mobile equipment.	
Report incidents like viruses, thefts and losses.	
Be aware, all actions carry consequences.	

N.B.: Les auteurs ne présentent pas les items de leur instrument de mesure.

En conclusion, puisque ces instruments de mesure sont centrés sur la sensibilisation à la sécurité de l'information, il va de soi que la principale valeur qu'ils évoquent est « Importance accordée au développement des ressources humaines ». En effet, tous les instruments de mesure analysés dans cette -section ont pour but d'évaluer les connaissances des employés en matière de sécurité de l'information afin de déterminer leurs lacunes et parfaire leurs connaissances.

1.4.1 Les cadres de référence de la sensibilisation à la sécurité de l'information

À l'instar des instruments de mesure, on retrouve peu de cadres de références relatifs à la sensibilisation à la sécurité de l'information. La plupart des cadres de références de la sensibilisation à la sécurité de l'information ont pour objet de suggérer ou d'implanter des méthodes et des techniques de sensibilisation (programmes de sensibilisation, messages de sécurité, outils d'intelligence artificielle, etc.) sans être justifiés par des fondements théoriques (Tsohou et al., 2012).

Ces cadres de références sont exposés dans le tableau A6 en présentant leurs dimensions, leur description ainsi que leurs forces et faiblesses. Ils sont ensuite analysés afin de déterminer les potentielles croyances, valeurs et caractéristiques du climat qui pourraient leur être liées.

Tableau A6 : Cadres de référence de la sensibilisation à la sécurité de l'information

Cadre	Auteur(s)	Dimensions évaluées	Description	Forces et faiblesses	Analyse
Cybersecurity awareness and education framework	Kortjan & Von Solms (2014)	1. Strategic layer 2. Tactical layer 3. Preparation layer 4. Delivery layer 5. Monitoring layer 6. Resources	• Cadre de référence • Validé auprès de 2 experts en sécurité de l'information	**Force(s):** • Assiste l'implantation de la sensibilisation et la formation à la sécurité de l'information à l'échelle nationale **Faiblesse(s):** • Nécessite un processus de validation plus rigoureux	Étant donné que ce cadre de référence concerne la sensibilisation et la formation des employés à la sécurité de l'information, la valeur qui transparait ici est « Importance accordée au développement des ressources humaines ».
Security Awareness Program Evaluation	Rantos et al. (2012)	1. Surveys 2. Awareness/Security Days 3. Independent Observations 4. Audit Department Reports 5. Risk Department Reports 6. Security Incidents 7. Measuring the Effectiveness of Individual Modules 8. Awareness Sessions 9. Information Security Website 10. e-learning 11. E-mails 12. iNotices 13. Posters	• Méthodologie d'évaluation • Chaque dimension fait l'objet d'une pondération dans le calcul du score résultant de l'évaluation	**Force(s) :** • Se concentre sur l'aspect organisationnel de la sensibilisation à la sécurité de l'information • Fait l'utilisation de méthodes qualitatives et quantitatives **Faiblesse(s) :** • N'a pas fait l'objet d'un processus de validation	La valeur qui ressort de ce cadre de référence est « Importance accordée au développement des ressources humaines » car il évalue les programmes de sensibilisation à la sécurité de l'information tout en proposant des métriques à cet effet. De plus, le cadre de référence accorde une grande importance aux artefacts (posters, site web, etc.) et aux rituels (sessions de sensibilisation) de la sécurité de l'information, ce qui s'aligne avec la définition de la culture de la sécurité de l'information, élaborée plus tôt dans le chapitre 2.

Le premier cadre de référence du tableau A1.6 a été développé par Kortjan & Von Solms (2014) et s'intitule C*ybersecurity Awareness and Education Framework* (l'intégralité du cadre de référence se trouve à dans le tableau A6.1). Il guide l'implantation et la gestion d'un programme de sensibilisation à la sécurité de l'information à une échelle nationale. Néanmoins, il a été validé auprès de seulement deux experts en sécurité de l'information. Un cadre de référence de cette ampleur aurait nécessité une validation plus rigoureuse. Par ailleurs, il ne s'applique qu'à la sensibilisation à la sécurité de l'information sur Internet de la société sud-africaine et ne peut pas être appliqué à un autre pays compte tenu des différentes caractéristiques qui sont propres à chaque nation. L'examen de ce cadre de référence permet d'affirmer que la valeur qui transparait ici est « Importance accordée au développement des ressources humaines » puisque l'outil vise à développer les habiletés en termes de sécurité de l'information des individus par un programme de sensibilisation.

Tableau A6.1 : C*ybersecurity Awareness and Education Framework* de Kortjan & Von Solms (2014)

Dimensions	Explications
1. The strategic layer	This layer reflects the overall vision of the government concerning cyber-security awareness and education.
2. The tactical layer	This layer suggests the schemes that SA should employ to realise its cyber-security awareness and education goals.
3. The preparation layer	This layer prepares the contents of the scheme identified in the tactical layer.
4. The delivery layer	This layer defines the recipients of the preparations made in the preparation layer, namely: the target audience.
5. The monitoring layer	This layer examines the progress made by the scheme towards fulfilling the government's vision.
6. Resources	This component defines the resources, which should comprise the inputs in all the aforementioned layers.
Échelle de mesure: *N/A*	

En ce qui concerne Rantos et al. (2012), ils ont élaboré *Security Awareness Program Evaluation* (dont les détails sont dans le tableau A6.2), une méthodologie d'évaluation qui vise à évaluer et à gérer un programme de sensibilisation. L'avantage de ce cadre de référence est qu'il fait une évaluation approfondie du construit de la sensibilisation à la sécurité de l'information en organisation. En effet, toutes les activités d'un programme de sensibilisation font l'objet d'une évaluation à l'aide de méthodes qualitatives ou quantitatives. On constate que la valeur « Importance accordée au développement des ressources humaines » est appuyée par cet outil. La particularité de ce cadre de référence réside dans l'importance accordée aux artefacts (par exemple, posters, site web, etc.) et aux rituels (par exemple, les sessions de

sensibilisation) de la sécurité de l'information, ce qui soutient la définition de la culture élaborée dans ce chapitre.

Tableau A6.2: *Security Awareness Program Evaluation* de Rantos et al. (2012)

Dimensions	Explications
1. Surveys	Questionnaire-based surveys conducted on technical and security policy issues are one of the most reliable means of measuring a program's effectiveness.
2. Awareness Security Days	Security days offer a unique opportunity for the awareness team to directly communicate with employees and get their feedback. Metrics : statistical analysis of monthly surveys on specific organzation's divisions, statistical analysis of annual surveys, statistical analysis of security days attendance
3. Independent Observations	Independent observations on the security behaviour of employees should be carried out silently by awareness team members or representatives that have been assigned to this task.
4. Audit Department Reports	Auditing can be used to determine if security awareness related incidents identified by audits are declining.
5. Risk Department Reports	Input from the risk department can be used to identify risks related to security awareness. Metrics: statistical analysis of unsuccessful mock phishing attacks, statistical analysis of new threat bulletin's readership
6. Security Incidents	Security incidents are a valid point of reference regarding awareness program evaluation, and their processing should go beyond a simple check on the volume of incidents. Metrics: number of employees who are the source of at least one security incident that stems from nonsecure behavior (of the total number of employees), number of employees who are the source of at least one security incident that falls within their responsibilities but were not identified by them (of the total number of employees).
7. Measuring the Effectiveness of Individual Modules	Methods deployed for delivering awareness material cannot be equally effective.
8. Awareness Sessions	This is considered one of the easiest methods to evaluate given the existence of multiple communication paths for getting the required feedback.
9. Information Security Website	The number of employees who visit the Website where information security-related content is posted demonstrates users' interest in the corresponding topics. Metrics: statistical analysis of sessions attendance, statistical analysis of sessions effectiveness
10. e-learning	Statistics can provide useful information regarding the number of employees visiting, registering, and completing the e-learning program. Metrics: statistical analysis of information security Website visits, statistical analysis of e-learning program visits, statistical analysis of e-learning program, statistical analysis of completions
11. Emails	Awareness content delivered through emails is bound to reach the target. Metric: statistical analysis of email views
12. iNotices	As with emails where content is delivered electronically, links can be provided in iNotices for follow up information. Metric: statistical analysis of iNotices readings
13. Posters	Measuring posters contribution to the awareness program is not a trivial task and can, in general, be accomplished by independent observations. Metric: statistical analysis of poster downloads
Échelle de mesure: métriques et mesures qualitatives	

