HEC MONTRÉAL
École affiliée à l'Université de Montréal

Market level consequences of information breach and effectiveness of crisis recoveries

par
Shahin Rasoulian

Thèse présentée en vue de l'obtention du grade de Ph. D. en administration
(option Marketing)

Janvier 2017

HEC MONTRÉAL

École affiliée à l'Université de Montréal

Cette thèse intitulée :

Market level consequences of information breach and effectiveness of crisis recoveries

Présentée par :

Shahin Rasoulian

a été évaluée par un jury composé des personnes suivantes :

Johanne Brunet
HEC Montréal
Présidente-rapporteuse

Renaud Legoux
HEC Montréal
Codirecteur de recherche

Sylvain Sénécal
HEC Montréal
Codirecteur de recherche

Yany Grégoire
HEC Montréal
Membre du jury

Thomas Dotzel
Desautels Faculty of Management, McGill University
Membre du jury

Michael Wiles
W.P. Carey School of Business, Arizona State University
Examinateur externe

Martin Boyer
HEC Montréal
Représentant du directeur de HEC Montréal

Résumé

La fuite d'information – la divulgation non-autorisée d'informations privées provenant de parties prenantes - est une source de préoccupation grandissante pour les gestionnaires à l'ère de l'information. Malgré le taux d'occurrence élevé de cet incident, notre connaissance de ses conséquences et des actions potentielles de récupération est limitée. Cette dissertation comporte deux essais qui visent à comprendre les conséquences au niveau du marché de la fuite d'information pour les entreprises coupables ainsi que l'efficacité des actions de récupération que ces entreprises peuvent offrir en retour.

En employant la méthode des études d'événements, le premier essai étudie l'effet des annonces publiques de fuite d'information sur la valeur actionnariale entreprises coupables. En se basant sur la littérature sur la perception de crises, cet essai propose la nature de l'information divulguée, la cause de la fuite ainsi que les caractéristiques de l'entreprise comme variables principales permettant d'expliquer l'ampleur de rendements anormaux des actions suite à une annonce publique de fuite d'information. En somme, ces rendements anormaux démontrent une réaction négative considérable suite à l'annonce publique d'une fuite d'information, en particulier lorsque les informations divulguées contiennent des données financières (versus des données non financières) et lorsque la fuite est la cause d'un piratage informatique. Aussi, les résultats révèlent que lorsque la fuite est causée par un piratage ou un virus, la rentabilité de l'entreprise peut amortir cet effet tandis que la taille de l'entreprise et son ancienneté peuvent amplifier l'impact négatif de la fuite d'information sur le rendement des actions de l'entreprise. Ces constatations contribuent à la littérature en identifiant la nature de l'information divulguée, la cause de la fuite et les caractéristiques de l'entreprise comme modérateurs clés qui peuvent influer sur l'ampleur du rendement anormal des actions d'une entreprise suite à l'annonce

publique d'une fuite d'information. De plus, cette recherche offre des recommandations managériales concrètes sur la mobilisation des ressources afin de gérer ces incidents de fuites qui peuvent nuire considérablement à la valeur actionnariale de l'entreprise.

Le deuxième essai emploie la méthode d'analyse de risques afin d'examiner l'effet atténuant de trois stratégies de service de récupération de crise suite à la fuite d'information, soit l'offre de compensations, l'amélioration des processus et la présentation d'excuses. En s'appuyant sur la théorie de la justice, cet essai justifie d'une part l'effet atténuant de l'offre de compensations (i.e. des redressements tangibles) ou de l'amélioration des processus (i.e. des processus organisationnels) sur le risque idiosyncratique auquel s'expose l'entreprise coupable dans l'année suivant l'annonce publique d'une fuite d'information. D'autre part, le fait de présenter des excuses augmente ce risque. En plus de contribuer à l'avancement de nos connaissances sur l'efficacité de diverses stratégies de récupération de crise, cette recherche informe les gestionnaires sur les meilleures stratégies à adopter afin de répondre aux parties prenantes dans le but de préserver leur valeur actionnariale suite à une fuite d'information.

Mots-clés: fuite d'information, crise de service, échec de service, valeur actionnariale, interface marketing-finance

Méthodes de recherche: Méthode des études d'événements, Méthode d'analyse de risques

Abstract

Information breach—the potential or malpractice of unauthorized access to private information of stakeholders—is of growing concern to managers in the information age. In spite of information breach's high rate of occurrence, our knowledge of its consequences and recovery actions remains limited. This dissertation comprises two essays that attempt to understand the market level consequences of information breach for responsible firms and the effectiveness of recovery actions that responsible firms can offer in response.

The first essay investigates the reaction of stock value of firms to information breach announcements, using an event study methodology. On the basis of the literature on crisis level perception, this essay proposes that the type of the breached data, the cause of the breach and the firm characteristics are principal variables that can fairly well explain the magnitude of firms' abnormal stock returns as a result of information breach announcements. In brief, the authors find that firms' stock returns show a considerable negative reaction to the announcement of an information breach, either when the breached information contains financial data (versus non-financial data) or when the breach is caused by a hacker attack. Moreover, results reveal that when the breach is caused by a hacker attack, firm profitability can buffer, and firm leverage and firm age can magnify the negative impact of the information breach on firms' stock returns. These findings make a contribution to the literature by identifying the type of the breached information, the cause of the breach and firm characteristics as key moderators that can change the magnitude of firms' abnormal stock return during information breach announcements. Also, these results add insights of managers on mobilizing their resources against those breach incidents that considerably threaten their firms' shareholder value.

The second essay employs risk analysis methodology to explore the mitigating role of three strategies of service crisis recovery—compensation, process improvement and apology—in response to information breach incidents. Building on justice theory, this essay suggests and finds empirical support that offering compensations (i.e., tangible redresses) or process improvements (i.e., improvements of organizational processes) lowers firm-idiosyncratic risk within the year after the announcements, while offering apology-based recoveries increases this risk. This research advances our understanding of the market level effectiveness of recovery actions and guides managers in how to respond to stakeholders following an information breach incident and thus to preserve their shareholder value.

Keywords: service crisis, service failure, firm risk, shareholder value, marketing-finance interface, information breach, service crisis recovery

Research methods: Event study, Risk analysis

Table of contents

Résumé vi
Abstract v
Table of contents vii
List of tables and figures viii
Acknowledgments x
Introduction 1
Chapter 1 Is information breach always costly for the firm? An event study analysis 6
Abstract 6
1.1 Introduction 7
1.2 Literature review 10
1.3 Conceptual framework 12
1.4 Research design 22
1.5 Results 27
1.6 Discussion 36
References 41
Chapter 2 Service crisis recovery and firm performance: Insights from information breach announcements 47
Abstract 47
2.1 Introduction 48
2.2 Research background 51
2.3 Hypotheses: Linking service crisis recoveries to firm-idiosyncratic risk 58
2.4 Research design 65
2.5 Results 72
2.6 Discussion 84
References 91
Conclusion 101
Appendices i

List of tables and figures

Chapter 1

Figure 1 A conceptual model for the market value loss of information breach announcement 9

Figure 2 Aggregated CAARs over time 25

Table 1 Definitions and frequencies of information breach causes 13

Table 2 Descriptive statistics and correlation matrix (N = 209) 28

Table 3 CAARs for information breach announcement 29

Table 4 Results of the impact of information breach on abnormal stock return (Market Model approach) 32

Table 5 Results of the robustness check of the impact of information breach on abnormal stock return 35

Chapter 2

Table 1 The differences between service crisis and other related constructs 52

Table 2 Industry composition of dataset 68

Table 3 Descriptive statistics and correlation matrix (N = 212) 74

Table 4 Results of the impact of service crisis recoveries on firm-idiosyncratic risk (Fama-French four-factor approach) 77

Table 5 Results of the impact of service crisis recoveries on firm-idiosyncratic risk (Market Model approach) 79

Table 6 Durational persistence of the impact of service crisis recoveries on firm-idiosyncratic risk (Fama-French four-factor approach) in different time horizons 81

To freedom of speech, justice and wisdom

Acknowledgments

I would like to express my sincere gratitude and appreciation to my doctoral supervisors and committee members: Prof. Legoux, Prof. Sénécal, Prof. Grégoire, Prof. Dotzel, and Prof. Wiles, my family members, and my friends and colleagues for all of their help, advice, support, patience and friendship.

Introduction

Widespread access to personal information of stakeholders helps firms to benefit their stakeholders in various ways. For instance, it allows firms to personalize their offerings, prices, communications and services with customers' expectations and needs (Martin & Murphy, 2016) and to maximize the effectiveness of their strategies regarding recruitment, training and retention of employees (Mukherjee, Bhattacharyya, & Bera, 2014).

However, the advent of the information age and firms' unbounded options for collecting and using the personal information of stakeholders have also led to serious concerns about the use of information in relation to privacy, accuracy, property and accessibility. Among these, there is evidence that challenges to information privacy are the most controversial and critical (Bélanger & Crossler, 2011; Smith, Dinev, & Xu, 2011).

While information privacy concerns and information breach incidents are in the headlines today, the concept of information privacy existed long before developments in information and communication technologies; nevertheless, these advances increased its importance and changed its occurrence, impacts and management and, in consequence, provoked new practical and theoretical movements.

As a result of continued worries about information privacy, a number of governmental and non-governmental organizations started developing regulations and procedures to educate individuals about information privacy and to protect them from information breaches. These efforts officially began with global principles of "fair information practices" that were articulated by the U.S. Department of Health, Education and Welfare in 1972 and expanded by the Organization for Economic Cooperation and Development (OECD) in 1980. Later, these principles formed the foundation of governmental regulations regarding information practices in

different countries, such as the guidelines of the Federal Trade Commission in the U.S. and the guidelines of the Personal Information Protection and Electronic Documents Act in Canada (Chan & Greenaway, 2005; Culnan & Bies, 2003). In general, these guidelines provide a set of instructions to businesses that range from procedures of collecting and securing the sensitive information of stakeholders to steps that should be taken following information breach incidents. In addition, non-governmental organizations, such as Privacy Rights Clearinghouse, became active in educating individuals about their privacy rights.

Furthermore, the importance of information privacy generated a fruitful area for research. Over the past four decades, numerous scholars in different disciplines, including information system, marketing, law, management and psychology, have contributed to the conceptualization of information privacy and identified a wide variety of topics and research streams relevant to this concept.

These research studies established two broad schools of thought on privacy: value-based and cognate-based. The value-based, or normative, approach views privacy as a human right or a moral right (e.g., Culnan and Williams 2009). This approach claims that the concept of privacy and its relevant sub-concepts and actions should be developed on the basis of the ethical, legal and societal values of various cultures (Smith et al., 2011). The cognate-based approach pictures privacy as one's absolute desire to have the ability to control information about oneself—regardless of the moral values surrounding one (e.g., Malhotra, Kim, and Agarwal 2004). In this approach the essence of individuals' desire to have autonomy over their personal information underlies the subsequent policies and discussions (Smith et al., 2011).

Adopting these approaches, researchers extended our knowledge on the origins and typologies of information privacy concerns, the role of culture in information privacy perception,

attitudes of individuals toward information privacy and its antecedents and consequences, the role of information technology in privacy protection, and practices and legislations to protect individuals' information privacy (Bélanger & Crossler, 2011; Smith et al., 2011).

Although several scholars have contributed significantly to shaping different aspects of information privacy, recent literature reviews in this domain (e.g., Bélanger and Crossler 2011; Smith, Dinev, and Xu 2011) have brought to light the existence of burning questions regarding this concept at the organizational level: What are the organizational level outcomes of breach of stakeholders' personal information? What consequential decisions should organizations make following information breach incidents? Answers to these questions are of high value for both managers and policy-makers. For managers, prior behavioral studies, which were conducted on the basis of perceptual measures, failed to map a clear reaction from stakeholders or apparent outcomes for firms as a result of the actual event of information breach. In addition, governmental guideline acts that must be taken by firms after the event mainly serve legal purposes and do not encompass actions to restore firms' reputation in the business community. For policy-makers, awareness of tangible and intangible outcomes of information breaches for firms can lead to more effective regulations that consider all the barriers and motivations of firms regarding fair information practices.

The present dissertation aims to disentangle these provocative debates by relating the outcomes of an information breach and its possible recovery actions to changes in the stock returns of the firms involved. In other words, this dissertation addresses the above questions by employing the perspective of firms' investors. Investors' perspective is a reliable assessment criterion, since it reflects the long-term impacts of a firm's events and strategies on its tangible and intangible resources and its subsequent performance (Rust, Ambler, Carpenter, Kumar, &

Srivastava, 2004; Srinivasan & Hanssens, 2009). Moreover, this evaluation criterion utilizes archival data to examine the relevant hypotheses in a way that leads not only to more rigorous findings and insights, compared to perceptual measures, but also differentiates this dissertation from the majority of prior studies in the field of information breach.

To investigate the outcomes of information breach incidents for organizations, we adopt the event study methodology. This methodology detects the shocks in stock returns of corporations as a result of a sudden event that is announced publicly. In general, the mechanism of event study is that, by using econometric models, it predicts future stock returns of a typical corporation, regardless of the target event announcement. Thereafter, it compares the predicted returns with actual returns of the corporation after the event announcement and considers their subtraction as the abnormal returns that are associated with the event.

The role of recovery actions following information breach incidents is examined through the methodology of firm risk analysis in this dissertation. This methodology illustrates the impact of firms' actions and strategies on the volatility of their stock returns. This volatility is measured by the variance of differences between actual returns of a corporation and that of the market average.

This dissertation, which is presented in two chapters, benefits investors and offers useful implications to managers—in addition to narrowing the existing knowledge gaps in the literature. The first chapter reveals the conditions under which an information breach event can devalue firm performance seriously and result in considerable loss for firms and their shareholders. The second chapter, offers practical directions on effective recovery actions that can attenuate the damage of information breach and protect shareholders' wealth to some extent.

References

Bélanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, *35*(4), 1017–1042.

Chan, Y. E., & Greenaway, K. E. (2005). Theoretical explanations for firms' information privacy behaviors. *Journal of the Association for Information Systems*, *6*(6), 7.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of social issues*, *59*(2), 323-342.

Culnan, M. J., & Williams, C. C. (2009). How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches. *MIS Quarterly*, *33*(4), 673-687.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research*, *15*(4), 336-355.

Martin, K. D., & Murphy, P. E. (2016). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 1-21.

Mukherjee, A. N., Bhattacharyya, S., & Bera, R. (2014). Role of Information Technology in Human Resource Management of SME: A Study on the Use of Applicant Tracking System. *IBMRD's Journal of Management & Research*, *3*(1), 1-22.

Rust, R. T., Ambler, T., Carpenter, G. S., Kumar, V., & Srivastava, R. K. (2004). Measuring marketing productivity: Current knowledge and future directions. *Journal of marketing*, *68*(4), 76-89.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, *35*(4), 989-1016.

Srinivasan, S., & Hanssens, D. M. (2009). Marketing and Firm Value: Metrics, Methods, Findings, and Future Directions. *Journal of Marketing Research*, *46*(3), 293-312.

Chapter 1

Is information breach always costly for the firm?

An event study analysis

Abstract

Using an event study methodology, the authors further investigate the stock market reaction to information breach announcements. Employing crisis perception literature, the present article reveals that a firm suffers from a negative abnormal stock return either when the breached information contains financial data or when it is caused by a hacker attack. Moreover, authors find that firm characteristics do not play any moderating role when the breached information contains financial data. However, when the breach is caused by a hacker attack, firm profitability can buffer and firm leverage and firm age can magnify the negative impact of information breach on firms' stock returns.

Keywords: event study, information breach, crisis level perception, marketing-finance interface

1.1 Introduction

In spite of years of research addressing the connection between an information breach announcement and the stock value of responsible firms, the findings to date remain inconclusive. The information privacy of a firm's stakeholders, such as employees or customers, is breached when it is accessed without authorization (Culnan & Williams, 2009). An examination of prior researches reveals that the announcement of information breach can result in a negative stock return (Acquisti, Friedman, & Telang, 2006; Campbell, Gordon, Loeb, & Zhou, 2003a; Cavusoglu, Mishra, & Raghunathan, 2004; Malhotra & Malhotra, 2010). However, our knowledge remains limited of what attributes of the event can change the magnitude of the stock return and what characteristics of the firm can preserve or harm the firm during this event.

From 2006 to 2015, the number of firms affected by information breaches increased from 643 to over 1500 annually (« Statistics | DataLossDB », 2016). Through a survey, it has been found that 85% of responding companies had experienced some sort of privacy breach during the previous year; 63% had reported multiple breaches (Bélanger & Crossler, 2011). While, a large body of research has urged the importance of information protection for stakeholder satisfaction (Culnan & Armstrong, 1999; Rifon, LaRose, & Choi, 2005; Sheehan & Hoy, 2000), little is known about the costs of information breach for the firm and its shareholders. Awareness of various damages of information breaches, especially reductions in stock value of firms that expresses their uncertain future performance (S. Srinivasan & Hanssens, 2009), helps managers decide efficiently on how to invest against information breaches.

This study seeks to narrow this knowledge gap by arguing that a firms' stock value reaction to the event of information breach depends on how serious the event is perceived by the firm's investors. Crisis level literature provides a grounded suggestion to predict this perception (Billings, Milburn, & Schaalman, 1980; Burnett, 1999). We estimate abnormal stock returns

using Market Model and we verify them using Fama-French four-factor and Market Model with GARCH (1, 1) estimation approaches.

More specifically, information privacy is one of the most basic expectations of all stakeholders (Ball, 2001; Carroll, 1991) and a key component of service quality (Lewis & Mitchell, 1990; Yang & Fang, 2004). The violation of this expectation would represent a "service quality" failure (Malhotra & Malhotra, 2011), and, when a large number of individuals are involved, could degenerate into an organizational service crisis, as it falls under close media or legal investigation and can damage the image and the reputation of the firm (Keown-McMullan, 1997; Romanosky & Acquisti, 2009; Romanosky, Telang, & Acquisti, 2011). These damages threaten firm survival and profitability (Pearson & Mitroff, 1993).

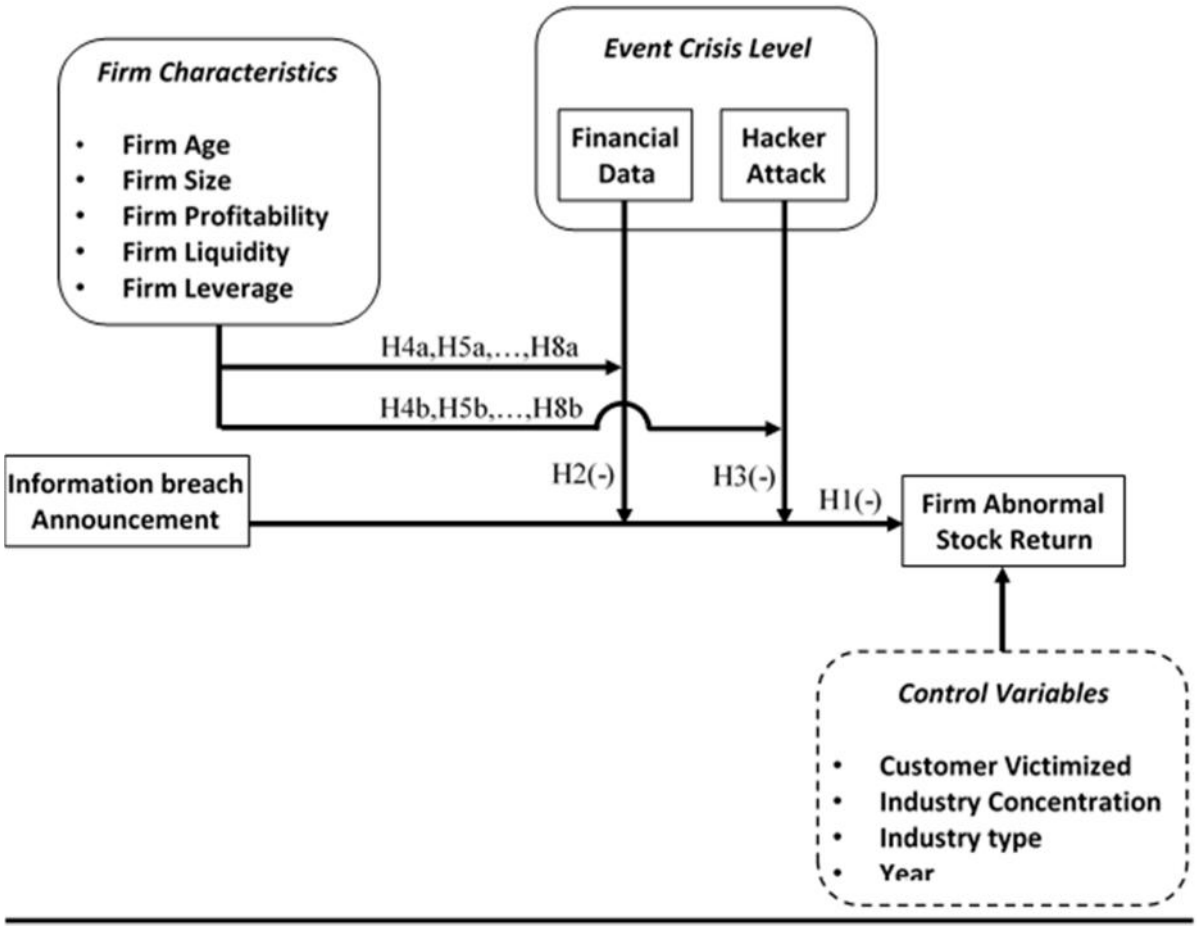
The crisis level literature claims that organizational crises range from low level to high level depending on seriousness of crises. Four dimensions are proposed to identify the crisis level of a negative event from the perspective of stakeholders. These dimensions are *value of loss*, *probability of loss*, *time pressure* and *degree of control* (Billings et al., 1980; Burnett, 1999). The more intense the event is in terms of these dimensions, the closer the event is perceived to a high level crisis for the firm. When an event is close to a high level crisis, the future survival of the firm is more threatened, because the firm falls under severe disruption of operations, financial stains and loss of reputation (Fink, 1986; Keown-McMullan, 1997). These in turn devalue the future cash flow prospects of the firm (Srivastava, Fahey, & Christensen, 2001; Thornhill & Amit, 2003), which is reflected in its stock value (Malkiel & Fama, 1970).