Après avoir analysé les cadres de référence de la sensibilisation à la sécurité de l'information, le constat tiré est le même que celui de l'analyse des instruments de mesure du même construit. En effet, la valeur qui en ressort est « Importance accordée au développement humain » étant donné qu'ils visent tous deux à guider la mise en place et a gestion d'un programme de sensibilisation à la sécurité de l'information au sein d'une organisation.

Annexe 2 : Protocole A - Rencontres individuelles avec les étudiants de la M.Sc. (étape A)

Préparation de la rencontre

- Bien s'assurer que le participant réponde aux critères de sélection.
- Faire parvenir au participant le protocole d'entrevue, si demandé.

Informations générales

- Lieu de la rencontre : Salle de réunion de HEC Montréal avec comme requis 2 places assises au minimum et une grande table
- Durée de la rencontre : 60-90 minutes
- Matériel nécessaire à la rencontre :
    - Appareil d'enregistrement audio
    - Papier et stylos (pour la prise de note du chercheur)
    - La définition de la culture de la sécurité de l'information imprimée sur une feuille de papier
    - Matériel du Q-sort (exercice de triage de carte) : 10 enveloppes et 39 cartes (selon la version préliminaire de l'instrument de mesure)
    - Formulaire de consentement (entrevue individuelle)

Avant la rencontre

- S'assurer que l'appareil d'enregistrement soit fonctionnel.

Pendant la rencontre

- Présenter le contexte de l'étude, faire signer le formulaire de consentement et demander l'autorisation d'enregistrer la rencontre:

« Je travaille actuellement sur mon mémoire en vue d'obtenir mon diplôme de M.Sc. en TI à HEC Montréal. Mon objectif de recherche est de mieux comprendre la culture de la sécurité de l'information et d'élaborer un instrument de mesure permettant de la mesurer.
La collecte de données que j'effectue a pour but d'amasser les commentaires et les impressions des participants quant à cet instrument de mesure. Soyez assuré qu'il n'y a pas de bonnes ou de mauvaises réponses; je souhaite seulement obtenir votre opinion d'expert sur le sujet.
Avant de procéder à la collecte de données, veuillez s'il-vous-plaît signer le formulaire de consentement. Je vous demande dans celui-ci de me donner la permission d'enregistrer vos propos afin de pouvoir me concentrer sur l'entrevue et de m'assurer de ne rien oublier. Les résultats de toutes les rencontres seront agrégés et serviront à améliorer l'instrument qui servira à mesurer la culture. Prenez le temps nécessaire pour prendre connaissance du formulaire et n'hésitez pas à me poser des questions. »

- Ramasser la feuille de consentement dûment signée.

- Démarrer une discussion au sujet de **la culture de la sécurité de l'information** avec le participant en posant les questions suivantes :
    - Quand je parle de « culture de la sécurité de l'information », est-ce un concept auquel vous avez déjà été confronté?
    - Si oui :
        - Quels en sont les éléments pertinents ?
        - En avez-vous une définition formelle ?
    - Si non :
        - Qu'est-ce que le concept de sécurité de l'information évoque pour vous ? À quoi réfère-t-il ? Quels aspects en sont selon vous importants ou pertinents ?

- Présenter la **définition écrite de la culture de la sécurité de l'information au participant** et, après quelques secondes données au participant pour en faire la lecture, poser les questions suivantes :

- Cette définition vous semble-t-elle juste? Complète ? Auriez-vous des suggestions de modifications, d'ajouts ou de retraits ?

- On en est à l'élaboration d'un instrument de mesure de la culture de la sécurité de l'information et on voudrait votre opinion sur le sujet. [Celui-ci est présenté en annexe à ce protocole.]

a) Exploration des dimensions :
    - Donner au participant les enveloppes sur lesquelles sont inscrites les **dimensions et leur définition**.
    - Demander au participant de **réagir aux dimensions et à leur définition** en posant les questions suivantes :
        - Les dimensions présentées semblent-elles liées à la culture de la sécurité de l'information?
        - Selon vous, devrait-on ajouter, modifier ou bien retirer une ou plusieurs dimensions? Pourquoi ?

Exercice de Q-sort :

- Présenter l'exercice et les instructions :
  « *Vous avez maintenant en main les enveloppes sur lesquelles sont inscrites chacune des dimensions de la culture de la sécurité de l'information. Nous allons maintenant réaliser un petit exercice. Il consiste à associer les items (imprimés sur des cartes) aux dimensions de la sécurité de l'information (imprimées sur les enveloppes). Nonobstant la discussion que l'on vient d'avoir sur la pertinence des dimensions, veuillez* ***classer les items imprimés sur des cartes*** *dans les différentes dimensions de ce qu'est la culture de la sécurité. Pour ce faire, basez-vous sur le lien entre la dimension et sa définition et le sens de l'item présenté sur la carte. Si vous pensez que l'item présenté sur une carte n'est lié à aucune dimension, vous pouvez mettre la carte de côté. Veuillez réaliser cet exercice en pensant à haute voix, c'est-à-dire en exprimant tout ce qui vous vient à l'esprit, votre raisonnement, les questions que vous vous posez, au fur et à mesure de l'exercice. N'hésitez pas à me poser des questions si vous avez besoin de clarifications sur la marche à suivre, mais il m'est impossible de vous donner de plus amples explications sur le contenu, autant sur les dimensions que sur les items. Vos commentaires/réactions/raisonnements/questions sur ces dimensions/items sont les bienvenus. Lors de l'analyse de l'enregistrement, cela nous permettra d'identifier et d'améliorer les dimensions ou les items qui vous ont posé problème.»*

- Lorsque l'exercice est terminé, demander au participant de faire part de ses observations par rapport au Q-sort en lui posant les questions suivantes:
    - Maintenant que vous avez fait l'exercice, avez-vous d'autres commentaires à formuler par rapport aux dimensions de l'instrument? Pensez-vous qu'il y a des dimensions à ajouter, à modifier ou à supprimer?
    - Les dimensions vous ont-elles posé des difficultés? Si oui, lesquelles?
    - La compréhension des cartes vous a-t-elle posé des difficultés particulières? Si oui, lesquelles? Avez-vous d'autres commentaires par rapport au contenu des cartes? Pensez-vous qu'il a des cartes à ajouter, à modifier ou à retirer? Est-ce que certaines vous ont semblé redondantes ?
    - Quel a été le plus grand défi que vous avez rencontré lors de cet exercice?

- Conclure la rencontre:
    - Demander au participant s'il veut émettre des commentaires ou des suggestions quant au déroulement de la rencontre.
    - Remercier le participant.
    - Demander au participant de ne pas toucher au résultat de leur exercice.
    - Arrêter l'enregistrement et ramasser le matériel utilisé lors de la rencontre tout en prenant bien soin d'insérer les items dans les enveloppes selon le classement du répondant.

Après la rencontre

- Compléter les notes prises en cours d'entrevue.
- Inscrire ses impressions sur l'ensemble de l'entrevue.
- Prendre en note le détail du classement du participant

Annexe 3 : Protocole B – Groupe de discussion avec experts en sécurité de l'information

Préparation de la rencontre

- Bien s'assurer que les participants répondent aux critères de sélection.
- Faire parvenir aux participants le protocole d'entrevue, si demandé.

Informations générales

- Lieu de la rencontre : Salle de réunion avec pour requis au minimum six places assises, une grande table, un projecteur, une surface sur laquelle coller des feuilles.
- Durée de la rencontre : environ 180 minutes
- Matériel nécessaire à la rencontre :
    - Appareils d'enregistrement audio
    - Appareil photo
    - Papier et stylos (pour la prise de note du chercheur et des participants)
    - Acétates pour la présentation
    - Les 27 éléments imprimés sur des feuilles A4
    - Les 3 grandes enveloppes qui contiennent chacune les 4 paquets de cartes (3x5 pouces).
    - Un rouleau de scotch tape
    - Trois formulaires de consentement (groupe de discussion)

Avant la rencontre

- S'assurer que les appareils d'enregistrement et le projecteur soient fonctionnels.
- Installer des feuilles et des stylos à chacune des places des participants.
- Pour l'exercice de priorisation des éléments:
    - 3 paquets de 7 cartes sur les croyances
    - 3 paquets de 9 cartes sur les valeurs
    - 3 paquets de 11 cartes sur le climat

    Chaque carte doit contenir le nom d'un élément donné, sa définition et des items (en guise d'exemple).

    a. Mélanger chaque paquet de cartes pour éviter de les présenter dans le même ordre aux participants.

    b. Ranger chaque paquet de cartes dans une enveloppe.

    c. S'assurer d'avoir imprimé sur des feuilles A4 le nom des éléments.

1. Mise en contexte

- Présenter le contexte de l'étude et l'objectif de la rencontre et faire signer les formulaires de consentement :

«Avant de commencer la rencontre, veuillez s'il-vous-plaît signer le formulaire de consentement. Nous vous demandons dans celui-ci de nous donner la permission d'enregistrer vos propos afin de pouvoir nous concentrer sur le contenu de la discussion et de nous assurer de ne rien oublier. Les résultats de cette rencontre seront agrégés et serviront à valider les éléments de la culture et du climat de la sécurité de l'information. Prenez le temps nécessaire pour prendre connaissance du formulaire et n'hésitez pas à me poser des questions. Nous aimerions vous remercier d'avoir accepté de participer à ce groupe de discussion. Comme vous le savez, l'objectif de recherche de notre projet est d'élaborer une liste d'éléments de la sécurité de l'information qui soit complète et parcimonieuse. Ce groupe de discussion a justement pour but d'amasser les commentaires et les impressions des participants quant à ces éléments.

- Ramasser les feuilles de consentement dûment signées.
- Demander à chacun des participants de se présenter (si ça n'a pas été naturellement fait).
- Expliquer aux participants le fonctionnement du groupe de discussion :

« Avant de continuer, je vais vous expliquer comment cette séance va se dérouler. Après chaque question que je vais vous poser ou chaque exercice que je vais vous assigner, vous pourrez prendre quelques secondes afin de réfléchir à votre réponse; si vous le désirez, vous pourrez prendre des notes, de manière individuelle, sur les feuilles qui vous ont été fournies. Une fois que vous serez tous prêts à partager le fruit de votre réflexion, nous allons procéder à un tour de table. L'ordre n'est pas important. Le but de vous avoir tous au même moment dans la même pièce est de vous permettre d'échanger et de vous alimenter les uns des autres. Si ce qu'un collègue dit vous fait penser à quelque chose, même si ce n'est pas sur votre feuille, exprimez-le. Ce sont vos réflexions individuelles et collectives qui, dans le cadre de cette discussion, nous intéressent.»

2**.** Démarrer une discussion sur la culture de la sécurité de l'information : « Est-ce que la culture de la sécurité de l'information est un concept discuté dans votre contexte? »

- Si oui :
  - Comment est-elle devenue un thème pertinent dans votre contexte ?
  - Quels en sont les éléments pertinents ?
  - Avez-vous essayé de la mesurer ?
- Si non :
  - Est-ce que la culture de la sécurité de l'information est un concept important dans votre pratique ? Pourquoi ?
  - Qu'est-ce que le concept de sécurité de l'information évoque pour vous ? Quels sont ses aspects qui sont, selon vous, les plus importants ou pertinents ?

3. Présenter le pourquoi de la recherche : montrer le modèle du continuum de la culture de la sécurité de l'information.

4. Demander leur définition de la culture de la sécurité de l'information : « *Quelle est votre définition de la culture de la sécurité de l'information?* »

5. Présenter la variable dépendante (la mise en œuvre de pratiques sécuritaires par les employés) et démarrer une discussion à ce sujet.

- *La mise en œuvre des pratiques sécuritaires par les employés grâce à la conformité et l'intelligence en sécurité de l'information vous semble-t-elle pertinente pour comprendre la culture de la sécurité de l'information?*
- *Dans votre contexte, comment expliquez-vous la mise en œuvre des pratiques sécuritaires par les employés?*

6. Présenter les définitions des concepts abordés au cours du groupe de discussion (culture de la sécurité de l'information, croyances, valeurs, climat de la sécurité de l'information) :

La **culture de la sécurité de l'information** au sein d'une organisation est un ensemble de manifestations visibles et invisibles partagées par les membres de l'organisation. Ces manifestations incluent les valeurs, les croyances, les hypothèses, les pratiques formelles et informelles, le climat et les artéfacts qui influencent les décisions et les comportements des employés quant à la protection de l'information.
Les **croyances organisationnelles** reflètent des convictions profondes, qui existent souvent universellement au-delà des murs de l'entreprise et que l'entreprise a faites siennes.
Les **valeurs organisationnelles** reflètent des idées implicites ou explicites partagées au sein de l'organisation sur ce qui est important pour l'organisation ou à quoi l'organisation tient beaucoup.
Le **climat de la sécurité de l'information** correspond aux perceptions partagées au sein de l'organisation quant aux politiques organisationnelles, aux règles, aux normes et aux pratiques de sécurité mises en œuvre. Le climat de la sécurité de l'information représente les perceptions partagées par les employés à propos de « comment les choses se passent chez nous. ».

7. Faire les 3 exercices de priorisation des éléments.

7.1. Exercice de priorisation des croyances

- *« Nous allons maintenant réaliser le premier exercice de priorisation. J'ai ici 7 cartes sur lesquelles sont inscrites les croyances, leur définition et des items pouvant faire partie d'un questionnaire, à titre d'exemple. Je vous demande de classer par ordre de priorité les cartes qui, selon vous, favorisent la mise en œuvre des pratiques sécuritaires par les employés (concept que nous avons expliqué un peu plus tôt) : en d'autres mots, on devrait retrouver au haut de la liste les croyances qui sont, selon vous, les plus importantes. Pour cela, basez-vous sur le lien entre la mise en œuvre de pratiques sécuritaires par les employés et la définition ainsi que les exemples des croyances. Pour effectuer le classement avec les cartes, je vous suggère de les ordonner sur la table car je dois en prendre une photo. Veuillez réaliser cet exercice individuellement. Sachez qu'il n'y a pas de bonnes ou de mauvaises réponses, je souhaite seulement obtenir votre opinion sur le sujet. Je vais vous laisser quelques minutes pour réaliser cet exercice. Faites-moi signe lorsque vous aurez fini de faire le classement. Nous allons faire un tour de table afin que chacun puisse partager sa réflexion. »*
- Distribuer les enveloppes étiquetées « Exercice de priorisation – Croyances » à chacun des participants.
- Une fois que les participants aient fini de réaliser leur exercice, prendre rapidement une photo de chacun des classements.
- Placer les classements de chacun côte-à-côte pour qu'ils puissent les comparer et en discuter.
- Faire le tour de table : « *Je vous invite à nous faire part de votre raisonnement pour le classement de chaque élément.* »
- *« À la lumière des réflexions de chacun, nous allons maintenant faire le même exercice de manière collective. Je vous invite donc à discuter entre vous afin de réaliser la priorisation des éléments ensemble. Au fur et à mesure que vous arrivez sur un consensus quant au classement d'un élément, nous allons l'afficher sur le mur. »*
- Afficher les éléments sur le côté **gauche** du mur.