In the context of information breach, we argue that two dimensions of *value of loss* and *time pressure* are intensified when the breached information of stakeholders contains financial

data versus non-financial data. Also, three dimensions of *probability of loss*, *degree of control* and *time pressure* are aggravated when the information are breached by a hacker attack.

In addition to investigating the impact of financial data breach and hacker attack—as indicators of high level crises—on firm abnormal stock returns, we explore the extent to which firm characteristics, including firm size, firm age and firm financial resources—as main elements of resource-based potential of a firm (Grant, 1991)—can buffer a firm against the announcement of high level crises of information breaches. Figure 1 presents an overview of our conceptual framework.

Figure 1 A conceptual Model for the market value loss of information breach announcement



From a theoretical aspect, our study transposes crisis level literature to marketing-finance interface and examines how crisis level literature can explain the reaction of stock market to negative news. Also, we extend the literature on information breach (e.g., Cavusoglu, Mishra, and Raghunathan 2004; Rifon, LaRose, and Choi 2005) by exploring the role of attributes of the event (type of the breached information and cause of the breach) and firm characteristics in the magnitude of financial consequences of this event. Managerially, we grant managers a deeper insight on the reaction of investors to information breach announcements so that managers can mobilize their resources effectively against only serious breaches to protect their shareholder value.

The remainder of this article is organized as follows: after reviewing the literature on the impact of information breach on firm abnormal stock return, we develop the linkage between crisis level of an event and abnormal stock return, and we offer our hypotheses accordingly. Next, we explain our data collection and measures. Finally, we present results and discuss implications and limitations of our research.

1.2 Literature review

Our literature review on the market level consequences of information breach suggests that a large body of prior studies has focused primarily on information technology (IT) *security* breach—which is a specific category of information breach. IT security breach is defined as a malicious attempt to interfere with a company's information system, such as a hacker attack (Cavusoglu et al., 2004). Therefore, they have overlooked cases of information breaches that are not caused by IT security breaches, such as cases of losing equipment that contains sensitive information of stakeholders.

For instance, Campbell et al. (2003) reported negative abnormal returns for the announcement of unauthorized access to private information of customers or firms, as a result of

IT security breaches. Similarly, Cavusoglu, Mishra, and Raghunathan (2004) found negative abnormal stock returns for IT security breaches, especially when they happen to internet-specific companies (i.e., firms whose selling channels are only online). Malhotra and Malhotra (2010) examined the moderating role of firm size, type of the breached information (financial vs. personal), and number of breached records on firms' stock returns, after IT security breaches that affect only customers.

To the best of our knowledge, to date, the only research that has explored the market level consequence of information breach with respect to most of its possible causes is the study of Acquisti, Friedman, and Telang (2006). Indeed, in addition to hacker attack, they considered lost equipment, theft equipment, insider intentional attack, bad security practices and software flaw as different causes of information breaches. However, they failed to determine significantly in what conditions the magnitude of information breach is higher. Martin, Borah, and Palmatier's (2016) article that explores the moderating role of firms' privacy policies and number of affected customers in the linkage between information breach and stock value, did not limit their observations to specific causes of information breaches. However, they did not consider differentiation between various causes of information breaches and did not take into account the attributes of the event and the role of firm characteristic in their study.

Overall, the economic consequences of information breach announcement for firms remain a question. The dominant conclusion of prior studies is that the announcement of information breaches is always associated with negative abnormal returns. However, these studies have been limited in terms of the number of observations and the range of causes and attributes of events. Surprisingly, the role of firm characteristics which is salient in protecting the firm against crises (Newbert, 2008; Thornhill & Amit, 2003), has not been recognized as much

as it deserves. Thus, there is a need for a research that investigates the effect of information breach announcements on the abnormal stock returns and that involves simultaneously the role of event cause, event attributes and firm characteristics. Such a study offers a solider understanding on the cost of information breach for firms. Our study seeks to address this matter.

1.3 Conceptual framework

The impact of information breach announcement on abnormal stock return

Information breach Based on the article of Culnan and Williams (2009), we define information breach as "an event signaling the potential or malpractice of unauthorized access to personal information of a group of stakeholders." The victimized stakeholders might be customers or employees of a firm. These failures might occur inside the firm or inside an external contactor of the firm. Our definition is broad enough to cover the majority of news announcements about the information breach.

In Table 1, we provide a taxonomy of different causes of information breaches that have happened in our dataset in addition to their frequencies. The extant literature does not provide any well-established typology for the causes of information breaches (Smith, Dinev, & Xu, 2011). We build our taxonomy on the basis of suggestions of Acquisti, Friedman, and Telang (2006), Romanosky, Hoffman, and Acquisti (2014) and Whitman (2004).

Table 1 Definitions and frequencies of information breach causes

Breach causes	Definition	Frequency N	Frequency (%)
1. Hacker attack	Electronic entry by an outside party, malware and spyware (Mookerjee, Mookerjee, Bensoussan, & Yue, 2011).	39	18.7
2. Theft equipment	Illegal confiscation of equipment, such as laptop or computer, or data sources, such as smartphone, portable memory device, CD, hard drive, and data tape by external thieves, inside or outside the firm (Whitman, 2004).	40	19.1
3. Improper disposal	Failing to dispose paper documents securely, such as discarding without shredding them (Culnan & Williams, 2009)	12	5.7
4. Misplaced data source	Misplaced data sources such as smartphone, portable memory device, CD, hard drive, and data tape, inside or outside the firm (Sarkar, 2010).	20	9.6
5. Accidental disclosure	Posting information publicly on a website, or sending to the wrong party via email, fax or mail, due to accidental mistake of human resource (Sarkar, 2010) or technical error of equipment, such as fax, computer, and website (Whitman, 2004).	34	16.3
6. Insider attack	Intentional breach of information by someone with legitimate access such as an employee or a contractor (Sarkar, 2010; Schultz, 2002).	64	30.6

The impact of information breach announcement The announcement of information breach corresponds with the concept of an organizational crisis. An organizational crisis is defined as a low probability, high impact event that threatens the viability of the organization and is characterized by ambiguity of cause, effect and means of resolution, as well as by a belief that decisions must be made swiftly (Pearson & Clair, 1998). Organizational crises usually fall under close media or legal investigation and can damage the image and the reputation of the firm (Keown-McMullan, 1997). These features fit well with what happens to an information breach event. Consequently, we view the announcement of information breach as an organizational crisis.

Organizational crises can threaten firm survival and profitability (Pearson & Mitroff, 1993). These threats stem from the damages that a failure causes to an organization's tangible and intangible assets. These damages include economic costs of compensating victims and repairing technical defects (Shrivastava, Mitroff, Miller, & Miglani, 1988), loss of reputation and disruption of operations (Coombs & Sherry, 2002).

In the context of information breach, depending on the attributes of the event, these damages for responsible firms include reputational loss, financial costs, and operational interruptions that can occur due to several reasons such as law enforcement investigations, sending notification to victimized stakeholders, settling legal penalties and fees, offering redresses to victimized stakeholders, developing the information protection standards of the firm (e.g., updating firewalls, training employees and improving organizational procedures), and repairing damages (e.g., physical damage to properties or digital damage to information systems) (Hansman & Hunt, 2005; Romanosky & Acquisti, 2009; Romanosky et al., 2011; Sarkar, 2010).

Furthermore, the extant literature provides evidence that reputational, financial and operational risks are associated with negative stock returns (Gillet, Hübner, & Plunus, 2010; Murphy, Shrieves, & Tibbs, 2009). In fact, the presence of these risks weakens firm resources and capabilities, which, in turn, devalue the competitive advantages of the firm, and, finally, depress future cash flow of the firm (Peteraf, 1993; Srivastava et al., 2001; Thornhill & Amit, 2003).

Thus, the announcement of information breaches erodes expected future cash flows of responsible firms. Since firms' stock returns are reflected by news about their future cash flows (Malkiel & Fama, 1970), we expect negative abnormal stock returns as a result of information breach announcements. Formally:

H1: The announcement of information breach is negatively associated with the firm abnormal stock return.

The impact of information breach crisis level on abnormal stock return

Organizational crises are not equal in terms of magnitude. An organizational crisis starts with a triggering incident. Depending on its severity and damage, it might escalate from a low level crisis to a high level crisis. In the high level crisis, severe disruption of operations, financial strain, inability of managers to cope with the failure, and threat of survival of the firm happens (Billings et al., 1980; Fink, 1986; Keown-McMullan, 1997).

According to the above argument, we suggest that the magnitude of abnormal stock return, as a result of an information breach event, depends on the level of the crisis in which the firm is involved. Indeed, when the attributes of an event of information breach indicate the presence of a high level crisis for the firm, more damages to operational, reputational, and financial resources of the firm is expected. As a result, the future cash flow of the firm is more devalued from the perspective of investors and this market uncertainty is projected in a greater negative abnormal return. However, in low level crises, damages are not so considerable that be able to devalue the cash flow of the firm remarkably.

Billings, Milburn, and Schaalman (1980) offered three dimensions to evaluate the level of a crisis that a firm is involved in as a result of a negative event: *value of loss*, *probability of loss*, and *time pressure*. Thereafter, Burnett (1999) added the fourth dimension to this list which is *degree of control*. A firm's status shifts on the spectrum of crisis level from low to high depending on the intensity of the event in terms of these dimensions. It is noteworthy to mention that high intensity in only one dimension cannot escalate a negative incident to a high level crisis for the firm (Burnett, 1999).

With respect to the crisis level literature, *Value of loss* is referred to the importance of the loss. The more important the loss for the firm, the more the reputation of the firm declines and the more resources of the firm should be spent to resolve the issue. *Probability of loss* is defined as the extent to which the loss and its subsequent damages is likely. When the occurrence of loss and following damages is more probable, the firm should spend more resources to manage the issue. *Time pressure* is the perceived available time for the firm to offer a satisfactory solution for the issue. When the time pressure is high, the priority of managers and employees is to resolve the issue in a short amount of time, which is accompanied with high disruptions in routine operations. *Degree of control* is the amount of control of the firm over the environment to resolve the issue. When a firm has a high control to manage the issue, the probability of further losses decreases, so the firm is under less threat.

Adopting these dimensions to the context of information breach, we argue that the severity of the event in terms of two dimensions of *value of loss* and *time pressure* is identifiable by the type of the breached information and in terms of three dimensions of *time pressure*, *probability of loss* and *degree of control* is distinguishable by the cause of the information breach. Type of the breached information and cause of the information breach are two attributes that are mentioned in all announcements of information breaches and are two indicators of strength of the case from a legal perspective (Romanosky, Hoffman, & Acquisti, 2014; Romanosky et al., 2011).

Type of the breached information The breached information of stakeholders might contain financial data, including credit card, debit card and bank account information, or non-financial data, including name, social security number, driver's license number, date of birth, address, e-mail address, medical information, username and password of subscription accounts

and phone number. These information could be used in several fraudulent ways, such as incurring charges on accounts, applying for utilities (e.g., internet and electricity), applying for credit cards, mortgages and loans, tax return and unemployment return, which can cause financial and psychological harms to victims (Romanosky & Acquisti, 2009; Romanosky et al., 2011). Also, the breach of these information might cause reputational harms to victims, such as the breach of medical information (Kierkegaard, 2012).

Romanosky, Hoffman, and Acquisti (2014) argue that, among all, the breach of financial data is the most threatening loss against responsible firms, because in this case victimized individuals can easily pursue lawsuit against the firm by alleging financial harm, while they do not need to prove it at the beginning. Whereas, evaluating and alleging other harms is not so straightforward for victimized stakeholders. Romanosky, Hoffman, and Acquisti (2014) report that the odds of a firm being sued are 6 times greater when the breached information includes financial data. Hence, the breach of financial data of stakeholders intensifies the dimension of value of loss against the firm, since this incident increases the risk of lawsuit which is accompanied with loss of reputation and cost of settling legal and compensational responsibilities.

Moreover, due to the fact that the risk of harm is high when the breached information contain financial data, responsible firms are legally subject to criminal investigations and are obliged to send notification letters to victimized individuals, which causes a significant amount of time expenditure and operational distraction (Romanosky & Acquisti, 2009; Romanosky et al., 2011; Schwartz & Janger, 2007). Also, although firms are not legally obliged, they usually freeze the accounts or credit cards of victimized individuals on behalf of them because victimized individuals underestimate the seriousness of the event and refuse to freeze their own

accounts (Romanosky et al., 2011). Hence, in cases of financial data breaches, firms are obliged to administrate a great deal of activities in a timely manner which intensifies the dimension of time pressure against firms.

Consequently, the breach of financial data versus non-financial data aggravates two dimensions of crisis level against the firm. Accordingly, we argue that when the breached information contains financial data, the event is closer to a high crisis, and it should be projected in a considerable negative abnormal return. So, we hypothesize that:

H2: The magnitude of negative abnormal return for information breach is higher when breached information contains financial data than non-financial data.

Cause of the information breach An event of the information breach has one of the several causes that are mentioned in Table 1. We argue that, according to crisis level perception framework, among all causes of information breaches, hacker attack is the closest event to a high level crisis. Here, hacker attack is defined as an electronic entry to information system of a firm by a malicious outside party, malware or spyware with financial motivation (Mookerjee et al., 2011). In the case of a hacker attack, first, the probability of abusing the information (probability of loss) is the highest because the main purpose of the breach is to have unauthorized access to sensitive information with financial motivations, such as abusing the information directly or selling it to other criminals (Mookerjee et al., 2011). Second, the degree of firms' control to solve the issue is low because hackers are rarely identifiable (Hansman & Hunt, 2005; Spitzner, 2003), so it is highly unlikely that the firm be able to retrieve the breached information. Third, it is evidenced that hacker attacks can result in a severe business interruption due to causing hardware and software failures in firms' information systems as the principal infrastructure of business operations (Cerullo & Cerullo, 2004). In consequence, hacker attacks impel a serious

time pressure to firms to restore the integrity of their information system and to regain their business continuity.

All in one, the announcement of hacker attack intensifies three dimensions of crisis level; while, other causes of the information breach might aggravate only one or two dimensions of the crisis level against the firm. Hence, hacker attack is a signal of high level crisis and other causes of breaches are signals of low level crises against the firm.

Therefore, we hypothesize that:

H3: The magnitude of negative abnormal return for information breach is higher when the event is caused by hacker attack than other causes.

The impact of firm characteristics on abnormal stock return

Firm characteristics have a key role in our study due to the fact that by weakening or fastening the resource-based strength of the firm, they make the firm more or less vulnerable to crises (Esteve-Pérez & Mañez-Castillejo, 2008; Grant, 1991; Newbert, 2008; Thornhill & Amit, 2003). In fact, firms with stronger characteristics are less vulnerable to crises because they possess enough resources to tolerate threats and costs of crises. So, their future cash flow prospects have less uncertainties. The importance of firm size—as one of the key firm characteristics—has been investigated in previous studies (e.g., Cavusoglu, Mishra, and Raghunathan 2004; Acquisti, Friedman, and Telang 2006). In the present study, we explore the roles of a wider range of firm characteristics in the impact of information breaches on abnormal stock returns.

Since in our theoretical discussion we expect to find a considerable negative reaction only to high level crises (financial data breaches or hacker attacks), it makes sense that we hypothesize the role of firm characteristics only for high level crises.

Firm age Older firms are prone to inertia—stemming from both internal factors, such as homogeneity of member's perception, and external factors, such as inter-organizational agreements—that force them to continue their past practices and that does not let them update their knowledge and infrastructures to the changing competitive environment (Aldrich & Auster, 1986; R. Srinivasan, Sridhar, Narayanan, & Sihi, 2013). As a consequence, older firms are more vulnerable to crises, since crises demonstrate firms' obsolete infrastructures and make the stock market uncertain about the ability of older firms to modernize their systems and procedures in a timely and an economical manner, especially in the case of an information breach that signals the weakness of information systems and information protection policies of a firm which are among modern infrastructures. Accordingly, we hypothesize that:

H4a: The magnitude of negative abnormal return for financial data breach is higher for older firms than younger firms.

H4b: The magnitude of negative abnormal return for hacker attack is higher for older firms than younger firms.

Firm size Murphy, Shrieves, and Tibbs 2009 emphasize on two reasons—economy of scale and reputation—for the importance of firm size in buffering against firm losses. From an economy of scale perspective, if organizational crises impose fixed costs on the firm, then percentage losses will be smaller for larger firms. Also, larger firms have more resources and employees to allocate for resolving the issue. With a reputation perspective, larger firms with better brand names may more easily counter the reputational damage of a crisis, hence reducing the loss impact. Therefore, we hypothesize that:

H5a: The magnitude of negative abnormal return for financial data breach is lower for larger firms than smaller firms.

H5b: The magnitude of negative abnormal return for hacker attack is lower for larger firms than smaller firms.

Firm financial resources Financial resources are among important tangible assets of the firm that significantly influence the competitive advantage of the firm (Newbert, 2008) and can create a buffer against random shocks (Cooper, Gimeno-Gascon, & Woo, 1994). Access to financial resources guarantees the extent to which the firm can meets its short-term and long-term financial obligations to overcome the crisis (Wiklund, Baker, & Shepherd, 2010). Since during crises the firm might go under financial strain to compensate victims and fulfill legal liabilities, possessing a solid financial capital can buffer the pressure of crises. A great deal of financial ratios are offered as indicators of firms' financial capital (Beaver, 1966), among which we pick out the most recommended ones: profitability, liquidity, and leverage (Altman, 1968; Wiklund et al., 2010).

Profitability is the ability of a firm to generate revenues in excess of expenses. It is a key indicator of the ability of firm to repay its debts and acts as an internal buffer against crisis because it reflects a reliable financial process that is not weakened noticeably as a result of a crisis (Beaver, McNichols, & Rhie, 2005; Wiklund et al., 2010). So, we hypothesize that:

H6a: The magnitude of negative abnormal return for financial data breach is lower for firms with higher profitability than firms with lower profitability.

H6b: The magnitude of negative abnormal return for hacker attack is lower for firms with higher profitability than firms with lower profitability.

Liquidity—or the availability of internal funds—is the ability of a firm to meet its short-term financial obligations (Wiklund et al., 2010). Low liquidity can indicate that the firm is

suffered from lack of cash to fulfill its short term needs, which would devalue a firm's future cash flow when the firm is confronted with a crisis. Subsequently, we hypothesize that:

H7a: The magnitude of negative abnormal return for financial data breach is lower for firms with higher liquidity than firms with lower liquidity.

H7b: The magnitude of negative abnormal return for hacker attack is lower for firms with higher liquidity than firms with lower liquidity.

Leverage—which represents the long-term debts and liabilities—refers to the extent to which non-equity capital is used in a firm and to the long-term ability of the firm to pay for these capitals. High leverage is associated with firm financial vulnerability and risk of default. Higher levels of debt project claims on future cash flows and suggest a reduced ability for the firm to generate new, reasonably priced debt (Opler & Titman, 1994; Wiklund et al., 2010). Since a crisis might impose new long-term liabilities to the firm, the combination of new and current liabilities can degrade the future financial health of the firm. Thus, we hypothesize that:

H8a: The magnitude of negative abnormal return for financial data breach is higher for firms with higher leverage than firms with lower leverage.

H8b: The magnitude of negative abnormal return for hacker attack is higher for firms with higher leverage than firms with lower leverage.

1.4 Research design

Data and sample

We constructed our dataset using records and announcements from several sources (i.e., Privacy Rights Clearinghouse, Factiva and web search engines, and Standard & Poor's COMPUSTAT database). We started by collecting the announcements of information breach

events from the Privacy Rights Clearinghouse[1] database. The initial sample consists of 340 observations, involving publicly traded firms, from 2005 to 2013. Next, we checked these announcements through the Factiva database and web search engines to verify the precise announcement dates and to obtain the details of events from news websites and governmental databases. Following standard practice, we dropped cases with confounding announcements within one week before and after the event to make sure that the announcements about each particular case was not affected by other announcements (McWilliams & Siegel, 1997). We considered the following type of news as confounding announcements: earning announcements, mergers and acquisitions, and large profit announcement. Next, because this study aims to control for the impact of type of victimized stakeholders (employees versus customers), we removed cases in which both groups were affected. After following these steps, we were left with 209 cases.

Finally, we coded each event according to the type of breached information (financial vs. non-financial) and cause of the breach (hacker attack vs. others), and we computed Firm-level accounting data using Standard & Poor's COMPUSTAT database.

Abnormal Stock Return Measurement

Measuring abnormal stock return is based on the assumption that the equity markets are efficient, in that, public information is incorporated into market price within a short amount of time. To measure the abnormal stock returns, we adopt the well-advised approach the Market Model (Binder, 1998; MacKinlay, 1997). In this approach, the abnormal return of each stock on

---

"Privacy Rights Clearinghouse" (accessed January 10, 2014), [available at https://www.privacyrights.org/data-breach].

each day is computed by subtracting its expected rate of return from its actual rate of return. The expected rate of return of each stock on each day is estimated by regressing its returns against returns of a market index over an estimation period prior to the event day. Equation (1) computes the parameters of expected rate of return of stock i on day t:

$$R_{it} = \alpha_i + \beta_i R_{mt} + \varepsilon_{it} \quad (1)$$

where, R_{it} is the rate of return of stock i on day t, R_{mt} is the rate of return on the CRSP value weighted index, β_i is sensitivity of firm i to market changes, α_i is the intercept, and ε_{it} is the error term.

For each event, we estimate Equation 1 using OLS regression over 120 trading day period which terminates 10 days prior to the announcement so as not to overlap the Market Model estimation for the event period.