- Répéter cet exercice de classification pour les valeurs et les caractéristiques du climat. Les feuilles sur lesquelles sont imprimées les valeurs vont au milieu du mur et celles des caractéristiques du climat à droite.

8. Discussion sur le classement collectif

- *« Maintenant que l'on voit ensemble le classement collectif global, y a-t-il quelque chose que vous voudriez modifier/ajouter/enlever? En particulier, je vous demande s'il y a des aspects qui ont été oubliés et qui vous semblent importants ou au contraire, des aspects qui sont inclus ici et dont vous ne voyez pas la pertinence. Prenez quelques minutes pour y penser. »*
- *Si le temps le permet :*
    - *Pour l'instant, on a un classement collectif pour les croyances, les valeurs et les caractéristiques du climat. Si le temps le permet, faire un exercice collectif global où on demande aux participants de classer les éléments. Commencer par leur demander parmi éléments, lesquels seraient dans leur top 10 – voir s'ils sont capables de s'entendre sur la nature et la priorisation du top 10.*
- Demander aux participants : « *Pensez-vous que les employés de votre organisation serait en mesure de répondre aux exemples (qui sont sur les cartes) sur une échelle allant de « complètement en désaccord à complètement en accord?* »

9. Conclusion

- Remercier les participants.
- Demander aux participants s'ils sont prêts à nous accorder une heure de plus pour une autre étape du projet.
- Arrêter l'enregistrement et ramasser le matériel utilisé lors de la rencontre.

Annexe 4 : Protocole C – Rencontres individuelles avec les professionnels en sécurité de l'information

Préparation de la rencontre

- Bien s'assurer que les participants répondent aux critères de sélection.
- Faire parvenir aux participants le protocole d'entrevue, si demandé.

Informations générales

- Lieu de la rencontre : Professionnels : Selon leur désir : leur bureau ou une salle de réunion de HEC Montréal
- Durée de la rencontre : environ 60-90 minutes
- Matériel nécessaire à la rencontre :
    - Appareils d'enregistrement audio
    - Appareil photo
    - Papier et stylos (pour la prise de note du chercheur et des participants)
    - Acétates pour la présentation
    - Les 3 paquets de cartes (3x5 pouces).
    - Formulaire de consentement (rencontre individuelles)

Avant la rencontre

- S'assurer que l'appareil d'enregistrement soit fonctionnel
- Pour l'exercice de priorisation des éléments organisationnels:
  - 1 paquet de 7 cartes sur les croyances
  - 1 paquet de 10 cartes sur les valeurs
  - 1 paquet de 11 cartes sur les caractéristiques du climat

  Chaque carte doit contenir le type et le numéro de l'élément, sa définition et ses propositions sous-jacentes.

  a. Mélanger chaque paquet de cartes pour éviter de les présenter dans le même ordre aux participants.

  b. Ranger chaque paquet de cartes dans une enveloppe.

1. Mise en contexte

- Présenter le contexte de l'étude et l'objectif de la rencontre et faire signer les formulaires de consentement :

«Avant de commencer la rencontre, veuillez s'il-vous-plaît signer le formulaire de consentement. Nous vous demandons dans celui-ci de nous donner la permission d'enregistrer vos propos afin de pouvoir nous concentrer sur le contenu de la discussion et de nous assurer de ne rien oublier. Les résultats de cette rencontre seront agrégés et serviront à valider les croyances, les valeurs et les caractéristiques du climat de la sécurité de l'information. Prenez le temps nécessaire pour prendre connaissance du formulaire et n'hésitez pas à me poser des questions. Nous aimerions vous remercier d'avoir accepté de participer à cette rencontre. Comme vous le savez, l'objectif de recherche de notre projet est de conceptualiser la culture et le climat de la sécurité de l'information et à élaborer une liste des éléments les composant qui soit complète et parcimonieuse. Cette rencontre a justement pour but d'amasser les commentaires et les impressions des participants quant à ces éléments de la sécurité de l'information.»

- Ramasser les feuilles de consentement dûment signées.
- Demander à chacun des participants de se présenter (et ne pas oublier de lui demander son nombre d'années d'expérience de travail en général et en sécurité de l'information)

2**.** Démarrer la présentation et la discussion sur la culture de la sécurité de l'information : « Est-ce que la culture de la sécurité de l'information est un concept discuté dans votre contexte? »

- Si oui :
    - Comment est-elle devenue un thème pertinent dans votre contexte ?
    - Quels en sont les éléments pertinents ?
    - Avez-vous essayé de la mesurer ?

- Si non :
    - Est-ce que la culture de la sécurité de l'information est un concept important dans votre pratique ? Pourquoi ?
    - Qu'est-ce que le concept de sécurité de l'information évoque pour vous ? Quels sont ses aspects qui sont, selon vous, les plus importants ou pertinents ?

3. Présenter le pourquoi de la recherche : montrer le modèle du continuum de la culture de la sécurité de l'information.

4. Demander leur définition de la culture de la sécurité de l'information : « *Quelle est votre définition de la culture de la sécurité de l'information?* »

5. Présenter la variable dépendante (la mise en œuvre de pratiques sécuritaires par les employés) et démarrer une discussion à ce sujet.

- *La mise en œuvre de pratiques sécuritaires par les employés grâce à la conformité et l'intelligence en sécurité de l'information vous semble-t-elle pertinente pour comprendre la culture de la sécurité de l'information?*
- *Dans votre contexte, comment expliquez-vous la mise en œuvre de pratiques sécuritaires par les employés?*

6. Présenter les définitions des concepts abordés au cours du groupe de discussion (culture de la sécurité de l'information, croyances, valeurs, climat de la sécurité de l'information) :

La **culture de la sécurité de l'information** au sein d'une organisation est un ensemble de manifestations visibles et invisibles partagées par les membres de l'organisation. Ces manifestations incluent les valeurs, les croyances, les hypothèses, les pratiques formelles et informelles, le climat et les artéfacts qui influencent les décisions et les comportements des employés quant à la protection de l'information.
Les **croyances organisationnelles** reflètent des convictions profondes, qui existent souvent universellement au-delà des murs de l'entreprise et que l'entreprise a faites siennes.
Les **valeurs organisationnelles** reflètent des idées implicites ou explicites partagées au sein de l'organisation sur ce qui est important pour l'organisation ou à quoi l'organisation tient beaucoup.
Le **climat de la sécurité de l'information** correspond aux perceptions partagées au sein de l'organisation quant aux politiques organisationnelles, aux règles, aux normes et aux pratiques de sécurité mises en œuvre. Le climat de la sécurité de l'information représente les perceptions partagées par les employés à propos de « comment les choses se passent chez nous. ».