Using Equation 2, we estimate abnormal returns of stock i on day t.

$$AR_{it} = R_{it} - (a_i + b_i R_{mt}) \quad (2)$$

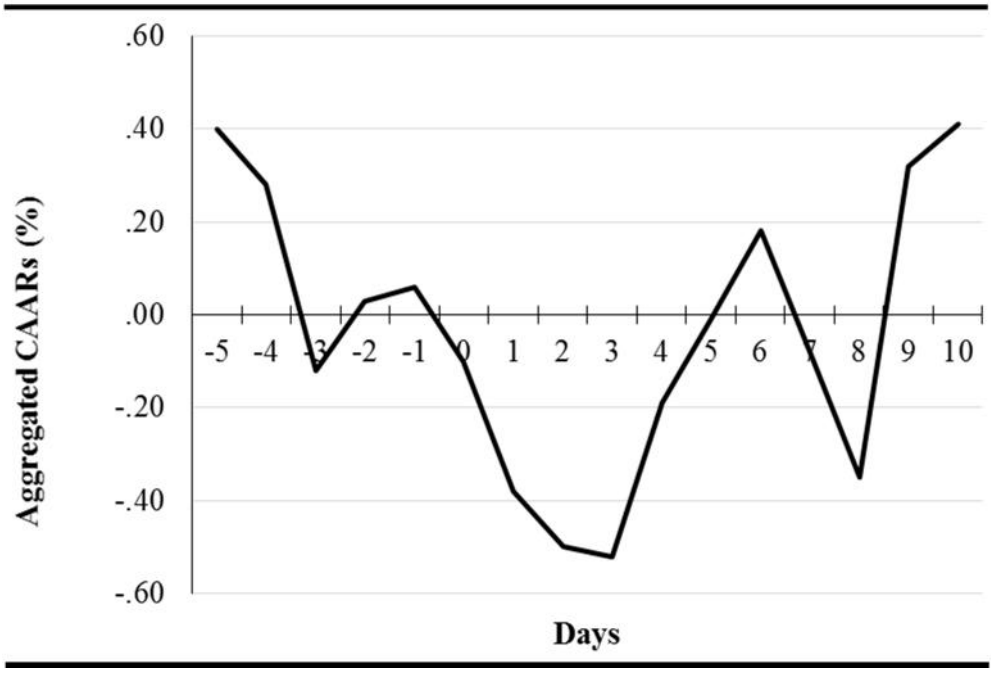
where a_i and b_i are the OLS estimates of α_i and β_i obtained from Equation 1.

To investigate our hypotheses, cumulative average abnormal return (CAAR) for each stock should be computed for an appropriate event window interval. Typically, the event window should be chosen around the event date to project the changes in the stock returns as a result of the event announcement. In terms of length, it should be optimized to allow the complete reaction of the market to the target event and to exclude reactions to previous or following irrelative events.

Figure 2 shows the plot of the aggregated cumulative average abnormal return from 5 days before to 10 days after the event. This graph illustrates in what time period the majority of reaction of stock market takes place to the target event. According to this graph, the negative

trend starts form day 0 to day 3, with no leakage before day 0. Although, there are negative noises on days 7 and 8, we cannot confidently associate them to our event of interest because of the time gap. In sum, the window [0, 3] covers the majority of negative reaction of stock market to the announcement of information breach.

Figure 2 Aggregated CAARs over time



In order to further verify the appropriateness of our event window, we examined the CAAR for several possible windows around the event date. Results show that the window [0, 3] is significant with the highest amount of cumulative average abnormal return (see Table 3).

Moderator and control variables

To test the moderating effects of firm characteristics, we measured firm age as the logarithm of the number of months that have elapsed since the stock's inclusion in CRSP (McAlister, Srinivasan, and Kim 2007). Firm size was measured as the logarithm of total assets value (Kalaignanam, Shankar, and Varadarajan 2007). We measured profitability as return on

total assets. Liquidity was measured as cash and short term investment to total assets, and leverage was computed as the ratio of long-term debt to total assets (Beaver 1966).

In addition, we controlled for important industry and event level covariates in our analysis to calibrate the extent to which the information breach announcement explains the abnormal stock return of firms. The following control variables were used:

Customers victimized Using a dummy variable, we controlled for the type of victimized stakeholders (employees versus customers) to explore if this variable changes abnormal stock return.

Third party responsible We coded whether the event has happened inside an external contractor or inside the main firm. The mutual responsibility of the external contractor might lighten the responsibility of the main firm.

Industry concentration We computed industry concentration by Herfindahl-Hirschman Index (HHI). HHI is measured as the sum of the squared market share of the individual firms in the industry based on three-digit SIC code. Market shares are calculated by sales data. HHI, industry concentration ratio, controls for industry's competitive intensity. Firms in less competitive environment are less vulnerable to crises because they engage in less competition and less innovation (Gaskill, Van Auken, & Manning, 1993).

Industry type Two-digit NAICS codes were used to control the industry-level changes. Natural financial performance varies in different industry sectors (Campbell, Lettau, Malkiel, & Xu, 2001). We used a fixed effect to operationalize this variable.

Year A fixed effect for the year when the event has happened was also considered. This market level variable calibrates for yearly microeconomic fluctuations (McGahan & Porter, 1997).

1.5 Results

Descriptive statistics

Table 2 shows descriptive statistics of our variables and Pearson's correlations between each pair of variables used in our research.

This table reports that pairwise correlations, except that between customers victimized and financial data, are lower than .333, which suggests that multicollinearity is not an issue in our regression analyses. The correlation between customers victimized and financial data is .448 which indicates a moderate relationship between these two variables. Due to the fact that customers victimized is an important control variable and its correlation with financial data is less than .5, we keep it in our analyses. As a further verification for the absence of multicollinearity among our variables, we computed Variance Inflation Factors (VIF) for all variables in our model. All VIFs are less than 1.35 illustrating no issue of multicollinearity (O'brien, 2007).

Table 2 Descriptive statistics and correlation matrix (N = 209)

Variables	M	SD	1	2	3	4	5	6	7	8	9	10
1. Abnormal return	-.009	.052										
2. Financial data	.190	.393	–.107									
3. Hacker attack	.079	.271	–.116	.212***								
4. Firm age	5.265	.953	.105	.005	.018							
5. Firm size	9.912	2.445	.098	.059	–.116	.085						
6. Firm profitability	.041	.086	.207**	–.197**	–.159*	.160*	–.073					
7. Firm liquidity	.108	.119	.052	–.208**	.123	–.211**	–.173*	.193**				
8. Firm leverage	.191	.195	.008	.096	–.022	–.041	–.141*	.111	–.107			
9. Customer victimized	.671	.471	–.047	.448***	.144*	–.005	.216**	–.146*	–.145*	.003		
10. Third party responsible	.219	.415	.023	–.161*	–.249***	–.030	–.002	.209**	.123	–.053	–.193 **	
11. Ind. concentration	1757.870	1600.890	–.031	–.095	.063	.082	–.333***	–.006	.024	–.058	–.107	.081

*p<.05.
**p<.01.
***p<.001.

Event study analysis

Results of the impact of information breach announcement on the stock return for several windows are shown in Table 3. CAARs of windows [–1, 0] and [–2, 0] are not significant showing that there is no leakage before the date of announcements in our study. As we discussed earlier, the window [0, 3] significantly covers the majority of market reactions to the event announcement.

Table 3 CAARs for information breach announcement

Event windows	Sample size (n)	CAAR (%)	Number with negative abnormal returns	Patell z	Generalized sign Z
(–2,0)	209	–.08	113(96)	–.367	–.687
(–1,0)	209	–.10	117(92)	–.625	–1.241
(0,0)	209	–.13	111(98)	–.777	–.410
(–1,+1)	209	–.36	125(84)	–1.421	–2.348**
(0,+1)	209	–.39	125(84)	–1.665*	–2.348**
(0,+2)	209	–.64	120(89)	–2.332**	–1.656*
(0,+3)	209	–.91	121(88)	–2.115*	–1.794*
(–1,+2)	209	–.61	123(86)	–2.073*	–2.071*
(–1,+3)	209	–.88	119(90)	–1.940*	–1.518

*p<.05.
**p<.01.
***p<.001.

Cowan generalized sign test (Generalized Sign Z)—a nonparametric test (Cowan, 1992)—and Pattell Test (Patell Z)—a parametric test (Patell, 1976)—confirm that the number of events with negative returns is significantly higher than the number of events with positive returns during the event window [0, 3]. Our examination shows that in three days period, starting from the date of announcement, the stocks of firms on average lose .91 % as a result of information breach announcement. Therefore, H1 is supported.

Cross-sectional regression results

Table 4 presents the main results. Model 1 assesses the effect of main variables on abnormal stock return without considering control variables. Model 2, the main model, estimates the direct effect of all variables on abnormal stock return. Model 3 examines the interactions among firm characteristics and high level crises (financial data breach and hacker attack). All models are estimated through fixed effect linear regressions.

An initial outlier diagnostic test, through minimum covariance determinant (MCD) method, illustrates the existence of 18 outliers in our dataset, 4 of which are bad leverage points (i.e., observations with outlying x and y that do not follow the pattern of the majority of observations) (Rousseeuw & Driessen, 1999). MCD method detects outliers by finding a subsample of observations whose covariance matrix has the lowest determinant. Then, using Equation 3, the robust distance of each observation from this subsample is computed.

$$RD(x_i) = [(x_i - T(X))^T C(X)^{-1}(x_i - T(X))]^{1/2} \quad (3)$$

where T(X) is the average of observations of the subsample and C(X) is their covariance matrix.

Those observations whose robust distance is higher than the cutoff value are detected as outliers. Cutoff value is equal to the square root of the 97.5% quantile of the chi-square distribution with degrees of freedom equal to the number of variables.

Outliers and leverage points are sources of multicollinearity that can cause a bias in the estimate of coefficients (Andrews & Pregibon, 1978; Kamruzzaman & Imon, 2002). To address this issue, we applied the M-estimator robust regression method to examine our hypotheses, which bounds the influence of outliers. This method is not robust to bad leverage data points but is useful when vertical outliers and good leverage points are a concern (Rousseeuw & Leroy, 1987), which is the case in the current research. This method also can reduce the concern about heteroscedasticity (Maronna, Martin, & Yohai, 2006).

In contrast to ordinary least square estimation (OLS) that minimizes the sum of squares of the residuals, M-estimator method minimizes the influence of outliers on the parameter estimation (Equation 4).

(4) $$\min \sum_i \rho(r_i(x))$$

where r is the residual vector ($r = y - Ax$) and ρ is the Huber loss function defined by:

(5) $$\begin{cases} \frac{t^2}{2} & \\ & \frac{c^2}{2} \end{cases}$$

where c is an estimate of σ (Huber, 1973).

Table 4 Results of the impact of information breach on abnormal stock return (Market Model approach)

Variables		Model 1 (Without controls)		Model 2 (Main model)		Model 3 (Interactions)	
		B	***SE***	***B***	***SE***	***B***	***SE***
Main Factors							
Financial data (FD)	H2	–.010***	.003	–.011***	.004	–.037	.028
Hacker attack (HA)	H3	–.010**	.004	–.011**	.005	.027	.038
Firm age		–.002	.002	–.002	.002	–.004*	.002
Firm size		.002**	.001	.002**	.001	.002	.001
Firm profitability		.002	.025	–.023	.028	.020	.038
Firm liquidity		.028*	.014	.040**	.016	.013	.019
Firm leverage		.006	.008	–.002	.010	.006	.015
Interactions							
(FD)× Firm age	H4a					.005*	.004
(FD)× Firm size	H5a					.000	.002
(FD)× Firm profitability	H6a					–.073	.053
(FD)× Firm liquidity	H7a					.004	.040
(FD)× Firm leverage	H8a					.007	.019
(HA)×Firm age	H4b					–.012**	.005
(HA)×Firm size	H5b					.005**	.002
(HA)×Firm profitability	H6b					.251***	.058
(HA)×Firm liquidity	H7b					.002	.038
(HA)×Firm leverage	H8b					–.104**	.030
Controls							
Customer victimized				–.001	.004	–.006	.004
Third party responsible				–.001	.004	–.004	.004
Industry concentration				–.001*	.001	–.001**	.004
Industry type dummies					Yes		Yes
Year dummies					Yes		Yes

*p<.1.
**p<.05.
***p<.01.

The results of estimation of Model 2 show that financial data breach (β = –.011, SE = .004, chi-square = 7.16, p < .001) and hacker attack (β = –.011, SE = .005, chi-square = 4.54, p < .05) explain a significant amount of variance in investors' reaction following information breach announcements. These results support H2 and H3.

To fully capture the extent to which financial data breaches and hacker attacks constitute the .91% wealth loss that was found in H1, we computed cumulative average abnormal returns for each of these two groups of events separately. We found that hacker attack is associated significantly with 2.22% value loss (CAAR = –2.22%, Z_{gsign} = –2.984, $p < .01$), while other causes of information breach on average do not lead to a significant loss (CAAR = –.61%, Z_{gsign}= 0.506, not significant). Also, financial data breaches result in 1.52% value loss (CAAR = –1.52%, Z_{gsign}= –2.225, $p < .05$), yet non-financial data breaches do not show a significant loss (CAAR = –.43%, Z_{gsign}= –0.348, not significant).

The estimation of Model 3 reveals that interactions between financial data breaches and firm characteristics are not significant except the barely one between Financial data and firm age which does not persist during robustness check. So, we have lack of support for H4a, H5a, H6a, H7a and H8a. It demonstrates that firm characteristics cannot secure the firm against the negative reaction of investors to financial data breaches.

However, interactions between hacker attack and firm age (β = –.012, SE = .005, chi-square = 5.81, $p < .05$), firm profitability (β = .251, SE = .058, chi-square = 17.22, $p < .001$), and firm leverage (β = –.104, SE = .030, chi–square = 6.31, $p < .05$) are significant. Hence, H4b, H6b and H8b are supported.

In Table 4, the interaction between firm size and hacker attack seems significant; however, this significance does not persist throughout the validation check. Therefore, results do not show significant supports for H5b and H7B. Therefore, firm size and liquidity cannot protect firms against hacker attacks.

Considering control variables, we do not observe any significant effect of customers victimized versus employees victimized, indicating that the type of victimized group of an

information breach event does not change the reaction of investors. Also, industry class did not display any significant effect showing the generalizability of our findings across different industry sectors. Furthermore, the effect of a third party responsibility is not significant, meaning that main firm is the primary responsible of the event of information breach from investors' viewpoint.

Robustness tests

To assure the robustness of our results, we analyzed the sensitivity of our results to alternative approaches of abnormal stock return computation. To this end, first, we repeated Market Model approach with equal weighted index, and we obtained consistent results with value weighted index. Second, we computed stock returns using Fama-French four-factor approach and Market Model with GARCH (1, 1) estimation approach. Fama-French four-factor approach estimates the expected returns and abnormal returns of each stock on each day by regressing the stock returns against the daily returns on CRSP, difference between daily returns of small and big stocks, difference between daily returns of high and low book-to-market stocks, and difference between daily returns of high and low performing stocks (Carhart, 1997). In turn, Market Model with GARCH (1, 1) estimation approach, estimates the parameters of expected returns by assuming that the residuals of the regressions of Market Model approach can be conditionally heteroskedastic and then corrects this issue by modeling the heteroscedasticity as a variance (Corhay & Rad, 1997; Engle, 2001).

Table 5 shows the results of these two approaches. Results of Model 2 remained unchanged, so the impact of financial data breach and hacker attack is persistent. As mentioned earlier, the significance of the interaction between financial data and firm age, and between

hacker attack and firm size are not found in Fama-French four-factor approach. So, supports for these interaction are not strong enough.

Table 5 Results of the robustness check of the impact of information breach on abnormal stock return

Variables		Fama–French Four–Factor Approach				Market Model Approach (GARCH Estimation)			
		Model 2 (Main model)		Model 3 (Interactions)		Model 2 (Main model)		Model 3 (Interactions)	
		B	*SE*	*B*	*SE*	*B*	*SE*	*B*	*SE*
Main Factors									
Financial data (FD)	H2	−.016***	.004	−.055*	.032	−.012***	.004	−.050*	.029
Hacker attack (HA)	H3	−.010*	.005	.116**	.046	−.010**	.005	−.015	.038
Firm age		−.001	.002	−.002	.003	−.002	.002	−.004	.003
Firm size		.002*	.001	.001	.001	.002**	.001	.001	.001
Firm profitability		.007	.028	.008	.041	−.026	.027	.004	.040
Firm liquidity		.025	.017	.037*	.021	.025*	.015	.015	.019
Firm leverage		.002	.011	−.011	.016	.007	.010	.003	.016
Interactions									
(FD)×Firm age	H4a			.002	.004			.006	.004
(FD)×Firm size	H5a			.002	.002			.001	.002
(FD)×Firm profitability	H6a			.006	.060			−.063	.056
(FD)×Firm liquidity	H7a			.012	.039			−.054	.035
(FD)×Firm leverage	H8a			.021	.020			.030	.020
(HA)×Firm age	H4b			−.012*	.006			−.005**	.005
(HA)×Firm size	H5b			−.002	.003			.004*	.002
(HA)×Firm profitability	H6b			.308***	.069			.203***	.053
(HA)×Firm liquidity	H7b			−.148***	.044			.023	.036
(HA)×Firm leverage	H8b			−.109**	.036			−.068**	.028
Controls									
Customer victimized		.005	.005	.007	.005	−.004	.004	.004	.004
Third party responsible		−.013***	.005	−.011**	.005	.002	.004	.001	.004
Industry concentration		.001	.001	.001	.001	−.001**	.000	−.001**	.001
Industry type dummies			Yes		Yes		Yes		Yes
Year dummies			Yes		Yes		Yes		Yes

*p<.1.
**p<.05.
***p<.01.

Severity of financial data breach versus hacker attack

Our results suggest that a firm suffers considerably from a negative abnormal stock return in both cases of a financial data breach and a hacker attack. To statistically compare the severity of these two cases, we employ the "standard method" suggested by Schenker and Gentleman (2001). This method builds an interval around the difference between the point estimates of two dimensions. To do so, it adds and subtracts the z-value multiplied by the square root of the sum of the squared standard error of each point estimate ($((Q_1 - Q_2) \pm 1.96(SE_1^2 + SE_2^2)^{1/2})$. If the interval does not include zero, the difference between the two dimensions is statistically significant. In our case, the 95% confidence interval for the difference between these two dimensions includes zero ($CI_{95\%} = -.006$ to .006). This result indicates that there is no significant difference between the predictive validity of financial data breach versus hacker attack, so these two incidents have statistically equal severity.

1.6 Discussion

Damages of information breaches and solutions to resist them are among ongoing challenges of managers. Prior studies not only have limited their concentration on only information security breaches, but also have neglected the role of event attributes and firm characteristics in the reaction of market to information breaches. Our theoretical framework explains substantial amount of variance in the market level cost of information breach announcements for firms.

Building on crisis level literature, our results highlight that the reaction of stock market to information breach announcements has a considerable magnitude when events signal high level crises against the firm, such as when the breached information contains financial data or when the breach has been caused by a hacker attack; otherwise, the event is not considerably costly for the firm.

Regarding firm characteristics, our findings suggest that in cases of financial data breaches firm characteristics do not play any significant positive or negative role. Nevertheless, the results depict that when the information is breached by a hacker attack, profitable firms are less vulnerable and leveraged firms and older firms are more vulnerable to the event and endure more negative abnormal returns. Conceptually, we link this dissimilar role of firm characteristics to different degrees of uncertainties that are associated with two cases of financial data breaches versus hacker attacks. In fact, we argue that the event of hacker attack carries more uncertainties compared with the event of financial data breaches because of the time, the nature, and the amount of loss that it can cause to responsible firms. Here, the logic is that hackers are not identifiable and predictable, and, in consequence, the time and nature of their decision to hazard the information are not completely predictable by the market. As a result, firms with stronger potentials are expected to take measures to attenuate the upcoming damages. However, in cases of financial data breaches, the very sensitive information of stakeholders is already under a high risk and it makes a reasonable level of certainty regarding the reaction of victimized stakeholders to the event. That is, the scale of damage is more predictable and resource potentials of the firm cannot attenuate it confidently. Therefore, the market shows its complete reaction to the event regardless the characteristics of responsible firms.

Implications for theory

Our research, first, contributes to the literature on crisis level perception by adopting four dimensions of crisis level and examining the extent to which they can explain the consequences of negative events for firms. We show that four dimensions of *value of loss*, *probability of loss*, *time pressure* and *degree of control* are able to evaluate the seriousness of crises.

Second, we add more insights on financial consequences of information breach announcements (e.g., Acquisti, Friedman, and Telang 2006; Campbell et al. (2003); Cavusoglu, Mishra, and Raghunathan 2004; Malhotra and Malhotra 2010). More specifically, our study differentiates between high level and low level crises and illustrates that those events of information breaches that signal high levels of crises are mainly costly for firms. To put it more bluntly, we add to this literature two variables of financial data breach and hacker attack as two key moderators that can signal high level crises against the firm and can depreciate the stock value of the firm as a consequence. In other words, we found that those events of information breach that do not signal high level of crises are not costly for the firm. Moreover, we elaborate the key role of firm characteristics during information breaches. We showed that for investors the firm profitability is a valuable resource to protect the future financial performance of the firm during crises, while high firm leverage and high firm age are indicators of vulnerability that deteriorate the value of firms during crises.

Third, this research provides contribution for the literature on marketing-financial interface. We draw crisis level perception literature to marketing-financial interface, which offers a valuable perspective to study shareholders' wealth loss as a result of negative events. We presented strong evidence that the reaction of investors to negative events is influenced by the level of crisis that the firm is involved in, and the level of crisis can be evaluated by four dimensions of crisis level perception.

Implications for managers

For managers, this study provides insights that the event of information breach is not always accompanied with wealth loss for shareholders. Information breach is costly for shareholders either when it happens by a hacker attack or when it breaches the financial data of

stakeholders. Also, these finding are stable for the breach of both employees' and customers' information and for all industry sectors. These findings guide managers in how they should strategically invest against information breaches. Particularly, we suggest that firms should invest against occurrence of high level crises information breaches, such as the breach of financial data and hacker attack. It means that firms should give priority to development of security of their information systems, in order to prevent the intrusion of hackers. Also, firms that collect financial data of stakeholders should set up rigorous procedures and systems to protect the security of this type of information.

Furthermore, our results suggest that old firms should modernize their knowledge, systems and standards to decrease their vulnerability during crises. In fact, the inertia of keeping traditions in old firms makes investors hesitated about the potential of old firms to survive easily during crises. However, by updating their procedures and systems, old firms can guarantee the stability of their future financial health during crises.

Finally, firms with low profitability and high leverage should take practices of information protection and the event of information breach more serious, since these groups of firms will be damaged more as a results of information breach incidents, from a market level perspective.