7. Faire les trois exercices de priorisation des éléments (croyances, valeurs, caractéristiques du climat).

7.1. Exercice de priorisation des croyances.

- *« Nous allons maintenant réaliser le premier exercice de priorisation. J'ai ici sept cartes sur lesquelles sont inscrites, sur chacune d'elles, le numéro d'une croyance, sa définition et ses propositions, que je vais vous distribuer une à une. Une fois que toutes les cartes sont entre vos mains, je vous demande de classer par ordre de priorité les croyances qui, selon vous, favorisent la mise en œuvre de pratiques sécuritaires par les employés (concept que nous avons expliqué un peu plus tôt) : en d'autres mots, on devrait retrouver au haut de la liste les croyances qui sont, selon vous, les plus importantes. Pour cela, basez-vous sur le lien entre la mise en œuvre des pratiques sécuritaires et la définition ainsi que les propositions inscrites sur les cartes. Pour effectuer le classement avec les cartes, je vous suggère de les ordonner sur la table car je dois en prendre une photo. Sachez qu'il n'y a*

pas de bonnes ou de mauvaises réponses, je souhaite seulement obtenir votre opinion sur le sujet.»

- Distribuer les cartes de l'enveloppe étiquetée « Exercice de priorisation – Croyances » au participant.
- Une fois que le participant ait fini de réaliser leur exercice, prendre rapidement une photo de son classement.

7.2. Répéter cet exercice de classification pour les valeurs.

7.3. Répéter cet exercice de classification pour les caractéristiques du climat.

8. Faire une rétroaction sur les exercices :

- Sortir le top 3 de chaque classement et les présenter au participant.
- *« À la lumière de tous les éléments que vous avez vu, y a-t-il quelque chose que vous voudriez modifier/ajouter/enlever? Si on regarde le top 3 de chaque classement, pensez-vous qu'on a les éléments les plus importants? Il y a-t-il quelque chose qui n'aurait pas été couvert dans ces tops 3? Prenez quelques minutes pour y penser.»*
- Demander au participant : « *Pensez-vous que les employés de votre organisation serait en mesure de répondre aux exemples (qui sont sur les cartes) sur une échelle allant de « complètement en désaccord à complètement en accord?* »

9. Conclusion

- Remercier le participant.
- Demander aux participants s'ils sont prêts à nous accorder une heure de plus pour une autre étape du projet.
- Arrêter l'enregistrement et ramasser le matériel utilisé lors de la rencontre.

Annexe 5 : Cartes des exercices de priorisation de l'étape B

Croyances

RESPONSABILITÉ D'ASSURER LA SÉCURITÉ DE L'INFORMATION

Croyance partagée dans l'organisation qui indique qui a la responsabilité d'assurer la sécurité de l'information.

Par exemple :

- *Dans mon organisation, on croit que la sécurité de l'information est une responsabilité partagée par tous les employés de l'organisation.*
- *Dans mon organisation, on croit que c'est le département informatique (ou l'équivalent) qui a la responsabilité d'assurer la sécurité de l'information.*

VISION DE L'ORGANISATION QUANT À LA NATURE DES DÉFIS EN TERMES DE SÉCURITÉ DE L'INFORMATION

Croyance partagée dans l'organisation qui indique la vision que l'organisation a de la nature des défis rencontrés en sécurité de l'information.

Par exemple :

- *Dans mon organisation, on croit que la sécurité de l'information nécessite une vision globale qui inclut des aspects techniques, humains et managériaux.*
- *Dans mon organisation, on croit que la sécurité de l'information doit être traitée comme un problème technique.*

IMPORTANCE GÉNÉRALE QU'A LA SÉCURITÉ DE L'INFORMATION DANS L'ORGANISATION

Croyance partagée dans l'organisation qui réfère à l'importance générale que l'on donne à la sécurité de l'information.

Par exemple :

- *Dans mon organisation, on croit que la sécurité de l'information doit être une priorité organisationnelle.*
- *Dans mon organisation, on croit que l'argent investi en sécurité de l'information représente une dépense inutile.*

AUTO-EFFICACITÉ ORGANISATIONNELLE FACE AUX MENACES

Croyance partagée dans l'organisation qui réfère à la capacité de l'organisation à se défendre contre les menaces à la sécurité de l'information.

Par exemple :

- *Dans mon organisation, on croit qu'il est possible de protéger l'information contre les actions des personnes malveillantes.*
- *Dans mon organisation, on croit qu'il est possible de mettre en place un ensemble de moyens pour contrer les menaces à la sécurité de l'information.*

RESPONSABILITÉ MORALE DE PROTÉGER L'INFORMATION

Croyance partagée dans l'organisation qui réfère à l'obligation morale que l'entreprise a de protéger les informations.

Par exemple :

- *Dans mon organisation, on croit qu'on a l'obligation de faire ce que l'on peut pour protéger l'information.*
- *Dans mon organisation, on croit qu'on a l'obligation d'assurer la sécurité de l'information afin de protéger les intérêts de ceux qui souffriraient d'un incident qui la mettrait en jeu.*

NATURE GÉNÉRALE DE L'ÊTRE HUMAIN (SES MOTIVATIONS PROFONDES)

Croyance partagée dans l'organisation quant à la nature générale de l'être humain, et plus spécifiquement en ce qui a trait aux raisons qui motivent ses actions.

Par exemple :

- *Dans mon organisation, on croit que les gens agissent dans le meilleur intérêt de l'organisation quand on leur fait confiance.*
- *Dans mon organisation, on croit qu'exercer un contrôle très strict est le seul moyen de s'assurer que les gens font ce qu'ils sont censés faire.*

LE MAILLON FAIBLE EN SÉCURITÉ DE L'INFORMATION

Croyance partagée dans l'organisation quant au rôle que joue l'être humain dans la sécurité de l'information.

Par exemple :

- *Dans mon organisation, on croit que les gens peuvent jouer un rôle essentiel pour minimiser les risques liés à la sécurité de l'information.*
- *Dans mon organisation, on croit que les gens constituent le maillon faible en sécurité de l'information.*

Valeurs

BASES GÉNÉRALES SUR LESQUELLES LES DÉCISIONS SONT PRISES DANS L'ORGANISATION

Réfère aux bases sur lesquelles les décisions sont généralement prises au sein de l'organisation.

Par exemple :

- *Dans mon environnement de travail, les « chiffres » (analyses quantitatives, métriques, benchmarking, etc.) sont toujours les critères les plus importants au moment de prendre une décision.*
- *Dans mon environnement de travail, on privilégie l'intuition et les émotions (« gut feelings ») plutôt que les « chiffres » (analyses quantitatives, métriques, benchmarking, etc.) au moment de prendre une décision.*

HORIZON TEMPOREL HABITUEL DE LA PLANIFICATION DANS L'ORGANISATION

Réfère aux habitudes de planification de l'organisation.

Par exemple :

- *Dans mon environnement de travail, on se concentre principalement sur la planification d'objectifs à court terme.*
- *Dans mon environnement de travail, on croit aux bénéfices de la planification à long terme (3 ans et plus).*

PRÉDISPOSITIONS ÉTHIQUES DE L'ORGANISATION

Réfère à la place de l'éthique dans l'organisation.

Par exemple :

- *Les comportements éthiques sont la norme dans mon environnement de travail.*
- *Dans mon environnement de travail, le respect de principes éthiques est intégré aux processus décisionnels.*

ATTITUDE DES EMPLOYÉS ENVERS LA CONFORMITÉ

Réfère à l'attitude générale des employés envers la conformité et le respect des règles et des politiques définies au sein de l'organisation.

Par exemple :

- *Dans mon environnement de travail, le respect des politiques et règlements de l'organisation est très important.*
- *Dans mon environnement de travail, l'autonomie individuelle est plus valorisée que le respect des politiques et règlements de l'organisation.*

IMPORTANCE ACCORDÉE AU DÉVELOPPEMENT DES RESSOURCES HUMAINES

Réfère à la place du développement des connaissances et des habiletés des employés dans l'organisation.

Par exemple :

- *Dans mon environnement de travail, on prend au sérieux le développement continu des habiletés de chaque employé afin de maximiser sa contribution au succès de l'organisation.*
- *Dans mon environnement de travail, on appuie fortement la formation continue des employés.*

ATTITUDE GÉNÉRALE DES EMPLOYÉS FACE AU CHANGEMENT

Réfère à l'attitude générale des employés face au changement organisationnel.

Par exemple :

- *Dans mon environnement de travail, on accepte facilement que les façons de faire évoluent et changent.*
- *Dans mon environnement de travail, le changement rend les gens très inconfortables.*

FORCE DU RÉSEAU AU SEIN DE L'ORGANISATION

Réfère aux relations entre les membres de l'organisation et plus spécifiquement à la force du réseau intra-organisationnel.

Par exemple :

- *Mon environnement de travail est caractérisé par un véritable esprit d'équipe.*
- *La coopération et le partage de l'information sont deux mots qui décrivent très bien mon environnement de travail.*

RÉACTION HABITUELLE DE L'ORGANISATION FACE AUX PROBLÈMES

Réfère à la réaction première de l'organisation face à un problème ou à un incident.

Par exemple :

- *Dans mon environnement de travail, on nous encourage à partager nos problèmes plutôt que de les cacher.*
- *Dans mon environnement de travail, lorsque qu'un problème survient, le premier réflexe est de chercher un coupable.*

RÉPONSE HABITUELLE DE L'ORGANISATION FACE AUX PRESSIONS EXTERNES

Réfère à l'attitude générale de l'organisation face aux pressions provenant des clients, gouvernement, standards nationaux et internationaux, etc.

Par exemple :

- *Dans mon environnement de travail, on croit que l'objectif en sécurité de l'information est de faire le minimum qui permette de réussir les audits de conformité.*
- *Dans mon environnement de travail, on prend au sérieux les pratiques de sécurité imposées/recommandées par les organismes externes en nous assurant que des pratiques internes correspondantes soient implantées.*

Caractéristiques du climat

SOUTIEN PROJETÉ PAR LES GESTIONNAIRES

Réfère aux gestes et comportements des gestionnaires par rapport à la sécurité de l'information.

Par exemple :

- *Dans mon environnement de travail, les gestionnaires montrent l'exemple en respectant les pratiques de sécurité de l'information définies.*
- *Dans mon environnement de travail, les gestionnaires montrent peu d'intérêt quant au respect ou non des pratiques de sécurité de l'information.*

COMMUNICATION ORGANISATIONNELLE

Réfère à la capacité de l'organisation à communiquer des messages clairs par rapport à la sécurité de l'information.

Par exemple :

- *Dans mon environnement de travail, le niveau d'effort à investir pour protéger l'information est clairement communiqué.*
- *Dans mon environnement de travail, les attentes en termes de sécurité de l'information sont clairement communiquées.*

SOUTIEN À L'APPRENTISSAGE

Réfère aux moyens mis en place pour soutenir les employés dans l'apprentissage et l'application des pratiques de sécurité de l'information.

Par exemple :

- *Mon organisation offre les outils permettant à chaque employé de bien comprendre les pratiques de sécurité de l'information dont il a la responsabilité.*
- *Dans mon environnement de travail, les employés reçoivent le soutien nécessaire (en termes de formation, assistance, documents de référence, etc.) afin de pouvoir mettre en œuvre les pratiques de sécurité de l'information dont ils ont la responsabilité.*

IMPLICATION DES EMPLOYÉS

Renvoie à l'implication des employés aux étapes du cycle de vie des pratiques de sécurité de l'information.

Par exemple :

- *Dans mon environnement de travail, les employés se sentent impliqués dans l'évolution des pratiques de sécurité de l'information.*
- *Dans mon environnement de travail, les suggestions des employés pour améliorer les pratiques de sécurité de l'information sont prises au sérieux.*

ADÉQUATION AU CONTEXTE ORGANISATIONNEL

Réfère à l'adéquation (le « fit ») entre les pratiques de sécurité de l'information de l'organisation et les caractéristiques du contexte organisationnel.

Par exemple :

- *Les pratiques de sécurité de l'information sont bien alignées sur les pratiques d'affaires de mon organisation.*
- *Les pratiques de sécurité de l'information respectent la culture de mon organisation.*

ADÉQUATION AUX TÂCHES

Réfère à l'adéquation (le « fit ») entre les pratiques de sécurité de l'information de l'organisation et les tâches à réaliser.

Par exemple :

- *Dans mon environnement de travail, les pratiques de sécurité de l'information ont été définies de façon à ne pas nuire au rendement au travail.*
- *Dans mon environnement de travail, on pense qu'il est difficile de respecter les pratiques de sécurité de l'information si on veut satisfaire les exigences de notre travail.*

ENGAGEMENT ORGANISATIONNEL

Renvoie au lien affectif qui unit les employés à l'organisation.

Par exemple :

- *Dans mon environnement de travail, les employés s'investissent pour aider notre organisation à connaître le succès.*
- *Dans mon environnement de travail, les employés tendent à parler très positivement de notre organisation.*

COMMUNICATION DES PROBLÈMES/ERREURS

Réfère à la possibilité de discuter ouvertement dans l'environnement de travail des problèmes/erreurs liés à l'application des pratiques de sécurité de l'information.

Par exemple :

- *Dans mon environnement de travail, les problèmes liés à l'application des pratiques de sécurité peuvent être ouvertement discutés.*
- *Dans mon environnement de travail, les erreurs qui sont commises dans l'application des pratiques de sécurité sont discutées en groupe afin qu'elles soient une source d'apprentissage collectif.*

RÉCOMPENSES/SANCTIONS

Réfère à la façon dont le respect des pratiques de sécurité de l'information est encouragé ou le manque de respect de celles-ci est réprimandé.

Par exemple :

- *Dans mon environnement de travail, le système de récompense encourage le respect des pratiques de sécurité de l'information.*
- *Dans mon environnement de travail, le respect des pratiques de sécurité de l'information est un élément sérieusement considéré lors de l'évaluation de la performance des employés.*

FACON DONT LE MONITORAGE DU RESPECT DES PRATIQUES DE SÉCURITÉ SE FAIT

Réfère à la façon (confiance et/ou contrôle) privilégiée par l'organisation pour s'assurer du respect des pratiques de sécurité.

Par exemple :

- *Dans mon environnement de travail, on tend à prendre pour acquis que les employés respectent les pratiques de sécurité de l'information parce qu'on leur fait confiance.*
- *Dans mon environnement de travail, le respect de chacune des pratiques de sécurité de l'information est minutieusement contrôlé.*

IMPORTANCE RÉELLE ACCORDÉE À LA SÉCURITÉ DE L'INFORMATION

Réfère à l'importance qui est accordée au quotidien à la sécurité de l'information.

Par exemple :

- *Dans mon environnement de travail, la sécurité de l'information est une priorité.*
- *Dans mon environnement de travail, la sécurité de l'information est un élément rarement considéré.*

Annexe 6 : Cartes des exercices de priorisation de l'étape C

Croyances

CROYANCE #1

Croyance partagée dans l'organisation qui indique qui a la responsabilité d'assurer la sécurité de l'information.

Plus on croit dans l'organisation que la sécurité de l'information est du ressort exclusif du département informatique, moins les employés se sentiront responsables de mettre en œuvre des pratiques sécuritaires. À l'opposé, si on croit que tout le monde dans l'organisation a une responsabilité quant à la sécurité de l'information, plus les employés se sentiront responsables de mettre en œuvre des pratiques sécuritaires.