Limitations and further research

Our findings and conclusions are subject to some limitations that equally propose some questions for future researches. Firstly, like other event-studies, the generalizability of our study is limited to publicly traded U.S. firms. Also, the method of event-study cannot detail the mechanism that underlies the reaction of investors to the announcement in media. We assume that the literature of crisis level perception in addition to our statistical analyses can explain the

movements in stock value of firms following an information breach announcement. Future behavioral studies can enhance the rigorousness of our conceptual framework, using surveys and interviews with investors

Secondly, one key variable that has not been considered in this study is the number of breached records. This variable is not disclosed in all announcements of information breaches; that is why we did not include it in our analyses. Theoretically, we do not assume that a large number of breached records can signal a high level crisis, because according to the crisis level theory, a large number of breached records can only intensify the dimension of time pressure against the firm, which is not enough to be considered as a signal of high level crisis. But, the existence of this variable could add more statistical and theoretical insights to our study.

Thirdly, future studies would benefit from testing the applicability of crisis level theory in other contexts of crises, such as product-harm crisis or disasters and environment crises (e.g., Dutton 1986) to examine how applicable this perspective is.

References

Acquisti, A., Friedman, A., & Telang, R. (2006). Is There a Cost to Privacy Breaches? An Event Study. *ICIS 2006 Proceedings*. Consulté à l'adresse http://aisel.aisnet.org/icis2006/94

Aldrich, H., & Auster, E. R. (1986). Even dwarfs started small: Liabilities of age and size and their strategic implications. *Research in Organizational Behavior*, *8*(1), 165 186.

Altman, E. I. (1968). Financial ratios, discriminant analysis and the prediction of corporate bankruptcy. *Journal of Finance*, *23*(4), 589 609.

Ball, K. S. (2001). The use of human resource information systems: a survey. *Personnel review*, *30*(6), 677 693.

Beaver, W. H. (1966). Financial ratios as predictors of failure. *Journal of Accounting Research*, *4*(1), 71 111.

Beaver, W. H., McNichols, M. F., & Rhie, J.-W. (2005). Have financial statements become less informative? Evidence from the ability of financial ratios to predict bankruptcy. *Review of Accounting Studies*, *10*(1), 93 122.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, *35*(4), 1017–1042.

Billings, R. S., Milburn, T. W., & Schaalman, M. L. (1980). A model of crisis perception: A theoretical and empirical analysis. *Administrative Science Quarterly*, *25*(2), 300 316.

Binder, J. (1998). The event study methodology since 1969. *Review of Quantitative Finance and Accounting*, *11*(2), 111 137.

Burnett, J. J. (1999). A strategic approach to managing crises. *Public relations review*, *24*(4), 475 488.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003b). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431 448.

Carhart, M. M. (1997). On persistence in mutual fund performance. *Journal of Finance*, *52*(1), 57 82.

Carroll, A. B. (1991). The pyramid of corporate social responsibility: Toward the moral management of organizational stakeholders. *Business horizons*, *34*(4), 39 48.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, *9*(1), 69 104.

Cerullo, V., & Cerullo, M. J. (2004). Business continuity planning: A comprehensive approach. *Information Systems Management*, *21*(3), 70 78.

Cooper, A. C., Gimeno-Gascon, F. J., & Woo, C. Y. (1994). Initial human and financial capital as predictors of new venture performance. *Journal of Business Venturing*, *9*(5), 371 395.

Corhay, A., & Rad, A. T. (1997). Conditional heteroskedasticity adjusted market model and an event study. *The Quarterly Review of Economics and Finance*, *36*(4), 529 538.

Cowan, A. R. (1992). Nonparametric event study tests. *Review of Quantitative Finance and Accounting*, *2*(4), 343 358.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104 115.

Dutton, J. E. (1986). The processing of crisis and non crisis strategic issues. *Journal of Management Studies*, *23*(5), 501 517.

Engle, R. (2001). GARCH 101: The use of ARCH/GARCH models in applied econometrics. *The Journal of Economic Perspectives*, *15*(4), 157 168.

Esteve-Pérez, S., & Mañez-Castillejo, J. A. (2008). The resource-based theory of the firm and firm survival. *Small Business Economics*, *30*(3), 231 249.

Fahy, J., & Smithee, A. (1999). Strategic Marketing and the Resource Based View of the Firm. *Academy of Marketing Science Review*, *1999*(10), 1 20.

Fink, S. (1986). *Crisis management: Planning for the inevitable*. American Management Association.

Gaskill, L. R., Van Auken, H. E., & Manning, R. A. (1993). A factor analytic study of the perceived causes of small business failure. *Journal of Small Business Management*, *31*(4), 18.

Gillet, R., Hübner, G., & Plunus, S. (2010). Operational risk and reputation in the financial industry. *Journal of Banking & Finance*, *34*(1), 224 235.

Grant, R. M. (1991). The resource-based theory of competitive advantage: implications for strategy formulation. *California management review*, *33*(3), 114–135.

Hansman, S., & Hunt, R. (2005). A taxonomy of network and computer attacks. *Computers & Security*, *24*(1), 31–43.

Hovav, A., & D'Arcy, J. (2003). The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms. *Risk Management and Insurance Review*, *6*(2), 97–121.

Keown-McMullan, C. (1997). Crisis: When Does a Molehill Become a Mountain? *Disaster Prevention and Management*, *6*(1), 4–10.

Kierkegaard, P. (2012). Medical data breaches: Notification delayed is notification denied. *Computer Law & Security Review*, *28*(2), 163–183.

Kozlenkova, I. V., Samaha, S. A., & Palmatier, R. W. (2014). Resource-based theory in marketing. *Journal of the Academy of Marketing Science*, *42*(1), 1–21.

Lewis, B. R., & Mitchell, V. W. (1990). Defining and measuring the quality of customer service. *Marketing intelligence & planning*, *8*(6), 11–17.

MacKinlay, A. C. (1997). Event studies in economics and finance. *Journal of economic literature*, *35*(1), 13–39.

Malhotra, A., & Malhotra, C. K. (2010). Evaluating Customer Information Breaches as Service Failures: An Event Study Approach. *Journal of Service Research*, 1–16.

Malkiel, B. G., & Fama, E. F. (1970). Efficient capital markets: A review of theory and empirical work. *The journal of Finance*, *25*(2), 383–417.

Martin, K. D., Borah, A., & Palmatier, R. W. (2016). Data privacy: Effects on customer and firm performance. *Journal of Marketing*.

McGahan, A. M., & Porter, M. E. (1997). How much does industry matter, really? *Strategic Management Journal*, *18*(1), 15–30.

McWilliams, A., & Siegel, D. (1997). Event studies in management research: Theoretical and empirical issues. *Academy of Management Journal*, *40*(3), 626–657.

Mookerjee, V., Mookerjee, R., Bensoussan, A., & Yue, W. T. (2011). When hackers talk: Managing information security under variable attack rates and knowledge dissemination. *Information Systems Research*, *22*(3), 606–623.

Murphy, D. L., Shrieves, R. E., & Tibbs, S. L. (2009). Determinants of the stock price reaction to allegations of corporate misconduct: Earnings, risk, and firm size effects. *Journal of Financial and Quantitative Analysis*, *43*(3), 581 612.

Newbert, S. L. (2008). Value, rareness, competitive advantage, and performance: a conceptual level empirical investigation of the resource based view of the firm. *Strategic Management Journal*, *29*(7), 745 768.

O'brien, R. M. (2007). A Caution Regarding Rules of Thumb for Variance Inflation Factors. *Quality & Quantity*, *41*(5), 673 690.

Opler, T. C., & Titman, S. (1994). Financial distress and corporate performance. *Journal of Finance*, *49*(3), 1015 1040.

Patell, J. M. (1976). Corporate forecasts of earnings per share and stock price behavior: Empirical test. *Journal of Accounting Research*, *14*(2), 246 276.

Pearson, C. M., & Mitroff, I. I. (1993). From crisis prone to crisis prepared: a framework for crisis management. *The Academy of Management Executive*, *7*(1), 48 59.

Peteraf, M. A. (1993). The cornerstones of competitive advantage: A resource-based view. *Strategic Management Journal*, *14*(3), 179 191.

Privacy Rights Clearinghouse. (2016, mai 12). Consulté 12 mai 2016, à l'adresse

Rifon, N. J., LaRose, R., & Choi, S. (2005). Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. *Journal of Consumer Affairs*, *39*(2), 339 362.

Romanosky, S., & Acquisti, A. (2009). Privacy costs and personal data protection: Economic and legal perspectives. *Berkeley Technology Law Journal*, *24*(3), 1061 1101.

Romanosky, S., Hoffman, D., & Acquisti, A. (2014). Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies*, *11*(1), 74 104.

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management*, *30*(2), 256 286.

Sarkar, K. R. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. *information security technical report*, *15*(3), 112 133.

Schenker, N., & Gentleman, J. F. (2001). On Judging the Significance of Differences by Examining the Overlap Between Confidence Intervals. *The American Statistician*, *55*(3), 182 186.

Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security*, *21*(6), 526 531.

Schwartz, P. M., & Janger, E. J. (2007). Notification of data security breaches. *Michigan Law Review*, *105*(5), 913.

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing*, *19*(1), 62 73.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, *35*(4), 989 1016.

Spitzner, L. (2003). The honeynet project: Trapping the hackers. *IEEE Security & Privacy*, *1*(2), 15 23.

Srinivasan, R., Sridhar, S., Narayanan, S., & Sihi, D. (2013). Effects of opening and closing stores on chain retailer performance. *Journal of Retailing*, *89*(2), 126 139.

Srivastava, R. K., Fahey, L., & Christensen, H. K. (2001). The resource-based view and marketing: The role of market-based assets in gaining competitive advantage. *Journal of Management*, *27*(6), 777 802.

Statistics | DataLossDB. (2016, janvier 2). Consulté 25 janvier 2016, à l'adresse http://datalossdb.org/statistics

Thornhill, S., & Amit, R. (2003). Learning about Failure: Bankruptcy, Firm Age, and the Resource-Based View. *Organization Science*, *14*(5), 497 509.

Wernerfelt, B. (1984). A Resource-Based View of the Firm. *Strategic Management Journal*, *5*(2), 171 180.

Whitman, M. E. (2004). In defense of the realm: understanding the threats to information security. *International Journal of Information Management*, *24*(1), 43 57.

Wiklund, J., Baker, T., & Shepherd, D. (2010). The age-effect of financial indicators as buffers against the liability of newness. *Journal of Business Venturing*, *25*(4), 423 437.

Yahoo. (s. d.). Consulté 5 avril 2016, à l'adresse http://ca.yahoo.com

Yang, Z., & Fang, X. (2004). Online service quality dimensions and their relationships with satisfaction: A content analysis of customer reviews of securities brokerage services. *International Journal of Service Industry Management*, *15*(3), 302 326.

Chapter 2

Service crisis recovery and firm performance: Insights from information breach announcements

Abstract

The extant literature has studied the effects of a firm's service recovery efforts on the reactions of customers and employees following an individual service failure or a personal offense. However, the impact of recovery efforts on firm performance after a public and large service failure has received scant attention. To address this gap, the current research develops a framework and finds support for the impact of *service crisis recoveries* on firm performance, as measured by firm-idiosyncratic risk. Using a unique dataset of service crisis recoveries, the authors find that firms that offer compensations (i.e., tangible redresses) or process improvements (i.e., improvements of organizational processes) show more stable performance (less idiosyncratic risk) over the year after the announcement of their recovery plan. Interestingly, firms that offer apology-based recovery plans display more volatile performance (higher idiosyncratic risk), possibly because of a greater liability risk (e.g., lawsuits).

Keywords: service crisis, service failure, firm risk, shareholder value, marketing-finance interface, information breach, service crisis recovery

2.1 Introduction

How should a firm respond to a service crisis that affects a large group of stakeholders (customers or employees), so that its financial performance does not suffer? The literature on service recovery and organizational justice typically focuses on small scale failures and private responses (Blodgett, Hill, & Tax, 1997; Cohen-Charash & Spector, 2001; Maxham III & Netemeyer, 2002; Smith, Bolton, & Wagner, 1999). Little attention has been given to the effectiveness of recovery efforts after a service crisis—that is, a public service failure affecting a large number of individuals. Despite the inevitable occurrence of service crises (Shrivastava, Mitroff, Miller, & Miclani, 1988), we still have limited insights on the impacts of recovery efforts after such crises on shareholder value and financial performance—which are issues of prime importance for managers. In light of these gaps, the current research emphasizes three contributions: 1) defining the particularities of service crises and their recoveries, 2) understanding the effects of these recovery efforts using investors' responses, and 3) adopting firm-idiosyncratic risk to capture firm investors' reactions and firm performance.

As its *first contribution*, this research pays special attention to defining the concept of service crises, compared to other related concepts such as private service failures and product-harm crises. In general, a crisis is a low probability, high impact event that can greatly damage a firm's reputation (Pearson & Clair, 1998). The marketing literature has devoted considerable attention to *product-harm crises*—defined as well-publicized events involving defective or dangerous products (Klein & Dawar, 2004). This literature, surprisingly, has somewhat overlooked crises that derive from service failures that affect a large number of individuals. Although the literature counts hundreds of articles and a few meta-analyses on *private* service failures (e.g., Gelbrich and Roschk 2010a), there are only a few studies on *service crises*. For instance, Gijsenberg et al. (2015) examine the longitudinal effects of service crises on travelers'

perception of service quality, whereas Malhotra and Malhotra (2011) study the depreciatory effects of information breaches on firms' abnormal stock returns.

This research defines a *service crisis* as a service performance that fails to reach the expectations of a large group of stakeholders (employees or customers), and that becomes well-publicized in media. The inability of TJX to protect the private information of 45.7 million customers against hackers (Kawamoto, 2007), and the problems in Amazon's cloud infrastructure that caused serious disruptions for Netflix customers (Darrow, 2015) are examples of such crises. Relatedly, we introduce the concept of *service crisis recovery* and define it as a firm's public attempts to redress and repair inconveniences of stakeholders who are affected by such crises.

The current research selects information breaches—i.e., the potential or malpractice of unauthorized access to personal information of a group of individuals (Culnan & Williams, 2009)—as the service crisis of interest. In this information age, data security is one of the most basic expectations of all stakeholders (Ball, 2001; Carroll, 1991) and a key component of service quality (Lewis & Mitchell, 1990; Yang & Fang, 2004). The violation of this expectation would represent a "service quality" failure that could degenerate into a service crisis, when a large number of individuals are involved (Malhotra & Malhotra, 2011).

As our *second contribution*, we aim to examine the effects of three service crisis recovery efforts—compensation, process improvement and apology—on investors' responses as an indicator of firms' future financial performance. Service crises possess important differences from product-harm crises in terms of recovery strategies (Gijsenberg et al., 2015). Product-harm crises rely mainly on the implementation of a "product recall strategy" ((Dawar & Pillutla, 2000), which is not applicable in a service context because of the intangible and inseparable

nature of services (Gijsenberg, Van Heerde, & Verhoef, 2015; Wilson, Zeithaml, Bitner, & Gremler, 2012). When there is a service crisis, it may be difficult to isolate and repair a given problem, such as a loss in privacy (Rushton & Carson, 1985). Then, because of the inseparability of services and consumption, a service crisis may affect a large group of individuals who are simultaneously using that service. For instance, a power outage immediately affects thousands, even millions, of customers. Because of these characteristics, firms need to rely on different recovery efforts for service crises, and the current research examines the differentiated effects of these recoveries on investors' responses.

We argue that investors could react differently from other stakeholders to service crisis recoveries. Investors are loss averse and pursue long-term returns that are influenced by firms' decisions (Barberis & Huang, 2001; Fama, 1998), whereas customers and employees are mainly concerned about event-specific satisfaction (Saad Andaleeb & Conway, 2006). As a result, investors could favorably respond to compensation and process improvements; these actions respectively improve a firm's relational capital and its operational efficiency in the long term (Johnston & Michel, 2008; Smith et al., 1999). However, investors could unfavorably react to a public apology because this action represents an "admission of a guilt" that could be used in a class-action lawsuit against a firm (Cohen, 1999; Robbennolt, 2003).

As our *third contribution*, we adopt *firm-idiosyncratic risk* as the evaluation criterion to measure investors' responses to different service crisis recoveries (e.g., Dechow 1994; Luo et al. 2014; Luo and Bhattacharya 2009). To the best of our knowledge, the current research is the first to use this metric in a service crisis context. Firm-idiosyncratic risk (or stock return volatility) is a critical indicator of firms' financial stability and performance, which is influenced by firms' actions and resources (Dechow, 1994; Goyal et al., 2003; Srinivasan & Hanssens, 2009). Since

investors evaluate firms' decisions in the long term, this metric is a solid indicator of strategic consequences of firms' decisions (Luo & Bhattacharya, 2009; Rust, Ambler, Carpenter, Kumar, & Srivastava, 2004). We calculated this metric by using the Fama-French four-factor approach in our main analyses and by referring to the Market Model approach as a robustness check.

In the remaining sections, we review the literature on our foundational constructs (i.e., service crisis, information breach and firm-idiosyncratic risk). Then, we present a theoretical framework explaining the impact of service crisis recoveries on firm-idiosyncratic risk. Next, we describe our research, and discuss the implications of our results.

2.2 Research background

Defining service crisis and service crisis recovery

Service crisis A *private* service failure is defined as a performance that falls below the expectations of a given customer (e.g., Smith et al. 1999) or an employee (when this individual is viewed as an internal customer). Our focus goes beyond private and individual-based service failures that have been widely studied in the last 20 years (e.g., Smith et al. 1999; Tax et al. 1998). Building on the crisis literature (Keown-McMullan, 1997; Pearson & Clair, 1998), we use the label *service crisis* to describe our context of interest. As previously noted, this type of crisis happens when a service performance fails to reach the expectation of a large group of stakeholders, and when this crisis is publicized in the media.

We further explain the differences between service crisis and other related concepts by using a "two by two" matrix (see Table 1) inspired by Gijsenberg et al. (2015). The first dimension makes a distinction between the contexts involving defective products or service failures, whereas the second dimension relates to the number of affected individuals (i.e., private versus mass). This matrix provides key definitions, references and a summary for each quadrant.

Table 1 The differences between service crisis and other related constructs

Number of affected individuals	Type of offering: Product	Type of offering: Service
Private (one or a few individuals)	*Private product failure:* A product that fails to match the average quality of similar devices. • Earliest research efforts in this area (Traynor 1964); • Examination of the attributional antecedents leading to different customers' responses (Folkes, 1984, 1988).	*Private Service failure:* A service performance that falls below the expectation of a given individual. • The richest quadrant with hundreds of articles; • The variables belonging to the "cognitions – emotions – behaviors" process are well studied; • See meta-analyses on justice theory (Gelbrich & Roschk, 2010a; Orsingher, Valentini, & de Angelis, 2010) and attribution theory (Van Vaerenbergh, Orsingher, Vermeir, & Larivière, 2014).
Mass (a large group of individuals)	*Product-harm crisis:* A well-publicized event wherein products are found to be defective or dangerous. • A rich quadrant in which the responses to product recalls are well studied (see Laufer [2015] for a special issue); • Product recall is the recovery strategy of choice (e.g., Dawar and Pillutla 2000; Klein and Dawar 2004); • For instance, research has documented customer responses toward product recall (e.g., Cleeren et al. 2008), and the effectiveness of post marketing actions (Cleeren, Van Heerde, & Dekimpe, 2013).	*Service crisis:* When a service performance fails to reach the expectations of a large group of stakeholders, and is intensively publicized in diverse media. • The less studied quadrant (see Gijsenberg et al. [2015] and Malhotra and Malhotra [2011] for exceptions); • This context differs from private service failure because managers need to publicly recover for other entities (such as the investors); • Because of the intangibility of services, a "recall" strategy is not possible; the problem cannot be easily isolated and repaired; • The service failure cannot be "separated" from a broader service, and a small event can affect a whole network of individuals. **<u>General purpose of the current research:</u>** Understanding the effectiveness of recovery efforts on investors' responses after service crises

Inspired by Gijsenberg et al. (2015).

The two quadrants that relate to *private* responses have received abundant attention in the literature. The earliest research efforts in this whole area were devoted on studying private product failures—that is, a product that fails to match the average quality of similar devices (Traynor, 1964). For instance, Folkes (1984) used attribution theory to explain when managers should replace, repair or offer a compensation after a product's failure. In turn, the quadrant on private service failures is probably the richest of all, in terms of content. Research has intensively examined the process "cognitions – emotions – behaviors" for individuals (see Gelbrich and Roschk [2010a] and Orsingher et al. [2010] for meta-analyses).

At a mass level, most research focuses on product-harm crisis rather than service crisis, as witnessed by a recent special issue on product-harm crisis (Laufer, 2015). Product-harm crises are defined as well-publicized events wherein products are found to be defective or dangerous (Klein & Dawar, 2004). A product-harm crisis typically happens when a firm's product fails to meet safety standards or contains a defect that could cause substantial inconvenience, harm or even death (Chen, Ganesan, & Liu, 2009). Firms' responses to product-harm crises mainly include implementing a product recall strategy and then offering replacement and apology (Dawar & Pillutla, 2000). Research also discussed customers' responses to recall (e.g., Ahluwalia et al. 2000; Cleeren et al. 2008) and the effectiveness of post marketing actions (Cleeren et al., 2013).

We argue that service crises deserve special attention because they possess different characteristics that affect managers' recovery plans. In contrast to *private service failures*, managers need to recover *both* privately and publicly from these events. In fact, managers need to redress the inconvenience for all participants involved in the incident (i.e., stakeholders,

investors, suppliers or the community) to restore the firm's reputation. This research focuses on investors' responses because of their influence on a firm's value.

Compared to *product-harm crises*, the recovery approach used for service crises is also different because of the intangible and inseparable natures of services (Gijsenberg et al., 2015; Wilson et al., 2012). Because defective products are easy to identify, a product recall is the method of choice for product-harm crises (Dawar & Pillutla, 2000). A firm can easily identify the dangerous product, notify customers to stop its consumption, remove it from the market, and fix it. The firm's other products remain unaffected because managers can circumscribe the impact of a product-harm crisis (Gijsenberg et al., 2015). In contrast, the recovery plan is not as straightforward for service crises. Because of the intangibility of services, the cause of a crisis may be difficult to identify, isolate and repair (Rushton & Carson, 1985). For example, it takes some time to understand the nature of an information breach; and once the information is disclosed, there is no clear solution to restore the loss in "privacy" to the state in which it was before the crisis (Malhotra & Malhotra, 2011). Using a metaphor, it is like trying to put back the toothpaste in a tube once the toothpaste is out. The inseparability of services also becomes an issue in a time of crisis. A service crisis typically affects all individuals who are simultaneously using that service; while in the case of a product-harm crisis, a small fraction of customers are affected (Gijsenberg et al., 2015). For example, a disruption in delivering Internet service affects all the users of that service at the same time, and the population size may be remarkable. Because of the difficulties associated with recovering from service crises, the current research examines the effectiveness of different recovery measures.

Service crisis recovery efforts For private service failures, a service recovery can be broadly defined as a firm's attempts to redress the inconvenience and to provide reparation to a

given individual (Smith et al., 1999). These private service recovery efforts—by enhancing individuals' perceptions of justice (Gelbrich & Roschk, 2010a)—have the ability to restore a higher level of satisfaction among customers or employees (Smith et al., 1999).

We extend this concept to our crisis context and define *service crisis recovery* as a firm's *public* attempts to redress and repair inconveniences to stakeholders affected by a service crisis. Given our interest in investors' responses, we pay special attention to the *public* recovery efforts available to the firm. Although there is limited literature on this topic in a service crisis context, we identify three recovery efforts available to managers: compensation (i.e., tangible outcomes), process improvement (i.e., improvements of deficient procedures) and apology (i.e., acknowledgement of a firm's blameworthiness). In the hypothesis section, we elaborate on the ways these recoveries influence investors' responses in different manners.

Information breach as a service crisis

We use information breaches as our service crisis context. According to Culnan and Williams (2009), an information breach is defined as an event signaling the potential or malpractice of unauthorized access to personal information of a group of stakeholders. Due to firms' massive collection of customers' personal data, the security of such information is a necessary condition leading to the development of strong customer relationships (Winer, 2001). Prior research provides evidence indicating that information privacy and confidentiality are important attributes forming service quality which result in customer satisfaction and trust (e.g., Lewis and Mitchell 1990; Yang and Fang 2004; Zeithaml et al. 2002). Accordingly, customers should view any violation of their confidentiality and privacy as a serious lack of service quality and as a major service failure. By not securing their promise of confidentiality sufficiently, firms fail to perform one of their basic obligations: protecting their customers.

From the employees' standpoint, firms must respect these individuals' right to safety, privacy and fair treatment (Carroll, 1991). Here, employees can be viewed as "customers inside the firm," and managers are responsible for providing their employees with services that satisfy their needs (Berry, 1981). The growth in strategic "Human Resources Management" systems has produced an increased demand for employees' personal information. In this context, an implicit social contract is established between employees and employers; firms need to carefully protect this information to maintain harmonious relationships with their employees (Ball, 2001). Because employee satisfaction is based largely on their perceptions of safety and fairness (Batt, 2002; Chuang & Liao, 2010), they would perceive any violation of this "contract" as an important "internal" service failure.

Consistent with these views, Malhotra and Malhotra (2011) urge marketing managers to view information breaches as customer service failures—rather than information systems failures—for two key reasons. First and as discussed, an information breach is a violation of the implicit social contract between important stakeholders (i.e., customers and employees) and a firm (Martin & Murphy, 2016). When personal information is disclosed in unauthorized manners, stakeholders perceive a form of betrayal, a key aspect characterizing important service failure (Grégoire & Fisher, 2008; Martin, Borah, & Palmatier, 2016). Second, Malhotra and Malhotra (2011) explain that frontline employees often play an important role in recovering information breaches. In that regard, the recovery process following an information breach is almost identical to the process in other forms of service failures. On the basis of these explanations, we argue that information breaches are major service failures.

In addition, the information breach context fits well the general purpose of our research in three ways. First, information breaches tend to be failures that inconvenience a large group of

stakeholders and that receive substantial media attention; these two characteristics correspond to our definition of service crisis. Second, information breaches are becoming more prevalent, so managers need to find effective ways to redress them. From 2006 to 2015, the DatalossDB.org database showed that the number of occurrences increased from 643 to over 1500 annually (« Statistics | DataLossDB », 2016). According to a recent survey (Bélanger and Crossler 2011), 85 percent of the responding companies had experienced a privacy breach in the previous year. Third, information breaches possess sufficient magnitude to influence the responses of investors (K. Campbell, Gordon, Loeb, & Zhou, 2003; Culnan & Williams, 2009).

Firm-idiosyncratic risk as a way to capture investors' responses

In finance, firms' stock risk—as reflected in stock-price volatility—is a key metric that reflects the future vulnerabilities and uncertainties of firms' cash flows. Accordingly, this metric is an indicator of firms' long term valuation. Total firm risk has two components: systematic and unsystematic risks. In particular, systematic risk—defined as the sensitivity of a firm's stock return to variation of the entire stock market return—stems from macroeconomic factors (such as inflation and interest rates) that are beyond the control of management. Unsystematic or idiosyncratic risk—defined as firm-specific volatility of stock return—is driven by micro firm-level factors (such as marketing strategies) that are controllable by management (Goyal & Santa-Clara, 2002; Srinivasan & Hanssens, 2009). In general, idiosyncratic risk accounts for the largest component of total firm risk (around 80%) (Goyal et al., 2003).

In light of this definition, this research focuses on idiosyncratic risk as the main evaluation criterion. By capturing investors' reactions to firms' decisions and news, this measure can represent the advantages or disadvantages associated with a firm's strategies (Srinivasan & Hanssens, 2009). The logic behind this metric is that firms' strategies influence their earnings

and cash flow fluctuations, and that investors carefully predict these changes and react to them in order to secure their investments. In other words, firm-idiosyncratic risk reflects market beliefs and is a valuable criterion to evaluate the effectiveness of marketing strategies (Rust et al., 2004). The marketing literature has used this metric to understand the effectiveness of several marketing strategies, such as corporate social responsibility (Luo & Bhattacharya, 2009), brand management (Rego, Billett, & Morgan, 2009) and service transition (Josephson, Johnson, Mariadoss, & Cullen, 2016). We follow a similar approach by examining the effects of service crisis recoveries on firm-idiosyncratic risk.

From an investment point of view, investors prefer stable earnings over volatile ones (Goyal et al., 2003) because high levels of volatility increase the number of securities required to generate a well-diversified portfolio (J. Y. Campbell, Lettau, Malkiel, & Xu, 2001). Therefore, understanding the financial impact of service crisis recoveries through idiosyncratic risk can benefit investors in managing their investment portfolios. From a managerial standpoint, managers carefully manage firm-idiosyncratic risks (Brown & Kapadia, 2007) because their compensation plans are significantly influenced by this metric (Core, Holthausen, & Larcker, 1999; Dechow, 1994). As a result, having more insights into the financial consequences of their service crisis recovery plans could assist them in enhancing their firm's performance and their own earnings.

2.3 Hypotheses: Linking service crisis recoveries to firm-idiosyncratic risk

A growing body of literature supports the fundamental logic that firm value corresponds to its resource-based potential (e.g., Tuli and Bharadwaj 2009; Luo and Bhattacharya 2009). The resource-based theory of the firm claims that valuable, rare and inimitable firm resources contribute to a sustainable competitive advantage leading to superior performance (Kozlenkova, Samaha, & Palmatier, 2014; Wernerfelt, 1984). Various resources have been illustrated as

valuable, such as well-established organizational processes, firm relations or reputation, and human capital resources (Barney, 1991; Srivastava, Fahey, & Christensen, 2001). Furthermore, firms' access to valuable resources results in profitability. Such outcome stems from a firm's competitive advantage over its competitors, and better relations between the firm and its stakeholders (Srivastava et al., 2001).

We argue that service crisis recovery efforts have the ability to impact important firms' resources. Accordingly, these recovery efforts could influence key processes and the relationships between firms and their stakeholders, which should ultimately result in firms' competitive advantage and greater performance. Investors should foresee the effects of recovery efforts, and the metric firm-idiosyncratic risk will reflect the responses of these individuals.

The effect of compensation

Compensations are tangible benefits that a firm offers to its stakeholders to restore their loss (Davidow, 2003; Smith et al., 1999). It can be offered as a correction, discount or replacement (Gelbrich, Gäthke, & Grégoire, 2016). Justice theory (Gelbrich & Roschk, 2010a) states that offering compensations to stakeholders increases their satisfaction through their perceptions of distributive justice. Here, distributive justice is defined as the appropriateness of the outcomes received by stakeholders after a service crisis (Smith et al., 1999).

We highlight that compensation does not *only* have an effect on distributive justice; this recovery effort also influences the other justice dimensions, but to a lesser extent. Indeed, Gelbrich and Roschk (2010a) in their meta-analysis found coefficients of .53, .30 and .22 between compensation and the distributive, procedural and interactional justice dimensions, respectively. Consistent with this larger effect size, researchers generally assume that

compensation operates mainly through its effects on distributive justice (Gelbrich, Gäthke, & Grégoire, 2015)

In line with this view, several studies and meta-analyses in service marketing find that a compensation leads to customers' positive reactions, such as satisfaction, loyalty, and positive word-of-mouth (Davidow, 2003); Gelbrich and Roschk 2010a; Orsingher, Valentini, and de Angelis 2010), through its effect on distributive justice. In their meta-analysis, Cohen-Charash and Spector (2001) report that distributive justice, as perceived by employees, advances job performance, organizational commitment and trust. Using this cumulative evidence, we posit that providing a compensation to customers and employees after a service crisis should enhance their perception of distributive justice, and help restore their relationship with the firm.

The current research makes a natural link between the noted positive effects of compensation and a firm's market value (as estimated by investors). Indeed, there is evidence that a substantial portion of a firm's market value relies more on its intangible assets—such as its processes, reputation and relationships with stakeholders—than on its tangible assets (Srivastava, Shervani, & Fahey, 1998). Relatedly, Pruitt and Peterson (1986) find that the loss of reputation and business relationships (i.e., intangible assets) due to a product-harm crisis is more impactful than the short-term loss of financial (and tangible) assets due to a product recall. These arguments suggest that the long-term value of compensations—in terms of reputation gain and relationship building—outweighs their short-term costs. We expect that investors will foresee these comparative effects (between intangible and tangible assets) in a service crisis context.

In sum, we argue that the restored relationship between a firm and its stakeholders after a compensation is an important resource that should lead to the firm's future cash flow stability. Consistent with this argument, a large number of studies (e.g., Edmans 2011; Ngobo et al. 2012;

Tuli and Bharadwaj 2009) empirically illustrate the positive impact of stakeholder satisfaction and strong relationships on shareholder value—which would mean a reduced firm-idiosyncratic risk in the current study. Formally:

H1: Offering compensation is negatively associated with firm-idiosyncratic risk.

The effect of process improvement

We define process improvement as a firm's actions that aim to improve its deficient procedures in order to prevent future failures (Johnston & Michel, 2008). This recovery effort focuses on minimizing the reoccurrence of a failure as well as on enhancing trust, satisfaction and relationship quality among stakeholders (Davidow, 2000; Johnston & Fern, 1999; Johnston & Michel, 2008).We argue this recovery effort improves firm performance in three ways.

First, the development of processes to protect stakeholders' information should naturally lead to a competitive advantage, which results into superior performance. Here, organizational processes have been defined as important intangible resources that carry a great deal of value for firms (Srivastava et al., 1998). Second, process improvement indicates a firm's willingness to invest in relationships with its stakeholders; these perceived investments enhance stakeholders' trust and commitment, which encourages them to stay in relationship with a firm. Third, this recovery effort should have a direct and positive impact on perception of procedural justice[2] (Gelbrich & Roschk, 2010a; Johnston & Michel, 2008; Martin & Murphy, 2016), which is defined as the appropriateness of the policies and practices that a firm puts in place to serve its

---

Similar to the effects of a compensation, the efforts of process improvement influence the two other justice dimensions (i.e., distributive and interactional) (Gelbrich & Roschk, 2010a). However, the effect of process improvement on procedural justice (.51) is much stronger than its effects on interactional justice (.14) and distributive justice (.12).

stakeholders (Tax et al., 1998). This heightened sense of procedural justice should enhance stakeholders' perceptions of trust and relationship quality (Cohen-Charash & Spector, 2001; Tax, Brown, & Chandrashekaran, 1998; Van Vaerenbergh, Larivière, & Vermeir, 2012). Based on these reasons, the extant research provides evidence that process improvement increases customers' satisfaction and repurchase intention (Johnston & Fern, 1999; Palmatier, Dant, Grewal, & Evans, 2006; Van Vaerenbergh et al., 2012); and as well, it increases employees' citizenship behavior, organizational commitment and job satisfaction (Daileyl & Kirk, 1992; Tsui, Pearce, Porter, & Tripoli, 1997).

In sum, the advantages carried by process improvement should all ultimately improve the relationship quality between firms and stakeholders. According to the resource-based theory, these stronger relationships should become important intangible resources leading to a greater sustainable advantage, which in turn would result in greater firm performance. In a way similar to the argument made in H1, the long-term intangible benefits associated with process improvement should loom larger than its short-term costs (Srivastava et al., 1998). Hence:

H2: Offering process improvement is negatively associated with firm-idiosyncratic risk.

The counterintuitive effect of apology

Broadly defined, an apology refers to messages containing the acknowledgement of blameworthiness for a negative event; they can include expressions of remorse, sorrow or regret (Davidow, 2003; Roschk & Kaiser, 2013). By making an apology, a firm accepts its responsibility for the failure and shows regret for what happened (Liao, 2007). Consistent with prior research (Cohen, 1999; Robbennolt, 2003), we consider these different expressions—sorrow, remorse and regret—as part of the same "apology" construct. Although we see immense

value in experimentally manipulating different aspects of an apology (Roschk & Kaiser, 2013), field studies do not typically allow this level of control.

The ability of an apology to attenuate the negative responses of stakeholders versus investors is not as straightforward as the two other recovery efforts. An apology involves *both* the expression of a firm's concern for its stakeholders (which could strengthen the relationship) *and* a potential perception of guilt admission for the failure (which could be used against the firm) (Davidow, 2000; Miller, Craighead, & Karwan, 2000; Patel & Reinsch, 2003). Compared to compensation and process improvement, an apology more directly relates to a perception of blame acceptance (Davidow, 2000). Indeed, firms could provide compensation and improve their processes without accepting any direct blame for a service crisis. They could simply argue that they engaged in these last two recoveries to satisfy their stakeholders and not because they felt responsible for what happened. Hence, the effects of an apology are more complex—compared to the other two recoveries—because its effects could be either positive or negative.

On the one hand, the expression of an apology can show a firm's empathy and concern for its stakeholders. Such a gesture could restore stakeholders' self-esteem and remedy psychological loss, which would improve their relationship with the firm (Gelbrich & Roschk, 2010a; Liao, 2007; Orsingher et al., 2010; Smith et al., 1999; Wirtz & Mattila, 2004). Many studies have shown this general positive effect, and Gelbrich and Roschk's meta-analysis finds that an apology is positively linked to satisfaction. In general, an apology tends to have a favorable influence on some stakeholders.

On the other hand, a firm's acceptance of guilt and blame can create a perception of liability that could eventually hurt the firm (Boshoff, 1997; Davidow, 2000). First, acceptance of blame could acknowledge the weak performance of a firm, which could devalue its reputation.

Second, it could make the firm a potential target for lawsuits; the acceptance of blame can be used in court and could increase plaintiffs' chances of winning their cases (Cohen, 1999, 2000; Patel & Reinsch, 2003; Robbennolt, 2003; Tyler, 1997). For these reasons, lawyers and politicians regularly advise not to apologize after wrongdoing.

Interestingly, some prior research in services has confirmed the dual effect (i.e., positive versus negative) of an apology. Roschk and Kaiser (2013) show that an apology is only effective when it is offered on time and with high intensity and empathy. Other researchers find that an apology is mainly effective when it is incorporated with a tangible compensation (Wirtz and Mattila 2004). In turn, Fuchs-Burnett (2002) argues that an effective organizational apology needs to carry a deep acknowledgement of injury, a sense of accountability, and measures to prevent future failures. Finally, Brinke and Adams (2015) found that negative outcomes occurred for verbal apologies that were not accompanied by facial sadness. In sum, it appears that an apology could lose in effectiveness or even backfire under some conditions.

Building on this literature, even if regular *stakeholders* may favorably respond to an apology, we argue that *investors* may discard this information and respond negatively for two key reasons. First, investors are loss averse and mainly concerned about protecting their long-term investments. Because investors can easily interpret an apology as an acceptance of blame and an admission of guilt, they will fear the risk of lawsuits and expensive class actions. Investors perceive that a firm makes itself vulnerable by apologizing, as it could not easily deny its responsibility in court. Second, service crises can affect an especially large number of stakeholders: an ideal condition for such class actions. Translating this logic in financial terms, the risk of litigation, as perceived by the investors, could threaten the stability of a firm's cash flow. Therefore, the expression of an apology increases a firm's idiosyncratic risk. Formally:

H3: Offering apology is positively associated with firm-idiosyncratic risk.

In addition to the above hypotheses, we examine the interactions among these three service crisis recoveries so that we can identify the "optimal" combination of recoveries to reduce a firm's idiosyncratic risk (e.g., Blodgett et al. 1997). These interactions will also help us to understand the consequences of concurrently offering two or three service crisis recoveries. We do not offer a formal hypothesis for these interactions because recovery efforts have not consistently been found to interact with each other (Davidow, 2003). Moreover, little is known about these effects for investors.

2.4 Research design

Data and sample

We constructed our dataset using records and announcements from several sources (i.e., Privacy Rights Clearinghouse, Factiva and web search engines, and Standard & Poor's COMPUSTAT database). We started by collecting the announcements of information breach events from the Privacy Rights Clearinghouse (PRC) database.[3] This source contains data about information breach events and relevant consumer rights in North America. From 2001 to 2013, this database reported 4486 events, 1639 of which did not belong to public corporations, so we excluded them from our data collection process. The remaining 2847 events belonged to private and publicly traded firms in different industry sectors.

Given the large number of events, a subsample was drawn from the event population. For sub-sampling, we could not apply simple random sampling of events, because the list of events involving publicly traded firms was not available. To address this issue, we employed cluster

---

Privacy Rights Clearinghouse. *Chronology of Data Breaches*. Retrieved January 10, 2014 from https://www.privacyrights.org/data-breach

sampling technique, which is appropriate when the size of a database is large and when the list of relevant observations is not available (Hansen & Hurwitz, 1943; Henry, 1990). Cluster sampling divides the population in clusters of observations according to one of the characteristics of the observations. Thereafter, clusters are randomly selected by simple random sampling and all observations within those selected clusters are processed, and if appropriate (e.g., involve publicly traded firms), are added to the final dataset. We clustered the events of information breaches in the PRC database according to their calendar weeks of announcements.

We targeted a final sample size of at least 200 observations for our research according to the suggested rules of thumb (N > 104 + number of IVs or 10 observations per IV) (Maxwell, 2000; VanVoorhis & Morgan, 2007). Our initial inspection of the database revealed that each week, on average, included two to three events involving publicly traded firms. Hence, to achieve our targeted sample size and to have enough observations after attrition in further stages of data collection (for confounding events, missing data, etc.) (McWilliams & Siegel, 1997), we decided to randomly select 160 weeks from 2001 to 2013 and collected events that happened during those weeks. Selecting 160 weeks (out of 676 weeks) was appropriate to represent the diversity of the database. This sample size is subject to a margin of error of approximately 3%.

By considering 160 weeks, we collected 345 observations involving publicly traded firms or their subsidiaries. Next, we cross-checked these observations through the Factiva database and web search engines to obtain the details of the events, precise dates of announcements, and all subsequent recovery offerings from publicly available news websites and governmental databases. We removed 44 observations at this stage because we did not find any evidence of the occurrence of these events in other sources. In addition, we removed 41 cases because the available documents about the events were governmental documents that were not available to

the public, or because the available information was incomplete and did not allow coding our variables. Following standard practice (e.g., Dewan and Ren 2007), we dropped 37 cases with confounding announcements within one week, before and after the event, to make sure that the announcements about each particular case were not affected by other events. We considered the following type of news to be confounding announcements: earnings announcements, mergers and acquisitions, and large profit announcements. We removed two observations because of missing data in Standard & Poor's COMPUSTAT database, which was used to compute financial control variables. Finally, in order to be able to control for the type of victimized stakeholder (i.e., customers or employees) as an important control variable, we removed nine cases in which both groups were affected. After following these steps, we were left with 212 cases, including 171 different publicly traded companies.

Relevant announcements about each case usually extend over a one-week period (see Appendix 2 for an example). Based on the Efficient Markets Hypothesis (EMH) in finance, investors fully and immediately react to any new information that has value relevance (Srinivasan & Hanssens, 2009). Hence, in our context, the stock value of the involved firms is expected to start changing from the first announcement about the service crisis recovery. However, to make sure that investors have considered all the relevant information, we chose as our event dates five trading days (one calendar week) after the initial announcements about the recovery plans. The exclusion of these five days also makes our analysis unbiased by the abnormal returns surrounding the first announcement (Bansal & Clelland, 2004). Table 2 provides the industry composition of our sample firms in addition to examples; the industries are identified by the two-digit North American Industry Classification System (NAICS) code.

Table 2 Industry composition of dataset

Two-Digit NAICS Code	Industry Name	Frequency		Example
		N	%	
11	Agriculture, forestry, fishing and hunting	1	.5	Monsanto Co.
21	Mining and oil and gas extraction	2	1	Murphy Oil Corp.
22	Utilities	4	2	Xcel Energy Inc.
23	Construction	1	.5	MasTec Inc.
31-33	Manufacturing	40	19	Sony Corp.
42	Wholesale trade	6	3	PSS World Medical Inc.
44	Retail trade	15	7	Best Buy Inc.
48-49	Transportation and warehousing	4	2	Alaska Air Group Inc.
51	Information	42	20	Oracle Corp.
52	Finance and Insurance	67	31	Bank of America
53	Real estate and rental and leasing	4	2	Wyndham Worldwide Corp.
54	Professional, scientific and technical services	9	4	Ceridian Corp.
56	Administrative and support	6	3	Equifax Inc.
62	Health care and social assistance	1	.5	DaVita HealthCare Inc.
72	Accommodation and food services	10	4.5	McDonald's Corp.

In our dataset, the events of information breach were due to several causes, including hacker attack (39 cases), theft of equipment by an outsider (40 cases), misplaced data source (20 cases), employees' intentional breach (67 cases), employees' accidental mistake (35 cases) and technical errors (11 cases). Firm-level accounting data to compute the financial control variables were obtained from Standard & Poor's COMPUSTAT database.