CROYANCE #2

Croyance partagée dans l'organisation qui indique la nature des défis rencontrés en sécurité de l'information.

Plus on croit dans l'organisation que la sécurité de l'information est avant tout un défi d'ordre technique, moins les employés sentiront la nécessité de mettre en œuvre des pratiques sécuritaires parce qu'ils se fieront aux solutions technologiques. À l'opposé, plus on a la conviction dans l'organisation qu'il y a des composantes humaine, technique et managériale à la sécurité de l'information, plus élevées sont les chances que tout le monde jouera le rôle qu'il a à jouer afin de protéger l'information.

CROYANCE #3

Croyance partagée dans l'organisation qui réfère à l'importance générale que l'on accorde à la sécurité de l'information.

Plus on croit dans l'organisation que la sécurité de l'information est importante, plus les employés sentiront la nécessité de mettre en œuvre des pratiques sécuritaires. À l'opposé, si on croit dans l'organisation que la sécurité de l'information n'est pas importante, moins élevées sont les chances que les employés mettent en œuvre des pratiques sécuritaires.

CROYANCE #4

Croyance partagée dans l'organisation qui réfère à la capacité de l'organisation à se défendre contre les menaces à la sécurité de l'information.

Plus on croit dans l'organisation qu'il est fondamentalement impossible d'assurer vraiment la protection de l'information, moins les employés seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si on est convaincus dans l'organisation qu'il est possible de prendre des actions préventives et de protéger l'information, plus élevées sont les chances que les employés mettront en œuvre des pratiques sécuritaires.

CROYANCE #5

Croyance partagée dans l'organisation quant à la responsabilité morale que l'entreprise a de protéger les informations.

Plus on croit que l'organisation a la responsabilité morale de protéger l'information, plus les employés seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si on ne croit pas que l'organisation a cette responsabilité morale, moins élevées sont les chances que les employés mettent en œuvre des pratiques sécuritaires.

CROYANCE #6

Croyance partagée dans l'organisation quant à la nature générale de l'être humain et, plus spécifiquement, en ce qui a trait aux raisons qui motivent ses actions.

Plus on croit dans l'organisation que les gens agissent dans le meilleur intérêt de l'organisation et qu'on peut leur faire confiance, plus ils seront responsables et motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si on croit que les gens sont fondamentalement mauvais et qu'on les déresponsabilise en les contrôlant comme des enfants, moins les gens mettront en œuvre des pratiques sécuritaires.

CROYANCE #7

Croyance partagée dans l'organisation quant au rôle que joue l'être humain dans la sécurité de l'information.

Plus on croit dans l'organisation que les gens représentent le maillon faible en sécurité de l'information, moins les employés seront motivés à mettre en œuvre des pratiques sécuritaires parce que l'entreprise mettra en place des outils menant à une déresponsabilisation. À l'opposé, si on croit que les gens sont des maillons importants de la sécurité de l'information, plus élevées sont les chances que l'organisation leur fera confiance, les responsabilisera et que les employés agiront dans le meilleur intérêt de l'organisation en mettant en œuvre des pratiques sécuritaires.

Valeurs

VALEUR #1

Valeur partagée dans l'organisation quant aux bases sur lesquelles les décisions doivent être prises au sein de l'organisation.

Plus l'organisation privilégie les bases quantitatives pour asseoir ses décisions (analyses quantitatives, métriques, benchmarking, etc.), plus élevées sont les chances qu'elle évaluera les aspects liés à la sécurité de l'information d'une manière globale et complète menant à la mise en place d'outils stimulant davantage les employés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si on tend à privilégier des décisions basées sur l'intuition et les émotions (« gut feelings »), plus élevées sont les chances que l'on négligera de conduire une évaluation rigoureuse des aspects liés à la sécurité de l'information, menant ainsi à l'absence d'outils favorisant la mise en œuvre de pratiques sécuritaires.

VALEUR #2

Valeur partagée dans l'organisation qui reflète les habitudes de planification de l'organisation.
Plus l'organisation a l'habitude de planifier à long terme, plus élevées sont les chances qu'elle le fera aussi en sécurité de l'information, ce qui l'amènera à faire les investissements requis afin de favoriser la mise en œuvre de pratiques sécuritaires. À l'opposé, si le focus de l'organisation est surtout à court terme, moins élevées sont les chances que la sécurité de l'information fera l'objet des investissements nécessaires à la mise en œuvre de pratiques sécuritaires.

VALEUR #3

Valeur partagée dans l'organisation quant à la place de l'éthique dans l'organisation.
Plus l'organisation adopte une position éthique dans la conduite générale de ses affaires, plus élevées sont les chances qu'elle le fera aussi pour protéger les informations, menant ainsi à la mise en œuvre de pratiques sécuritaires. À l'opposé, si l'éthique n'est pas une valeur importante dans l'organisation, cela affectera négativement la mise en œuvre de pratiques peu sécuritaires.

VALEUR #4

Valeur partagée dans l'organisation quant au respect des règles et des politiques définies au sein de l'organisation.
Plus il existe dans l'organisation une prédisposition à respecter les règles et les politiques définies, plus élevées sont les chances que les employés respecteront aussi les pratiques de sécurité de l'information définies. À l'opposé, s'il existe un mépris généralisé envers les règles et les politiques organisationnelles, les chances sont que la même chose se produira pour la mise en œuvre des pratiques de sécurité de l'information définies par l'entreprise.

VALEUR #5

Valeur partagée dans l'organisation qui réfère à l'importance qu'a le développement des connaissances et des habiletés des employés dans l'organisation.
Plus il existe dans l'organisation une valorisation du développement des ressources humaines, plus élevées sont les chances que le même sentiment sera instauré par rapport à la sécurité de l'information et que les employés recevront tout le soutien nécessaire à la mise en œuvre de pratiques sécuritaires. À l'opposé, si le développement n'est pas valorisé, moins les employés mettront en œuvre des pratiques sécuritaires parce qu'ils seront livrés à eux-mêmes, sans soutien, ni formation.

VALEUR #6

Valeur partagée dans l'organisation quant à la façon de réagir au changement organisationnel.
Plus on valorise l'ouverture au changement dans l'organisation, plus il sera facile de changer les pratiques organisationnelles afin que les employés mettent en œuvre des pratiques de plus en plus sécuritaires. À l'opposé, si on tend à résister au changement, les chances sont plus élevées que les changements engendrés par la mise en œuvre de pratiques de plus en plus sécuritaires seront difficiles à accepter.

VALEUR #7

Valeur partagée dans l'organisation quant à la façon dont les gens travaillent ensemble (force du réseau intra-organisationnel).
Plus un réseau fort existe entre les membres de l'organisation, plus élevées sont les chances que les employés s'appuieront, se conseilleront et discuteront les problématiques liées à la sécurité de l'information, le tout favorisant la mise en œuvre de pratiques sécuritaires. À l'opposé, si les employés évoluent dans un environnement « en silo », l'individu sera livré à lui-même, ce qui aura pour effet de nuire à la mise en œuvre de pratiques sécuritaires.

VALEUR #8

Valeur partagée dans l'organisation quant à la réaction première de l'organisation face à un problème ou à un incident.
Plus la réaction instinctive de l'organisation face à un problème ou à un incident est de pointer un coupable, moins les employés seront motivés à partager les problèmes/incidents/difficultés entre eux et plus élevées sont les chances que les employés mettront en œuvre des pratiques non sécuritaires. À l'opposé, si la réaction est plutôt d'encourager les employés à partager leurs problèmes/incidents/difficultés, plus les chances sont élevées que ce sera aussi la même chose dans le cas de la sécurité de l'information, menant ainsi à la mise en œuvre de pratiques plus sécuritaires.