Service crisis recovery coding

For the content analysis of our public announcements and on the basis of our conceptual definitions, we defined *compensation* as offering any tangible redress to restore the loss of victimized groups (Davidow, 2003; Smith et al., 1999). *Process improvement* was defined as any promise or indication to improve or develop the organizational processes that led to the information breach (Davidow, 2000; Johnston & Fern, 1999; Johnston & Michel, 2008). *Apology* was defined as the presence of the terms "apology," "regret," "sorry," "remorse" or their synonyms by the responsible firm in their public communications (Cohen, 1999; Liao, 2007;

Roschk & Kaiser, 2013). Appendix 1 presents these definitions and representative examples taken from our dataset. In addition, Appendix 2 gives an example of the announcements of a specific case and shows how we coded the service crisis recoveries for this specific case.

Following Kassarjian (1977), we trained two independent coders to recognize the three service crisis recoveries of interest. A few "warm-up" sessions were necessary to adjust the coding scheme and help the coders to get familiar with the instructions. After these sessions, the level of agreement between coders was high. Applying Perreault and Leigh's (1989) reliability,[4] this index indicated high levels of agreement with scores of .921 for compensation, .852 for process improvement and .932 for apology. The coders used discussion to resolve disagreements.

Firm-idiosyncratic risk measure

We calculated idiosyncratic risk by using daily return data for each firm within the year following the recovery announcement. Our measure of idiosyncratic risk is based on a regression projection of stock returns of each firm on the returns of the market index and other relevant factors. We applied a widely accepted approach: the Fama-French four-factor model (e.g., Luo and Bhattacharya 2009). We also checked our results through the Market Model specification.

The Fama-French four-factor model proposes that a firm's daily stock return ($r_{i,d}$) is a function of market return (r_d^{MKT}), the difference of returns between small and big stocks (r_d^{SMB}), the difference of returns between high and low book-to-market stocks (r_d^{HML}), and return momentum (r_d^{UMD}), along with a residual ($u_{i,d}$):

$$r_{i,d} = \alpha_i + \beta_i^{MKT} r_d^{MKT} + \beta_i^{SMB} r_d^{SMB} + \beta_i^{HML} r_d^{HML} + \beta_i^{UMD} r_d^{UMD} + u_{i,d} \quad (1)$$

$I_r = \{[(F/N) - (1/k)][k/(k-1)]\}^{0.5}$, for $F/N > 1/k$; where F is the frequency of agreement between coders, N is the total number of judgments and k is the number of categories.

where α_i is the intercept term and $u_{i,d} = \rho u_{i,d-1} + \delta_{i,d}$. $\delta_{i,d}$ is assumed to be a normal random variable with a mean of "0" and variance of σ^2_{δ}, which allows Equation 1 to control for serial correlation in the residual term. Our measure of firm-idiosyncratic risk is the variance of residuals $[1/n \times (\Sigma^{n}_{d=1} u^2_{i,d})]$ of the regression of Equation 1, where n denotes 252 trading days (one calendar year) starting five trading days after the first service crisis recovery announcement.

Following Ferreira and Laux (2007) and Luo and Bhattacharya (2009), our dependent variable is relative idiosyncratic risk, which is the ratio of idiosyncratic risk to total firm risk and is equal to $1\text{-}R^2_i$, where R^2_i is the coefficient of determination for Equation 1. Because of the bounded nature of R^2_i, we use a logit transformation of $1\text{-}R^2_i$ as the measure of idiosyncratic risk:

$$V_i = \text{Ln}\left(\frac{1-R^2_i}{R^2_i}\right) \quad (2)$$

Ferreira and Laux (2007) argue that scaling idiosyncratic risk by total risk distinguishes firm-specific return volatility from market-related and industry-related returns volatility; and consequently, the results will be comparable across industries and years. It should be noted that some business activities are subject to economy-wide and industry-wide shocks that make the absolute idiosyncratic risk (variance of residuals) more volatile, with this volatility stemming from environmental factors (Durnev, Morck, Yeung, & Zarowin, 2003). Hence, this scaling helps us make our results comparable across the wide range of industries and years in our dataset. The required daily stock price data was obtained from the CRSP database, and the daily data for the Fama-French factors from the Kenneth R. French database.

Control variables

Following similar studies (Ferreira & Laux, 2007; Luo & Bhattacharya, 2009), we controlled for multiple firm, industry, and event level covariates in our analysis to capture the extent to which service recovery offerings can truly explain firm-idiosyncratic risk. Specifically:

Profitability We measured profitability as return on assets. Firms with high profitability show future financial health and are more favorable to investors (J. Campbell, Hilscher, & Szilagyi, 2008).

Profits' volatility This variable was measured as the standard deviation of the prior five years' return on assets. High variations in profitability reveal future cash flow uncertainty (J. Campbell et al., 2008).

Leverage The ratio of long-term debt to total assets was computed to control for leverage. Larger long-term debt indicates higher risk of default, which affects a firm's future cash flow (Ben-Zion & Shalit, 1975).

Market capitalization We computed this variable as the logarithm of multiplication of the number of shares outstanding by the market price. Firms with higher market capitalization show less volatile stock returns (Brandt, Brav, Graham, & Kumar, 2010).

Firm age The age of the firm was measured as the logarithm of the number of months since the stock's inclusion in CRSP database. Older firms exhibit creditworthiness, less risk of disappearance, and more cash flow stability (Ben-Zion & Shalit, 1975).

Firm size We measured firm size as the logarithm of total asset value. All else being equal, firms with a larger size exhibit more return stability (Ben-Zion & Shalit, 1975).

Industry concentration According to Campbell et al. (2001), industry-level variables are key variables to explain the volatility of stock returns. Hence, we measured a series of variables to control for industry-level variables. First, we computed industry concentration by the Herfindahl-Hirschman Index (HHI). HHI is measured as the sum of the squared market share of the individual firms in the industry based on the three-digit SIC code. Market shares are calculated by sales data. The HHI industry concentration ratio controls for the industry's

competitive intensity. Firms in highly concentrated industries are less risky because they engage in less competition and practice less innovation (Hou & Robinson, 2006).

Type of industry Two-digit NAICS codes were used as fixed effects to control the industry-level risk. Natural risk varies in different industry sectors (J. Y. Campbell et al., 2001). We grouped firms with close NAICS codes together to have at least 10 cases for each sector.

Year This refers to the year when the recoveries were offered. We used a fixed effect to operationalize this variable. This market-level variable calibrates for yearly microeconomic fluctuations (McGahan & Porter, 1997).

Event controls We controlled for the cause of the information breach to calibrate the type of failure, since different types of failures present different levels of loss (Smith et al., 1999; Weun, Beatty, & Jones, 2004), and these failures may signal different categories of firms' weaknesses to investors. We also controlled for the group of victimized stakeholders (customers or employees).

2.5 Results

Descriptive statistics

Table 3 presents descriptive statistics and the correlations among the variables used in the study. Out of the 212 cases, 71 failures occurred against employees and 141 against customers. Overall, 57 cases did not offer any recovery in their communication, and the rest of cases offered one or a combination of recoveries. Specifically, 108 cases offered compensation, 93 cases provided process improvement, and 96 cases expressed apology after the information breach.

This table shows that there is a low risk of collinearity among variables, with all correlations being below .5. In addition, the correlations between service crisis recovery efforts (as the focal variables of our study) are all below .39, which indicates that they are distinct constructs. For further assurance of the low linear dependence among variables, we computed

their variance inflation factors (VIF). All variance inflation factors were below 4, indicating low collinearity among variables (O'brien, 2007).

Table 3 Descriptive statistics and correlation matrix (N = 212)

Variables	M	SD	1	2	3	4	5	6	7	8	9	10	11
1. Firm-idiosyncratic risk	.60	.98											
2. Compensation	.51	.50	–.14**										
3. Process improvement	.46	.50	.02	.33***									
4. Apology	.45	.50	–.01	.21***	.39***								
5. Customers victimized	.67	.47	.10	–.24***	–.20***	–.19***							
6. Profitability	.04	.09	–.17**	.02	.05	–.01	–.15**						
7. Profits' volatility	.04	.09	.19***	–.06	–.02	.03	–.16**	.06					
8. Leverage	.19	.19	.12*	–.03	.05	.09	.01	.11*	–.02				
9. Market capitalization	9.11	2.12	–.46***	–.10	–.12*	–.15**	.09	.25***	–.21***	–.09			
10. Firm age	5.24	.99	–.11	–.10	.06	–.03	.03	.15**	–.01	–.02	.15**		
11. Firm size	9.89	2.46	–.45***	–.04	–.16**	–.24***	.21***	–.07	–.32***	–.15**	.38***	.06	
12. Industry concentration	1743.64	1593.94	.13*	.00	.11	.18**	–.10	.00	.04	–.06	–.19***	.09	–.32***

*p<.10; **p<.05; ***p<.01.

Tests of hypotheses

Model specification We tested our hypotheses through two fixed-effect simple linear regression models. Model 1 assesses the effect of three service crisis recoveries (compensation, process improvement and apology) on firm-idiosyncratic risk. Model 2 examines the interactions among these three recovery strategies.

An initial outlier diagnostic test, through the minimum covariance determinant (MCD) method, illustrates the existence of 10 outliers in our dataset, one of which is a bad leverage point (i.e., observations with outlying x and y that do not follow the pattern of the majority of observations) (Rousseeuw & Driessen, 1999). The MCD method detects outliers by finding a subsample of observations whose covariance matrix has the lowest determinant. Then, using Equation 3, the robust distance of each observation from this subsample is computed:

$$RD(x_i) = [(x_i - T(X))^T C(X)^{-1}(x_i - T(X))]^{1/2} \quad (3)$$

where T(X) is the average of observations of the subsample and C(X) is their covariance matrix. The observations whose robust distance is higher than the cutoff value are detected as outliers. Cutoff value is equal to the square root of the 97.5% quantile of the chi-square distribution with degrees of freedom equal to the number of variables.

Outliers and leverage points are sources of multicollinearity that can cause a bias in the estimate of coefficients (Andrews & Pregibon, 1978; Kamruzzaman & Imon, 2002). To address this issue, we applied the M-estimator robust regression, which bounds the influence of outliers, to examine our hypotheses. This method is not robust to bad leverage data points but is useful when vertical outliers and good leverage points are a concern (Rousseeuw & Leroy, 1987), as is the case in the current study. Also, this method can reduce the concern about heteroscedasticity (Maronna, Martin, & Yohai, 2006).

In contrast to ordinary least square estimation that minimizes the sum of squares of the residuals, the M-estimator method minimizes the influence of outliers on the parameter estimation (Equation 4):

$$\min \sum_i \rho(r_i(x)) \tag{4}$$

where r is the residual vector ($r = y - Ax$) and ρ is the Huber loss function defined by:

$$\begin{cases} \frac{t^2}{2} & \\ & \frac{c^2}{2} \end{cases} \tag{5}$$

where c is an estimate of σ (Huber, 1973).

Cross-sectional regression results The main results are presented in Table 4. The results of our first regression (i.e., Model 1) show that compensation (β = –.241, SE = .103, chi-square = 5.46, $p < .05$), process improvement (β = –.298, SE = .098, chi-square = 9.21, $p < .01$) and apology (β = .299, SE = .102, chi-square = 8.62, $p < .01$) significantly influence firm-idiosyncratic risk. These results support H1, H2 and H3, respectively. Specifically, Model 1 indicates that compensation and process improvement are associated with .241 and .298 decreases, respectively, in a firm's idiosyncratic risk for one year after the announcement of these recovery initiatives. As we predicted, the results demonstrate that apology raises a firm's idiosyncratic risk for the same period. Model 2 shows that the interactions among the different recovery efforts are not significant—these results indicate that the effects of the recovery efforts are independent of each other in this context.

Table 4 Results of the impact of service crisis recoveries on firm-idiosyncratic risk (Fama-French four-factor approach)

Variables	Hypothesis	Model 1 (Main model)		Model 2 (Interactions)	
		B	S.E.	B	S.E.
Effects					
Compensation (C)	H1(–)	–.241**	.103	–.288*	.147
Process improvement (P)	H2(–)	–.298***	.098	–.298*	.172
Apology (A)	H3(+)	.299***	.102	.340*	.195
C × P				.088	.262
C × A				–.060	.264
A × P				–.223	.293
C × P × A				.205	.394
Event controls[a]					
Customers victimized		.066	.111	.048	.110
Hacker attack		.057	.219	.104	.217
Theft of equipment by outsider		.173	.214	.222	.211
Misplaced data source		.256	.235	.279	.232
Employee intentional breach		.176	.212	.204	.209
Employee accidental mistake		–.049	.221	.003	.219
Technical error		0[b]	.	0[b]	.
Firm Controls					
Profitability		–1.046*	.629	.345	.766
Profits' volatility		1.300**	.535	1.019*	.536
Leverage		.024	.266	.080	.263
Market capitalization		–.117**	.045	–.148***	.046
Firm age		–.064	.045	–.072	.045
Firm size		–.064	.043	–.030	.044
Industry and market controls					
Industry concentration		–.001	.001	–.001	.001
Type of industry dummies			Yes		Yes
Year dummies			Yes		Yes

*p<.10; **p<.05; ***p<.01.

a. The reference category for the cause of the information breach is: technical error.

b. This parameter is set to zero because it is redundant.

Along with the three identified main effects (e.g., J. Campbell et al. 2008; Ben-Zion and Shalit 1975), we find that the control variables firm profitability and market capitalization are negatively associated with firm-idiosyncratic risk. Moreover, profits' volatility is positively associated with firm-idiosyncratic risk.

Robustness check

To verify the robustness of our results, first, we measured firm-idiosyncratic risk using the Market Model approach and repeated the estimation of Models 1 and 2. The Market Model approach relates a firm's daily stock return only to the market return. This single-factor model imposes fewer restrictions on returns compared to the Fama-French four-factor model; thus, it alleviates the concern about biases arising from restrictions (MacKinlay, 1997):

$$r_{i,d} = \alpha_i + \beta_i r_{md} + u_{i,d} \quad (6)$$

where, $r_{i,d}$ is the firm's daily stock return, r_{md} is the market return, α_i is the intercept and $u_{i,d}$ is the residual. As reported in Table 5, the results remained mostly unchanged.

Table 5 Results of the impact of service crisis recoveries on firm-idiosyncratic risk (Market Model approach)

Variables	Hypothesis	Model 1 (Main model)		Model 2 (Interactions)	
		B	S.E.	B	S.E.
Effects					
Compensation (C)	H1(–)	–.256***	.098	–.296**	.150
Process improvement (P)	H2(–)	–.333***	.094	–.339*	.177
Apology (A)	H3(+)	.189*	.098	.413**	.200
C × P				.218	.268
C × A				–.199	.271
A × P				–.361	.300
C × P × A				.314	.404
Event controls[a]					
Customers victimized		.135	.107	.036	.112
Hacker attack		.225	.209	.232	.222
Theft of equipment by outsider		.251	.204	.223	.216
Misplaced data source		.248	.226	.346	.236
Employee intentional breach		.094	.203	.176	.214
Employee accidental mistake		–.013	.211	.081	.224
Technical error		0[b]	.	0[b]	.
Firm Controls					
Profitability		1.087	.731	.763	.779
Profits' volatility		1.598***	.516	1.453***	.548
Leverage		.351	.257	.214	.268
Market capitalization		–.139***	.045	–.164***	.048
Firm age		.019	.045	.030	.048
Firm size		.010	.042	.022	.045
Industry and market controls					
Industry concentration		–.001	.001	–.001	.001
Type of industry dummies			Yes		Yes
Year dummies			Yes		Yes

*p<.10; **p<.05; ***p<.01.

a. The reference category for the cause of the information breach is: technical error.

b. This parameter is set to zero because it is redundant.

Second, we excluded low-priced stocks and small-cap firms from our dataset and repeated Model 1. In this way, we can verify whether the obtained results are not driven by firms

with low-priced stocks or small-cap, as these types of firms have relatively higher volatile stock returns (Brandt et al., 2010). We excluded firms with average annual stock prices below $5. Eight observations (4 %) were deleted. The new results mirrored the previous results: compensation (β = –.173, SE = .103, chi-square = 2.85, $p < .1$), process improvement (β = –.263, SE = .095, chi-square = 7.67, $p < .01$), and apology (β = .221, SE = .101, chi-square = 4.80, $p < .05$).

Finally, we excluded firms with market capitalizations that place them in the smallest NYSE/AMEX size decile of 10. The size deciles were obtained from CRSP Cap-based portfolio. Overall, 43 observations (20%) were omitted. Again, results were statistically similar: compensation (β = –.241, SE = .103, chi-square = 5.50, $p < .05$), process improvement (β = –.225, SE = .097, chi-square = 5.45, $p < .05$), and apology (β = .286, SE = .104, chi-square = 7.60, $p < .01$). In sum, we conclude that our findings are robust according to several stringent tests.

Additional analyses

To further test the robustness of our results, we conducted seven post-hoc analyses, which we summarize below and in Web Appendix C.

Durational persistence of impacts of service crisis recoveries The impact of firms' decisions and strategies on their stock value prevail during a finite time horizon because their stock value will capture other news and information over time. For our central analyses, we chose one calendar year time horizon, for this time horizon is long enough to capture the reaction of investors and to depict the gravity of the investigated recovery strategies (e.g., Luo and Bhattacharya 2009; Rego et al. 2009).

As described in this section, in order to better understand the durational persistence of the impacts of service crisis recoveries, we computed the idiosyncratic risk for different time

horizons (calendar quarters) and repeated Model 1 for each window. We estimated idiosyncratic risks trough the Fama-French four-factor approach, and we adjusted financial control variables corresponding to each window. For the sake of parsimony, Table 6 presents only the parameters associated with our three focal recovery plans for several time windows. These results reveal that the impact of service crisis recoveries on firm-idiosyncratic risk starts two quarters after their announcement and lasts for up to two calendar years (8 calendar quarters) after their announcement. After two years, the significance of compensation weakens, while the significance of other dimensions tends to persist.

Table 6 Durational persistence of the impact of service crisis recoveries on firm-idiosyncratic risk (Fama-French four-factor approach) in different time horizons

	Model 1 2 quarters (+1, +126)		**Model 1 3 quarters (+1, +189)**		**Model 1 5 quarters (+1, +315)**		**Model 1 7 quarters (+1, +441)**		**Model 1 8 quarters (+1, +504)**	
Variables	**B**	**S.E.**	**B**	**S.E.**	**B**	**S.E.**	**B**	**S.E.**	**B**	**S.E.**
Compensation	–.225*	.118	–.197*	.110	–.225**	.104	–.183*	.110	–.136	.106
Process improvement	–.189*	.113	–.230**	.106	–.271***	.099	–.239**	.105	–.238**	.101
Apology	.220*	.115	.222**	.110	.281***	.103	.227**	.108	.183*	.105

*p<.10; **p<.05; ***p<.01.

Interaction of type of victimized stakeholders and cause of information breach To better understand the effectiveness of the recovery efforts, we checked whether the type of victimized stakeholder (i.e., customers or employees) or the cause of information breach can influence the relationship between recovery efforts and firm-idiosyncratic risk. To this end, we examined the interaction of the variable "customers victimized" with the three recovery strategies. The results did not show any significant interaction with respect to compensation (β =

–.270, SE = .215, chi-square = 1.58, p = .210), process improvement (β = .330, SE = .210, chi-square = 2.39, p = .122) and apology (β = –.178, SE = .217, chi-square = .67, p = .413). Hence, the type of stakeholder does not change the effects of recovery strategies. Moreover, we interacted each cause of the information breach (type of failure) with the three recovery strategies. These interactions did not show any significant results either. Therefore, the type of failure does not influence the effects of recovery efforts, in our context.

Comparing the strength of compensation versus process improvement Prior studies report varied effect sizes for compensation versus process improvement (Cohen-Charash & Spector, 2001; Gelbrich & Roschk, 2010a). To compare the strength of the impact of these two recoveries on idiosyncratic risk, we employed the "standard method" suggested by Schenker and Gentleman (2001). This method builds an interval around the difference between the point estimates of two dimensions. To do so, the method adds and subtracts the z-value multiplied by the square root of the sum of the squared standard error of each point estimate ($(Q_1 - Q_2) \pm 1.96(SE_1 + SE_2)^{1/2}$). If that interval does not include zero, the difference between the two dimensions is statistically significant. In our case, the 95% confidence interval for the difference between these two dimensions includes zero ($CI_{95\%}$ = .94 to –.82). This result suggests that there is no significant difference between the predictive validity of compensation versus process improvement in our study.

The risk of apology and liability As presented earlier, our explanation for the positive effect of an apology on idiosyncratic risk relies on the increased liability risk associated with a lawsuit. To provide more evidence for this reasoning, we used the number of affected individuals as a proxy for liability risk. Our logic is that the more individuals who are affected by a breach, the more likely a firm is to suffer from a major class action lawsuit. Based on this variable, the

risk of liability is greater as the number of affected individuals increases. Firms do not always disclose the number of affected individuals; we had to consider a subsample of 114 observations.

We examined the interaction between the number of affected individuals and offering apology. We expected that the positive effect of an apology on firm idiosyncratic risk should be higher for a large number of individuals (i.e., high liability risk) versus a low number of individuals (i.e., low liability risk). When a large number of individuals experience a service crisis and the firm publicly apologizes for it simultaneously, investors should interpret this situation as being especially negative because of the high potential of a class-action lawsuit.

As expected, the interaction effect of the number of affected individuals and the presence of an apology was positive and significant ($\beta = .199$, SE = .103, chi-square = 3.75, $p < .05$). Also, we did a spotlight analysis at one standard deviation above and one standard deviation below the mean level of the number of individuals. Our results show that, in the low liability risk situation, the impact of offering apology on firm-idiosyncratic risk is negative but not significant ($\beta = -2.13$, SE = .128, chi-square = 2.76, $p > .05$). However, in the high liability risk situation, offering apology keeps its positive impact on firm-idiosyncratic risk ($\beta = 2.72$, SE = 1.23, chi-square = 4.85, $p < .05$). These findings suggest that offering an apology is more damaging for firms (in terms of idiosyncratic risk) when there are a large number of affected individuals—we argue that investors will then anticipate a potential class action lawsuit. This result is consistent with the rationale underlying H3.

The intensity of an apology We checked whether expressing high intensity apologies during communications have an impact on firm-idiosyncratic risk. To do so, we recoded the observations that offered apologies into low intensity (38 cases) and high intensity (58 cases). High intensity apologies include those cases in which firms express apologies either more than

once or accompanied with intensifying phrases such as "we deeply apologize". This time, the dummy code of apology has three levels of no apology, low intensity apology and high intensity apology. We replicated our Model 1 and we obtained similar results: Compensation ($\beta = -.244$, SE = .102, chi-square = 5.74, $p < .05$), process improvement ($\beta = -.307$, SE = .098, chi-square = 9.98, $p < .01$), and apology ($\beta = .194$, SE = .059, chi-square = 10.90, $p < .01$). These results suggest that an apology, even when it is offered with high intensity, can backlash against firms.

Impacts of combinations of recovery plans As mentioned earlier, some firms in our dataset offered no recovery plan, while others offered one or more recovery plans. To determine if there is a pattern associated with concurrent recovery strategies, we tested the interaction effects between the three variables. As presented in Table 4, the interactions between these recovery plans were not significant. Model 2, Table 4, shows that the three-way interaction as well as all the two-way interactions were not significant (all *p*s > .10). Further analyses in which we excluded the three-way interaction also yielded non-significant parameters for the two-way interactions. Overall, this suggests that investors do not see any "synergy effect" among the recovery efforts. In managerial terms, it means that the combination of both compensation and process improvement is the strategy with the greatest potential to reduce a firm's idiosyncratic risk. In turn, an apology tends to increase this risk, even when combined with other recoveries.

2.6 Discussion

A summary of our results

Our investigation reveals that offering compensation (H1) or process improvement (H2) reduces firm-idiosyncratic risk; however, offering apology can backfire for firms, as it increases this important risk (H3). Our findings are in line with the findings of Z. Fang et al. (2013), who show that offering compensations and process improvements to victimize stakeholders has a longer decay time effect on satisfaction, whereas offering apology has a shorter one.

Our analyses suggest that the type of victimized stakeholders (customers vs. employees), the cause of the breach, and apology intensity do not change the effects of the three recoveries. Moreover, we show that compensation and process improvement have an equal effect size on firm-idiosyncratic risk. It should be noted that this equality is different from what is found in behavioral meta-analyses that typically indicate a difference between these two strategies (e.g., Cohen-Charash and Spector 2001; Gelbrich and Roschk 2010a). In a customer context, Gelbrich and Roschk (2010a) discovered that compensation is the most influential of the three strategies. Finally, our durational persistence analyses show that the impact of service crisis recoveries on firm-idiosyncratic risk starts after two calendar quarters and persists for two years after their announcement. Overall, the three effects reported are important, robust and durable.

Theoretical implications

We highlight here five key contributions. Our first contribution is to the literature on service crisis and its recovery strategies (see Table 1). Prior studies have focused essentially on individual failures and private recoveries. In addition, the literature on product-harm crisis emphasizes product recall, which is not applicable for service crises. Building on these literatures, our study expands the concept of recovery to a service crisis context in which recoveries are publicly offered to stakeholders. Importantly, investors witness these recoveries and make their own judgments about a crisis—which in turn affects financial performance.

Second, research on service recovery (e.g., Smith et al. 1999; Gelbrich and Roschk 2010a) and product-harm crisis (e.g., Cleeren et al. 2013; Dawar and Pillutla 2000) has given limited attention to firm-level financial consequences. With the exception of ten Brinke and Adams (2015), who investigated the impact of offering an apology on a firm's abnormal stock return, we are not aware of any research that investigates changes in firms' financial

performance as a result of offering *multiple* recoveries. Briefly, ten Brinke and Adams (2015) examined the impact of normative (with sadness) versus deviant (with happiness) facial emotions during verbal apology on firms' abnormal stock returns. They reported negative effects for deviant facial emotions. Our research adds key insights to this literature by showing the long-term impact of *multiple* service crisis recoveries on firms' financial performance. In addition, we used a solid metric (i.e., firm-idiosyncratic risk) as the key criterion to measure this impact.

Third, we find that the role of apology is negative for investors after a service crisis. This result is in sharp contrast to most behavioral studies that report a positive effect for apology after private service failures (i.e., Gelbrich and Roschk 2010a). Here, we suggest that an apology is generally positive for regular stakeholders (i.e., employees and customers), whereas it is perceived negatively by investors facing service crises. This counterintuitive result has been discussed in the literature on crisis management and law, that is, in contexts in which the risk of litigation is important (e.g., Patel and Reinsch 2003; Tyler 1997). Investors fear that an apology could be interpreted as an admission of guilt, which in turn could boost the risk of litigation against a firm. In a service crisis context, apologies are made through formal communications; it may be difficult to emphasize empathy through these media. Although some research has predicted this negative effect, the current research takes the extra step by showing the concrete negative effect of apology on a firm's *financial performance*.

Fourth, our findings show that investors, compared to employees and customers, process the three recovery efforts in different manners. As just noted, behavioral studies have found that offering apologies showed a firm's empathy for its stakeholders. However, since investors are loss averse (Barberis & Huang, 2001), they respond negatively to an apology in order to avoid future losses. Considering the relative strength of compensation and process improvement in

behavioral studies, the value of compensation is more direct for victimized stakeholders. Therefore, the effect of compensation is stronger on stakeholders' satisfaction compared to process improvement (Gelbrich & Roschk, 2010a). However, for investors who possess a long-term perspective, we argue that these individuals perceive that both kinds of recoveries can equally strengthen the relationships between firms and stakeholders. Finally, our analyses show that investors do not take into consideration the type of failure when they evaluate the effectiveness of recoveries. For regular stakeholders, there is evidence that this attribute strongly matters to them (Smith et al., 1999; Weun et al., 2004).

Finally, this study contributes to the marketing-finance literature (e.g., Luo and Bhattacharya 2009; Rego et al. 2009). This research introduces service crisis recoveries as strategic firm decisions that contribute to the resource-based potential of firms, and it provides support for the association between valuable resources and firms' cash flow stability (e.g., (Josephson et al. 2016; Ngobo et al. 2012; Tuli and Bharadwaj 2009).

Managerial implications

Our results indicate that managers should emphasize both compensation and process improvement after a service crisis. The effectiveness of these plans has been supported from an individual standpoint in behavioral studies (Gelbrich & Roschk, 2010a), and it receives support from a market perspective in the current study. For information breaches, recoveries that signal compensation include offering free credit monitoring, identity theft insurance and discount on post purchases. In turn, plans that express process improvements consist of improving information protection policies, updating security software and training employees. The nonsignificant effect of most interactions suggests that these plans could be offered for both types of stakeholders and for all causes of information breaches with different degrees of

severity. In addition, managers could simultaneously use these two recovery measures; their respective effects are additive (although they do not interact).

The negative effect of an apology suggests that managers should pay special attention to the way they communicate about a service crisis. Here, they face a dilemma. On the one hand, victimized stakeholders prefer receiving an apology as a form of psychological compensation; strong cumulative evidence shows that they respond favorably to an apology. On the other hand, shareholders would prefer a denial of responsibility (i.e., no apology) to diminish the risk of litigation. Thus, firms are "trapped" between being honest with their stakeholders or distorting the reality for shareholders (Tyler, 1997). To resolve this dilemma, we suggest that firms should communicate in different manners, using different media, to their stakeholders and shareholders.

For victimized stakeholders, managers should try to contact them privately, ideally using phone or face-to-face conversations. Well-trained employees should be responsible for initiating these contacts. At this stage, it is important to communicate a warm apology that would convey sincerity and empathy. The employees should also be available to answer any questions, and they should explain the next steps of the recovery. As much as possible, these employees should use the approach that is typically followed for private service failures. The general idea is to treat stakeholders with a personal touch, despite the public nature of a service crisis, so that their relationship can be restored. The strong evidence cumulated by behavioral research suggests that such personal approach could elicit stakeholders' positive responses and be beneficial for firms.

Our prescription is different for investors and most public communications made in the mass media. Here, we suggest that managers should use a form of *equivocal communication*, namely, an ambiguous, tangential and evasive communication style (Bavelas, Black, Chovil, & Mullett, 1990). In this communication strategy, firms put the blame on uncontrollable accidents

such as technical errors (e.g., computer glitch, outdated firewalls and website programing errors), accidental human mistakes or employees' negligence. In this way, the firm does not deny the responsibility completely, but neither does it completely accept it. In this case, the communications are probably too ambiguous to be used as triggering factors leading to an expensive class action. When a large number of individuals are affected by a service crisis, there is a greater risk of class-action lawsuits, and firms should be especially careful in their communications. This context is probably ideal for the use of equivocal communications in the mass media.

Limitations and further research

The following limitations should be considered when interpreting or applying our findings. These limitations also provide interesting research avenues. First, similar to datasets in other articles in the marketing-finance interface, our dataset is limited to U.S. publicly-traded firms, because data on stock returns for foreigner firms are not easily obtainable. Hence, the generalizability of our research is limited to an American context. Future research could replicate our results in other countries to investigate cross-cultural judgment of investors.

Second, this methodology does not provide a detailed mechanism to explain how investors react to firms' strategies. Therefore, behavioral studies should also be conducted to better understand the process that would explain the different effects of the three recoveries, especially apology, for investors.

Third, we did not address in the current study the optimum level of compensation that managers should offer to their customers or employees (Gelbrich et al., 2015). Overcompensation happens when firms provide compensation that goes beyond the value of the initial loss. Behavioral studies show that overcompensation does not necessarily lead to more

satisfaction (Gelbrich and Roschk 2010b). Moreover, marketing-finance articles provide evidence that investments simultaneously made in different areas (such as R&D and advertising) result in negative financial consequences. With these kinds of investments, managers erode firms' financial resources and cash flow stability (Luo and Bhattacharya 2009). Applying this logic to our context, offering extra recoveries could have a similar effect on firm performance.

Fourth, due to limited diversity in the recovery plans in our context, we coded each of the recovery plans at the two levels of either present or absent. Further studies could extend our findings by examining how varying degrees of recovery plans can change firm performance (Tax et al., 1998). For instance, firms might offer either equal compensation to all individuals or varied levels of compensations based on the amount of their loss. Similarly, process improvement can be offered either as broad promises or with more details in terms of activities and schedules.

Fifth, this study focuses on the announcements of information breaches as service crises; however, similar research questions could be examined in other crisis contexts, such as environmental damage. Finally, some moderators could not be examined in our analyses because of constraints in collecting data: firms' reputation in complaint handling, stakeholders' switching barriers, or crisis history (Coombs, 2007; Hess Jr, 2008).

References

Ahluwalia, R., Burnkrant, R. E., & Unnava, H. R. (2000). Consumer response to negative publicity: The moderating role of commitment. *Journal of marketing research*, *37*(2), 203 214.

Andrews, D. F., & Pregibon, D. (1978). Finding the outliers that matter. *Journal of the Royal Statistical Society. Series B (Methodological)*, *40*(1), 85 93.

Ball, K. S. (2001). The use of human resource information systems: a survey. *Personnel review*, *30*(6), 677 693.

Bansal, P., & Clelland, I. (2004). Talking trash: Legitimacy, impression management, and unsystematic risk in the context of the natural environment. *Academy of Management Journal*, *47*(1), 93 103.

Barberis, N., & Huang, M. (2001). Mental accounting, loss aversion, and individual stock returns. *Journal of Finance*, *56*(4), 1247 1292.

Barney, J. (1991). Firm Resources and Sustained Competitive Advantage. *Journal of Management*, *17*(1), 99 120.

Batt, R. (2002). Managing customer services: Human resource practices, quit rates, and sales growth. *Academy of management Journal*, *45*(3), 587 597.

Bavelas, J. B., Black, A., Chovil, N., & Mullett, J. (1990). *Equivocal communication.* Sage Publications, Inc.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, *35*(4), 1017–1042.

Ben-Zion, U., & Shalit, S. S. (1975). Size, Leverage, and Dividend Record as Determinants of Equity Risk. *Journal of Finance*, *30*(4), 1015 1026.

Berry, L. L. (1981). The employee as customer. *Journal of retail banking*, *3*(1), 33 40.

Bharadwaj, S. G., Tuli, K. R., & Bonfrer, A. (2011). The impact of brand quality on shareholder wealth. *Journal of Marketing*, *75*(5), 88 104.

Blodgett, J. G., Hill, D. J., & Tax, S. S. (1997). The effects of distributive, procedural, and interactional justice on postcomplaint behavior. *Journal of Retailing*, *73*(2), 185 210.

Boshoff, C. (1997). An experimental study of service recovery options. *International Journal of Service Industry Management*, *8*(2), 110 130.

Brandt, M. W., Brav, A., Graham, J. R., & Kumar, A. (2010). The idiosyncratic volatility puzzle: Time trend or speculative episodes? *Review of Financial Studies*, *23*(2), 863 899.

Brown, G., & Kapadia, N. (2007). Firm-specific risk and equity market development. *Journal of Financial Economics*, *84*(2), 358 388.

Campbell, J., Hilscher, J., & Szilagyi, J. (2008). In Search of Distress Risk. *Journal of Finance*, *63*(6), 2899 2939.

Campbell, J. Y., Lettau, M., Malkiel, B. G., & Xu, Y. (2001). Have Individual Stocks Become More Volatile? An Empirical Exploration of Idiosyncratic Risk. *Journal of Finance*, *56*(1), 1 43.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431 448.

Carroll, A. B. (1991). The pyramid of corporate social responsibility: Toward the moral management of organizational stakeholders. *Business horizons*, *34*(4), 39 48.

Chen, Y., Ganesan, S., & Liu, Y. (2009). Does a firm's product-recall strategy affect its financial value? An examination of strategic alternatives during product-harm crises. *Journal of Marketing*, *73*(6), 214 226.

Chuang, C.-H., & Liao, H. U. I. (2010). Strategic human resource management in service context: Taking care of business by taking care of employees and customers. *Personnel Psychology*, *63*(1), 153 196.

Cleeren, K., Dekimpe, M. G., & Helsen, K. (2008). Weathering product-harm crises. *Journal of the Academy of Marketing Science*, *36*(2), 262 270.

Cleeren, K., Van Heerde, H. J., & Dekimpe, M. G. (2013). Rising from the ashes: How brands and categories can overcome product-harm crises. *Journal of Marketing*, *77*(2), 58 77.

Cohen, J. R. (1999). Advising clients to apologize. *Southern California Law Review*, *72*, 1009 1070.

Cohen, J. R. (2000). Apology and organizations: exploring an example from medical practice. *Fordham Urban Law Journal*, *27*(5), 1447 1482.

Cohen-Charash, Y., & Spector, P. E. (2001). The Role of Justice in Organizations: A Meta-Analysis. *Organizational Behavior and Human Decision Processes*, *86*(2), 278 321.

Coombs, W. T. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. *Corporate reputation review*, *10*(3), 163 176.

Core, J. E., Holthausen, R. W., & Larcker, D. F. (1999). Corporate governance, chief executive officer compensation, and firm performance1. *Journal of Financial Economics*, *51*(3), 371 406.

Culnan, M. J., & Williams, C. C. (2009). How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches. *MIS Quarterly*, *33*(4), 673 687.

Daileyl, R. C., & Kirk, D. J. (1992). Distributive and procedural justice as antecedents of job dissatisfaction and intent to turnover. *Human Relations*, *45*(3), 305 317.

Darrow, B. (2015, septembre 20). Amazon Web Services cloud hit by database problems - Fortune. Consulté 2 février 2016, à l'adresse http://fortune.com/2015/09/20/amazon-cloud-snafu/

Davidow, M. (2000). The Bottom Line Impact of Organizational Responses to Customer Complaints. *Journal of Hospitality & Tourism Research*, *24*(4), 473 490.

Davidow, M. (2003). Organizational Responses to Customer Complaints: What Works and What Doesn't. *Journal of Service Research*, *5*(3), 225 250.

Dawar, N., & Pillutla, M. M. (2000). Impact of product-harm crises on brand equity: The moderating role of consumer expectations. *Journal of Marketing Research*, *37*(2), 215 226.

Dechow, P. M. (1994). Accounting earnings and cash flows as measures of firm performance: The role of accounting accruals. *Journal of accounting and economics*, *18*(1), 3 42.

Dewan, S., & Ren, F. (2007). Risk and Return of Information Technology Initiatives: Evidence from Electronic Commerce Announcements. *Information Systems Research*, *18*(4), 370 394.

Durnev, A., Morck, R., Yeung, B., & Zarowin, P. (2003). Does greater firm specific return variation mean more or less informed stock pricing? *Journal of Accounting Research*, *41*(5), 797 836.

Edmans, A. (2011). Does the stock market fully value intangibles? Employee satisfaction and equity prices. *Journal of Financial Economics*, *101*(3), 621 640.

Fama, E. F. (1998). Market efficiency, long-term returns, and behavioral finance1. *Journal of Financial Economics*, *49*(3), 283 306.

Fang, Z., Luo, X., & Jiang, M. (2013). Quantifying the Dynamic Effects of Service Recovery on Customer Satisfaction Evidence From Chinese Mobile Phone Markets. *Journal of Service Research*, *16*(3), 341 355.

Ferreira, M. A., & Laux, P. A. (2007). Corporate Governance, Idiosyncratic Risk, and Information Flow. *Journal of Finance*, *62*(2), 951 989.

Folkes, V. S. (1984). Consumer reactions to product failure: An attributional approach. *Journal of consumer research*, *10*(4), 398 409.

Folkes, V. S. (1988). Recent attribution research in consumer behavior: A review and new directions. *Journal of Consumer Research*, *14*(4), 548 565.

Fuchs-Burnett, T. (2002). Mass public corporate apology. *Dispute Resolution Journal*, *57*(2), 26.

Gelbrich, K., Gäthke, J., & Grégoire, Y. (2015). How much compensation should a firm offer for a flawed service? An examination of the nonlinear effects of compensation on satisfaction. *Journal of Service Research*, *18*(1), 107 123.

Gelbrich, K., Gäthke, J., & Grégoire, Y. (2016). How a firm's best versus normal customers react to compensation after a service failure. *Journal of Business Research*.

Gelbrich, K., & Roschk, H. (2010a). A Meta-Analysis of Organizational Complaint Handling and Customer Responses. *Journal of Service Research*, 1 20.

Gelbrich, K., & Roschk, H. (2010b). Do complainants appreciate overcompensation? A meta-analysis on the effect of simple compensation vs. overcompensation on post-complaint satisfaction. *Marketing Letters*, *22*(1), 31 47.

Gijsenberg, M. J., Van Heerde, H. J., & Verhoef, P. C. (2015). Losses loom longer than gains: Modeling the impact of service crises on perceived service quality over time. *Journal of Marketing Research*, *52*(5), 642 656.

Goyal, A., Santa-clara, P., Subrahmanyam, A., Torous, W., Valkanov, R., Campbell, E. J., & Roll, R. (2003). Idiosyncratic risk matters. *Journal of Finance*, *58*(3), 975–1007.

Grégoire, Y., & Fisher, R. J. (2008). Customer betrayal and retaliation: when your best customers become your worst enemies. Journal of the Academy of Marketing Science, 36(2), 247–261.

Hansen, M. H., & Hurwitz, W. N. (1943). On the theory of sampling from finite populations. *The Annals of Mathematical Statistics*, *14*(4), 333 362.

Henry, G. T. (1990). *Practical sampling* (Vol. 21). California: Sage.

Hess Jr, R. L. (2008). The impact of firm reputation and failure severity on customers' responses to service failures. *Journal of Services Marketing*, *22*(5), 385 398.

Hou, K., & Robinson, D. T. (2006). Industry Concentration and Average Stock Returns. *Journal of Finance*, *61*(4), 1927 1956.

Huber, P. J. (1973). Robust regression: asymptotics, conjectures and Monte Carlo. *The Annals of Statistics*, *1*, 799 821.

Johnston, R., & Fern, A. (1999). Service Recovery Strategies for Single and Double Deviation Scenarios. *Service Industries Journal*, *19*(2), 69 82.

Johnston, R., & Michel, S. (2008). Three outcomes of service recovery: customer recovery, process recovery and employee recovery. *International Journal of Operations & Production Management*, *28*(1), 79 99.

Josephson, B. W., Johnson, J. L., Mariadoss, B. J., & Cullen, J. (2016). Service Transition Strategies in Manufacturing Implications for Firm Risk. Journal of Service Research, 19(2), 142–157.

Kamruzzaman, M. D., & Imon, A. (2002). High leverage point: another source of multicollinearity. *PAKISTAN JOURNAL OF STATISTICS-ALL SERIES-*, *18*(3), 435 448.

Kassarjian, H. H. (1977). Content analysis in consumer research. *Journal of consumer research*, *4*(1), 8 18.

Kawamoto, D. (2007, mars 30). TJX says 45.7 million customer records were compromised. Consulté 2 février 2016, à l'adresse http://www.cnet.com/news/tjx-says-45-7-million-customer-records-were-compromised/

Keown-McMullan, C. (1997). Crisis: When Does a Molehill Become a Mountain? *Disaster Prevention and Management*, *6*(1), 4 10.

Klein, J., & Dawar, N. (2004). Corporate social responsibility and consumers' attributions and brand evaluations in a product–harm crisis. *International Journal of research in Marketing*, *21*(3), 203 217.

Kozlenkova, I. V., Samaha, S. A., & Palmatier, R. W. (2014). Resource-based theory in marketing. *Journal of the Academy of Marketing Science*, *42*(1), 1 21.

Laufer, D. (2015). Emerging issues in crisis management. *Business Horizons*, *2*(58), 137 139.

Laufer, D., & Coombs, W. T. (2006). How should a company respond to a product harm crisis? The role of corporate reputation and consumer-based cues. *Business Horizons*, *49*(5), 379 385.

Lewis, B. R., & Mitchell, V. W. (1990). Defining and measuring the quality of customer service. *Marketing intelligence & planning*, *8*(6), 11 17.

Liao, H. (2007). Do it right this time: the role of employee service recovery performance in customer-perceived justice and customer loyalty after service failures. *Journal of applied psychology*, *92*(2), 475.

Luo, X., & Bhattacharya, C. B. (2009). The Debate over Doing Good: Corporate Social Performance, Strategic Marketing Levers, and Firm-Idiosyncratic Risk. *Journal of Marketing*, *73*(6), 198 213.

Luo, X., Kanuri, V. K., & Andrews, M. (2014). How does CEO tenure matter? The mediating role of firm employee and firm customer relationships. *Strategic Management Journal*, *35*(4), 492 511.

MacKinlay, A. C. (1997). Event studies in economics and finance. *Journal of economic literature*, *35*(1), 13 39.