VALEUR #9

Valeur partagée dans l'organisation qui réfère à la réponse habituelle de l'organisation face aux pressions provenant des clients, gouvernement, standards nationaux et internationaux, etc.
Plus l'organisation a tendance à adopter des comportements symboliques face aux obligations externes (clients, gouvernements, standards, etc.), plus élevées sont les chances qu'elle fera la même chose en ce qui a trait à la sécurité de l'information, au total menant à la mise en œuvre de pratiques moins sécuritaires. Au contraire, si l'organisation tend à prendre ces obligations/recommandations comme une occasion d'améliorer ses pratiques internes, les chances sont qu'elle fera la même chose en sécurité de l'information, ce qui mènera à la mise en œuvre de pratiques plus sécuritaires.

VALEUR #10

Valeur partagée dans l'organisation quant à l'imputabilité des employés, soit la responsabilité de chacun face aux conséquences des décisions prises et gestes posés.
Plus on tend au sein de l'organisation à assumer les conséquences des décisions prises et gestes posés, plus les employés se sentiront responsables et seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si on évolue dans un contexte organisationnel où personne n'est jamais responsable de rien, moins élevées sont les chances que les employés mettent en œuvre des pratiques sécuritaires.

Caractéristiques du climat

CARACTÉRISTIQUE DU CLIMAT #1

Cette caractéristique du climat organisationnel réfère aux gestes et comportements des gestionnaires par rapport à la sécurité de l'information.

Plus les gestionnaires ont tendance à montrer un appui à la sécurité de l'information (par leurs gestes, paroles, décisions et appuis concrets (comme des ressources financières), plus les employés comprendront que la sécurité de l'information est importante dans leur environnement de travail et seront motivés à mettre eux aussi en œuvre des pratiques sécuritaires. À l'opposé, si le message reçu des gestionnaires est que la sécurité de l'information a peu d'importance dans leur environnement de travail, plus les chances sont élevées que les pratiques sécuritaires ne seront pas mises en œuvre.

CARACTÉRISTIQUE DU CLIMAT #2

Cette caractéristique du climat organisationnel réfère à la capacité de l'organisation à communiquer des messages clairs par rapport à la sécurité de l'information.

Plus l'organisation arrive à communiquer des messages clairs quant à la sécurité de l'information (objectifs, importance, attentes, etc.), plus les employés seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si les messages sont absents ou confus, plus les chances sont élevées que les pratiques sécuritaires ne seront pas mises en œuvre.

CARACTÉRISTIQUE DU CLIMAT #3

Cette caractéristique du climat organisationnel réfère aux moyens mis en place pour soutenir les employés dans la mise en œuvre des pratiques de sécurité.

Plus l'organisation met en place les outils qui permettent de soutenir la formation et le développement de connaissances en sécurité de l'information, plus les employés seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si les employés ne reçoivent pas le soutien nécessaire, plus les chances sont élevées que les pratiques sécuritaires ne seront pas mises en œuvre.

CARACTÉRISTIQUE DU CLIMAT #4

Cette caractéristique du climat organisationnel renvoie à l'implication des employés aux étapes du cycle de vie des pratiques de sécurité de l'information.

Plus les employés se sentent impliqués dans l'élaboration et l'évolution des pratiques de sécurité, plus les employés seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, si les employés ne se sentent pas impliqués, plus élevées sont les chances que les pratiques sécuritaires ne seront pas mises en œuvre.

CARACTÉRISTIQUE DU CLIMAT #5

Cette caractéristique du climat organisationnel réfère à l'adéquation (le « fit ») entre les pratiques de sécurité de l'information dans l'organisation et les caractéristiques du contexte organisationnel.

Plus les pratiques de sécurité de l'information définies sont en adéquation avec les caractéristiques du contexte organisationnel comme la culture et les pratiques d'affaires, plus les employés seront enclins à mettre en œuvre ces pratiques sécuritaires. À l'opposé, s'il y a un « misfit » entre les pratiques de sécurité de l'information et les caractéristiques du contexte organisationnel, plus élevées sont les chances que les pratiques sécuritaires ne seront pas mises en œuvre.

CARACTÉRISTIQUE DU CLIMAT #6

Cette caractéristique du climat organisationnel réfère à l'adéquation (le « fit ») entre les pratiques de sécurité de l'information dans l'organisation et les tâches à réaliser.

Plus les pratiques de sécurité de l'information définies sont en adéquation avec la tâche (effort minimal, impact marginal sur le rendement, etc.), plus les employés seront enclins à mettre ces pratiques sécuritaires en œuvre. À l'opposé, si les pratiques ajoutent une lourdeur au travail quotidien, plus les chances sont élevées que les pratiques sécuritaires ne seront pas mises en œuvre.

CARACTÉRISTIQUE DU CLIMAT #7

Cette caractéristique du climat organisationnel renvoie au lien affectif qui unit les employés à l'organisation.

Plus les employés ont un sentiment partagé d'attachement à l'organisation, plus ils seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, plus un désengagement général est présent, plus les chances sont élevées que les pratiques sécuritaires ne seront pas mises en œuvre.

CARACTÉRISTIQUE DU CLIMAT #8

Cette caractéristique du climat organisationnel réfère à la possibilité de discuter ouvertement dans l'environnement de travail des problèmes/erreurs liés à la mise en œuvre des pratiques de sécurité de l'information.

Plus l'environnement de travail permet de discuter ouvertement des problèmes/erreurs liés à la mise en œuvre des pratiques de sécurité, plus les employés seront enclins à communiquer les problèmes/erreurs rencontrés, le tout favorisant la mise en œuvre de pratiques sécuritaires. À l'opposé, si l'environnement favorise plutôt de ne pas révéler et même de cacher les problèmes/erreurs, moins élevées sont les chances que les employés mettront en œuvre de pratiques sécuritaires.

CARACTÉRISTIQUE DU CLIMAT #9

Cette caractéristique du climat organisationnel réfère à la façon dont le respect des pratiques de sécurité de l'information est encouragé ou le manque de respect de celles-ci est réprimandé.

Plus l'organisation récompense le respect des pratiques de sécurité de l'information définies, plus les employés seront motivés à mettre en œuvre ces pratiques. Plus l'organisation sanctionne vraiment le non-respect des pratiques de sécurité de l'information, plus les chances sont élevées que les employés mettront en œuvre les pratiques sécuritaires définies.

CARACTÉRISTIQUE DU CLIMAT #10

Cette caractéristique du climat organisationnel réfère à la façon (confiance et/ou contrôle) privilégiée par l'organisation pour s'assurer du respect des pratiques de sécurité.

Plus l'organisation fait confiance aux employés qu'ils feront tout en leur pouvoir pour protéger l'information, plus ils seront engagés dans la protection de l'information et mettront en œuvre des pratiques sécuritaires. À l'opposé, plus l'organisation fait le monitorage continu du respect des pratiques, moins les employés se sentent responsabilisés et auront plutôt tendance à faire fi des pratiques de sécurité.

CARACTÉRISTIQUE DU CLIMAT #11

Cette caractéristique du climat organisationnel réfère à l'importance qui est accordée au quotidien à la sécurité de l'information dans l'environnement de travail.

Dans un environnement de travail donné, plus on accorde de l'importance à la sécurité de l'information, plus les employés seront motivés à mettre en œuvre des pratiques sécuritaires. À l'opposé, moins on accorde d'importance à la sécurité de l'information, moins élevées sont les chances que les employés mettent en œuvre des pratiques sécuritaires.