Malhotra, A., & Malhotra, C. K. (2011). Evaluating customer information breaches as service failures: an event study approach. *Journal of Service Research*, *14*(1), 1094670510383409.

Maronna, R., Martin, D., & Yohai, V. (2006). *Robust statistics: Theory and Methods*. John Wiley & Sons, Chichester. ISBN.

Martin, K. D., Borah, A., & Palmatier, R. W. (2016). Data privacy: Effects on customer and firm performance. *Journal of Marketing*.

Martin, K. D., & Murphy, P. E. (2016). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 1–21.

Maxham III, J. G., & Netemeyer, R. G. (2002). Modeling customer perceptions of complaint handling over time: the effects of perceived justice on satisfaction and intent. *Journal of Retailing*, *78*(4), 239–252.

Maxwell, S. E. (2000). Sample size and multiple regression analysis. *Psychological methods*, *5*(4), 434.

McGahan, A. M., & Porter, M. E. (1997). How much does industry matter, really? *Strategic Management Journal*, *18*(1), 15–30.

McWilliams, A., & Siegel, D. (1997). Event studies in management research: Theoretical and empirical issues. *Academy of Management Journal*, *40*(3), 626–657.

Miller, J. L., Craighead, C. W., & Karwan, K. R. (2000). Service recovery: a framework and empirical investigation. *Journal of operations Management*, *18*(4), 387–400.

Ngobo, P.-V., Casta, J.-F., & Ramond, O. (2012). Is customer satisfaction a relevant metric for financial analysts? *Journal of the Academy of Marketing Science*, *40*(3), 480–508.

O'brien, R. M. (2007). A Caution Regarding Rules of Thumb for Variance Inflation Factors. *Quality & Quantity*, *41*(5), 673–690.

Orsingher, C., Valentini, S., & de Angelis, M. (2010). A meta-analysis of satisfaction with complaint handling in services. *Journal of the Academy of Marketing Science*, *38*(2), 169–186.

Palmatier, R. W., Dant, R. P., Grewal, D., & Evans, K. R. (2006). Factors influencing the effectiveness of relationship marketing: a meta-analysis. *Journal of marketing*, *70*(4), 136–153.

Patel, A., & Reinsch, L. (2003). Companies Can Apologize: Corporate Apologies and Legal Liability. *Business Communication Quarterly*, *66*(1), 9–25.

Pearson, C. M., & Clair, J. A. (1998). Reframing Crisis Management. *Academy of Management Review*, *23*(1), 59–76.

Perreault, W. D., & Leigh, L. E. (1989). Reliability of nominal data based on qualitative judgments. *Journal of marketing research*, *26*(2), 135.

Rego, L. L., Billett, M. T., & Morgan, N. A. (2009). Consumer-based brand equity and firm risk. *Journal of Marketing*, *73*(6), 47–60.

Robbennolt, J. K. (2003). Apologies and legal settlement: An empirical examination. *Michigan Law Review*, *102*(3), 460–516.

Roschk, H., & Kaiser, S. (2013). The nature of an apology: An experimental study on how to apologize after a service failure. *Marketing Letters*, *24*(3), 293–309.

Rousseeuw, P. J., & Driessen, K. V. (1999). A fast algorithm for the minimum covariance determinant estimator. *Technometrics*, *41*(3), 212–223.

Rousseeuw, P. J., & Leroy, A. M. (1987). Related Statistical Techniques. In *Robust Regression and Outlier Detection* (p. 248–291). John Wiley & Sons, Inc.

Rushton, A. M., & Carson, D. J. (1985). The marketing of services: managing the intangibles. *European journal of marketing*, *19*(3), 19–40.

Rust, R. T., Ambler, T., Carpenter, G. S., Kumar, V., & Srivastava, R. K. (2004). Measuring marketing productivity: Current knowledge and future directions. *Journal of marketing*, *68*(4), 76–89.

Saad Andaleeb, S., & Conway, C. (2006). Customer satisfaction in the restaurant industry: an examination of the transaction-specific model. *Journal of Services Marketing*, *20*(1), 3–11.

Schenker, N., & Gentleman, J. F. (2001). On Judging the Significance of Differences by Examining the Overlap Between Confidence Intervals. *The American Statistician*, *55*(3), 182–186.

Shrivastava, P., Mitroff, I. I., Miller, D., & Miclani, A. (1988). Understanding Industrial Crises[1]. *Journal of Management Studies*, *25*(4), 285–303.

Smith, A. K., Bolton, R. N., & Wagner, J. (1999). A Model of Customer Satisfaction with Service Encounters Involving Failure and Recovery. *Journal of Marketing Research*, *36*(3), 356–372.

Srinivasan, S., & Hanssens, D. M. (2009). Marketing and Firm Value: Metrics, Methods, Findings, and Future Directions. Journal of Marketing Research, 46(3), 293–312.

Srivastava, R. K., Fahey, L., & Christensen, H. K. (2001). The resource-based view and marketing: The role of market-based assets in gaining competitive advantage. *Journal of Management*, *27*(6), 777–802.

Srivastava, R. K., Shervani, T. A., & Fahey, L. (1998). Market-based assets and shareholder value: A framework for analysis. *The Journal of Marketing*, *62*(1), 2–18.

Statistics | DataLossDB. (2016, janvier 2). Consulté 25 janvier 2016, à l'adresse http://datalossdb.org/statistics

Tax, S. S., Brown, S. W., & Chandrashekaran, M. (1998). Customer evaluations of service complaint experiences: implications for relationship marketing. *The journal of marketing*, 60–76.

ten Brinke, L., & Adams, G. S. (2015). Saving face? When emotion displays during public apologies mitigate damage to organizational performance. *Organizational Behavior and Human Decision Processes*, *130*, 1–12.

Traynor, R. J. (1964). Ways and Meanings of Defective Products and Strict Liability, The. *Tennessee Law Review*, *32*(3), 363–376.

Tsui, A. S., Pearce, J. L., Porter, L. W., & Tripoli, A. M. (1997). Alternative approaches to the employee-organization relationship: does investment in employees pay off? *Academy of Management journal*, *40*(5), 1089–1121.

Tuli, K. R., & Bharadwaj, S. G. (2009). Customer Satisfaction and Stock Returns Risk. *Journal of Marketing*, *73*(6), 184–197.

Tyler, L. (1997). Liability Means Never being Able to Say You're Sorry Corporate Guilt, Legal Constraints, and Defensiveness in Corporate Communication. *Management Communication Quarterly*, *11*(1), 51–73.

Van Vaerenbergh, Y., Larivière, B., & Vermeir, I. (2012). The impact of process recovery communication on customer satisfaction, repurchase intentions, and word-of-mouth intentions. *Journal of Service Research*, *15*(3), 262–279.

Van Vaerenbergh, Y., Orsingher, C., Vermeir, I., & Larivière, B. (2014). A meta-analysis of relationships linking service failure attributions to customer outcomes. *Journal of Service Research*, 1–18.

VanVoorhis, C. R. W., & Morgan, B. L. (2007). Understanding power and rules of thumb for determining sample sizes. *Tutorials in Quantitative Methods for Psychology*, *3*(2), 43 50.

Vassilikopoulou, A., Siomkos, G., Chatzipanagiotou, K., & Pantouvakis, A. (2009). Product-harm crisis management: Time heals all wounds? *Journal of Retailing and Consumer Services*, *16*(3), 174 180.

Wernerfelt, B. (1984). A resource-based view of the firm. *Strategic management journal*, *5*(2), 171–180.

Weun, S., Beatty, S. E., & Jones, M. A. (2004). The impact of service failure severity on service recovery evaluations and post recovery relationships. *Journal of Services Marketing*, *18*(2), 133 146.

Wilson, A., Zeithaml, V. A., Bitner, M. J., & Gremler, D. D. (2012). *Services marketing: Integrating customer focus across the firm*. McGraw Hill.

Winer, R. S. (2001). A framework for customer relationship management. *California management review*, *43*(4), 89 105.

Wirtz, J., & Mattila, A. S. (2004). Consumer responses to compensation, speed of recovery and apology after a service failure. *International Journal of service industry management*, *15*(2), 150 166.

Yang, Z., & Fang, X. (2004). Online service quality dimensions and their relationships with satisfaction: A content analysis of customer reviews of securities brokerage services. *International Journal of Service Industry Management*, *15*(3), 302 326.

Zeithaml, V. A., Parasuraman, A., & Malhotra, A. (2002). Service quality delivery through web sites: a critical review of extant knowledge. *Journal of the academy of marketing science*, *30*(4), 362 375.

Conclusion

This dissertation addresses two of the most important questions of firms regarding the event of information breach: What are the market level costs of information breach events? What are effective recovery actions after the event of information breach? While these examinations extend our knowledge on the domain of information privacy and service crisis recovery, a number of questions still remain unanswered and deserve the attention of future researchers. In the following, we categorize notable research gaps.

From a theoretical aspect, the literature on information privacy and information breaches suffers from an absence of well-agreed definitions regarding these constructs. As a result, researches are inconsistent in terms of conceptualization and operationalization, and findings and theoretical frameworks depend upon particular and limited contexts. Relatedly, this confusion is also reflected in the absence of a rigorous typology of types or causes of privacy concerns or privacy breaches, which obstructs future research. These shortcomings stem from the multidisciplinary nature of privacy because it is linked to ethics, sociology, culture, law, technology and psychology, as well as from its multilevel necessity of analysis that can involve individuals, societies, governments and organizations concurrently. In addition, the nature of information privacy continues to evolve as new technologies and new initiatives are adopted by firms to collect and use the personal information of stakeholders. Given these issues, grounded theory, ethnographic studies and interdisciplinary research projects are called for that will synthesize these different dimensions to determine the boundaries around this construct.

From a methodological perspective, literature reviews reveal that the majority of prior studies have employed primary data (e.g., surveys and experiments) as their central source of investigation (e.g., Bélanger and Crossler 2011; Smith, Dinev, and Xu 2011). One weakness with

these studies is that, since they rely on perceptual measures, they fail to provide sufficient insights on the impacts of actual events of information breach or real privacy concerns to decision makers. Therefore, there is an essential need for methodologies that are built upon practical and realistic foundations. Secondary databases could be rich sources of data for this purpose. Also, conducting case studies in communities or organizations that have been victims of these problems can considerably alleviate these weaknesses.

In terms of the level of analysis, organizational and societal levels do not appear in a large number of studies in comparison to the individual level—because of challenges in data collection. Indeed, at the organizational level, most of the studies have focused on the effectiveness of different information protection tools; however, more studies are required to gain a deeper understanding of the concerns of organizations about the privacy of their own and their stakeholders' information and the potential outcomes of these concerns. More specifically, companies possess certain concerns about the privacy of their own information, such as information about their organizational processes or future projects, which impel them to implement proactive standards to safeguard this information, such as not allowing their employees to take photos inside the organization or to discuss their work in public places. However, our knowledge on the effectiveness of these policies is insufficient. Moreover, depending on their cultures and mindsets, organizations have different degrees of attitudes and concerns about the privacy of their stakeholders' information that result in different levels of information protection policies. But the impact of these policies on stakeholders' responses is not clear enough. As a consequence, firms might be interested to learn about effective and optimum solutions of information practices to secure their own and their stakeholders' information. Additionally, researchers' efforts to explore the ultimate outcomes of these practices on firms'

strategic positions in terms of brand equity, sales, profits, partner relationships, and distribution channels can advance managerial insights significantly.

At the societal level, the role of culture and norms in shaping the privacy concerns of individuals across countries and societies needs more investigations. This research stream can shed light on the border between normative and non-normative antecedents of privacy concerns and can better illustrate the costs and benefits to individuals of disclosing information to organizations across cultures. In addition, it can help organizations and governments optimize their privacy regulations in line with relevant societal norms.

Apart from the concept of information privacy and breaches, this dissertation also outlines the concept of service crisis as a new construct in the literature on service. Because of the severity and prevalence of service crises, this concept can be the center of attention of managers and researchers in the future. To inspire future research in this area, we suggest four research avenues classified by the characteristics, antecedents, outcomes, and recoveries of service crises.

Awareness of the characteristics and antecedents of service crises not only can regulate boundaries of this construct, but also can suggest means to operationalize its damage scale. Moreover, knowledge on these antecedents can help managers to establish principles to prevent service crises from happening. Like other types of crises, a service crisis can derive from several factors, including human factors (e.g., operator mistakes, managerial mistakes, and purposive acts), organizational factors (e.g., ineffective procedures and inadequate resource allocations), technological systemic factors (e.g., technical error, faulty design, and defective equipment) and environmental factors (e.g., floods, earthquakes, and tornadoes) (Coombs, 2006; Shrivastava et al., 1988). In terms of characteristics, impacts of a service crisis might be localized to specific

geographic regions, such as when a company compromises the private information of a group of stakeholders living in a specific area, while sometimes these impacts might transcend geographic boundaries, as when a telecommunications company is subject to a technical error and cannot deliver appropriate services to its geographically dispersed customers. Also, threats of a service crisis might remain for a long time, such as the event of information breached, or perish in a short time, such as the case of an Internet service interruption. As a result of these different characteristics and antecedents, the occurrence of each category of service crises might be associated with different degrees of tangible and intangible losses for firms and impacts for stakeholders and the society. Future research can extend these dimensions to suggest relevant typologies of service crises and to develop valid measures to evaluate the damage scale of different categories of service crisis.

Advancing knowledge on the strategic outcomes of these crises is also worthwhile for academicians and practitioners. Besides routine outcomes that are examined in typical research studies, such as firms' financial performance or brand equity, one invaluable and relevant outcome that can significantly contribute to both theory and practice would be the reaction of the whole society to a crisis. More clearly, prior studies have concentrated primarily on the reaction of affected or directly involved stakeholders (e.g., the organization, partners, customers, and employees) to a potential or actual negative event. However, under the umbrella of *deontic justice*, it is expected that other stakeholders in the society who are not directly affected by a crisis will show reactions to it. Deontic justice argues that human beings might show reactions to injustice not because of personal benefits or rewards, but because they perceive a moral duty to uphold justice in their society (Cropanzano, Goldman, & Folger, 2003; Cropanzano, Massaro, & Becker, 2016). One facet of deontic justice claims that individuals will punish an unjust entity,

even when the victim is a stranger. Cropanzano, Goldman, and Folger (2003) provide evidence that people are often motivated to evaluate a harmful event on the basis of certain normative criteria or rules of justice. When a transgressor's behavior toward others violates these rules, the observer or witness believes that the victim has been treated unfairly and, as a result, punishes the transgressor.

Integrating these arguments with the unjust nature of a service crisis which indicates service providers' unfair input (Hess, Ganesan, & Klein, 2003), we put forth the view that unaffected stakeholders in a society might also demonstrate negative reactions to a service crisis to restore justice; and these reactions can be extremely costly for the firm. One instance of such reactions is calls for boycotts, such as launching the Boycott against *Game of Thrones* over graphic sexual violence (Chretien & Jalsevac, 2016) or against Facebook over depicting violence against women, which convinced many organizations to pull their ads from Facebook (Kerr, 2013). These reactions from the society or unaffected stakeholders might have alternative forms, such as generating negative word of mouth and loss intention to purchase, which devalue the performance of the firm in the long term.

Theoretically, the motivation of observers to punish the firm might depend on justice or the moral rules of observers, the amount of observers' empathy for victims, the extent to which rules of justice are applied in a society, and the type of injustice that the crisis indicates (distributive, procedural or international). These controversial debates are still unresolved and deserve the attention of future researchers. In addition, exploring the form of punishment offered by observers, its antecedents and outcomes can make substantial contributions.

Recovery actions from service crises, which is at the heart of the discussion in the second chapter of this dissertation, are not limited to compensations, process improvements or

apologies. Service crisis recovery can encompass a larger set of responses, including improving public relations (e.g., investing in research to prevent similar events in the society or donating to NGOs that are active in that area) or empathetic explanations from the manager or spokesperson about the cause of the crisis. While, these recoveries are not common in practice, suggesting and examining consequences of alternative recovery actions can extend the choices of managers when it comes to alleviating costs of crises.

For government policy-makers, these studies and investigations can form the foundation of an organization similar to the United States Consumer Product Safety Commission (CPSC) for service crises. The United States Consumer Product Safety Commission (CPSC)—an independent agency of the Unites States government—is in charge of developing uniform product safety standards and protecting the public from unreasonable risk of injury or death associated with defective products, such as household, outdoor, and sports products. In cases of potential product-harms that happen in the U.S., this organization is responsible for evaluating the product hazard; and if necessary, it has the authority to invite the responsible firm to engage in a product recall or to impose one upon it. In either case, the CPSC initiates an official recall announcement in a standard format jointly with the firm and collaborates with the firm to locate and remove all defective products from consumers and channel members and to give the public accurate information about the product defect, the extent of the hazard, and the firm's corrective plan in a timely manner (Chen, Ganesan, & Liu, 2009). Similar organizations and procedures, in cases of service crises, can regulate the market competition and assure stakeholders' rights.

Appendices

Appendix 1 Coding definitions and examples of three strategies of service crisis recovery

Service crisis recovery	Definition for coders	Examples
Compensation	Offering any tangible redress to restore the loss of victimized groups	"We provide affected individuals with a credit monitoring service for one year, at our expense." "We are offering up to two years of credit protection services for individuals affected by the breach." "Affected individuals will receive discount and promotion on their next purchase."
Process improvement	Any promise or indication to improve or develop the organizational processes that led to the information breach	"We try to improve our systems and procedures to prevent the future events." "We take steps to ensure these incidents will not happen again." "Anyone handling sensitive information must take training in our company." "We are taking steps to prevent this issue from reoccurring, including providing additional training to employees regarding the proper handling of confidential information." "Adjustments had already been made to prevent it from occurring again."
Apology	Presence of terms "apology," "regret," "sorry" or their synonyms in a firm's communications	"We sincerely apologize for any concern of inconvenience this matter may cause you." "We deeply regret that this incident occurred." "We deeply regret and apologize for this incident and the associated inconvenience to our customers/employees." "We are very sorry this happened." "Please accept our deepest apologies."

Appendix 2

Example of a case of information breach with coding service crisis recoveries

To illustrate how we coded the strategies of service crisis recoveries, we present in this appendix the public announcements of a case of information breach that happened to Ruby Tuesday Inc. (an American multinational foodservice retailer) in 2013. This firm offered all three recovery strategies to victimized stakeholders in response to an information breach. In these announcements, we underlined and italicized the statements that were indicators of different recovery strategies. It is noteworthy to mention that one news announcement does not cover all relevant details about the event and recovery strategies. Hence, we collected relevant news (as much as we could find) to ensure that we had not missed any detail.

Full text of the Eyewitness News, July 10, 2013
By: Susan Raff
Ruby Tuesday restaurant investigates possible security breach

NEW BRITAIN, CT (WFSB) - A popular chain restaurant could have a security breach problem on its hands.

A New Britain man received an email Wednesday from Ruby Tuesday that included names, bank accounts and Social Security numbers of more than 100 new employees.

The man, who is only identified as Justin, and two other people received the email from Ruby Tuesday's. The other two people have "Ruby Tuesday" email addresses; however, Justin does not.

The email was sent to his personal Gmail account. Justin told Eyewitness News that at one point he did work as a server at a Ruby Tuesday in West Hartford, but left in February.

According to Justin, the email included an attachment containing information that appeared to be from the company's payroll.

Justin emailed the company to inform them of the email he acquired. On Wednesday afternoon, the company emailed him back saying, "This information was erroneously sent to you. Please confirm that you have not forwarded the email or its attachment to anyone else."

Justin said he has not sent the confidential information to anyone, but told Eyewitness News that he was concerned that such sensitive information ended up somewhere it should not have been.

Eyewitness News reached out to Ruby Tuesday and learned that it was an accident. The company said they "are in the process of contacting all the people … telling them what happened."

They told Eyewitness News that they "don't believe it went any further - we are giving them information-we are offering them assistance."

According to the company, Justin is the only person who should not have received the email. They said if need be they will provide credit monitoring.

Reference: *The Eyewitness News.* (2013, July 10). *Ruby Tuesday restaurant investigates possible security breach.* Retrieved March 1, 2014 from http://www.wfsb.com/story/22807639/ruby-tuesday-restaurant-investigates-possible-security-breach

Full text from *The Knoxville News Sentinel*, Monday, July 15, 2013
By: Carly Harrington
Ruby Tuesday accidentally emails employees' personal info

Dozens of Ruby Tuesday employees' personal information was accidentally sent to a person who used to work for the Maryville-based restaurant chain.

Ruby Tuesday acknowledged that a former employee had been copied on an internal communication last week regarding 78 members of its staff. The company did not specify what information had been disclosed.

"We've launched a full investigation and have notified the team members of the exposure. We've received assurances from the former employee that the communication has been permanently deleted," Ruby Tuesday said in a statement.

A Connecticut media report identified the former employee as a resident of New Britain who had worked as a server for Ruby Tuesday until February. The report said the information sent by email appeared to be from the company's payroll and included names, bank accounts and Social Security numbers.

As a result of the error, Ruby Tuesday said it *has already adjusted its processes "to prevent anything of this nature from occurring again."*

"The safety and security of our team members' personal information is of the utmost importance to us and we are committed to ensuring that it remains protected. *We apologize for any inconvenience this has caused to the team members involved* and we have already contacted them to offer information and any assistance we can," Ruby Tuesday said.

A formal written notice of the exposure will be provided to impacted employees as well as to certain state regulators in accordance with applicable laws, the company said.

Ruby Tuesday is also *extending an offer to the affected team members to activate credit monitoring services for one year at its expense* to ensure the integrity of their personal information.

Reference: *The Knoxville News Sentinel*. (2013, July 15). *Ruby Tuesday accidentally emails employees' personal info*. Retrieved March 1, 2014 from http://www.knoxnews.com/business/ruby-tuesday-accidentally-emails-employees-personal-info-ep-357975691-355663341.html

Full text from *The Daily Times*, Monday, July 15, 2013

By: Robert Norris, bobn@thedailytimes.com
Ruby Tuesday email mistakenly reveals personal data

An email inadvertently sent by Ruby Tuesday Inc. to a former employee contained personal information concerning 78 current employees.

The Maryville-based casual dining chain said the email was accidentally copied on an internal communication and corrective action had been taken.

"We've launched a full investigation and have notified the team members of the exposure. We've received assurances from the former employee that the communication has been permanently deleted," the company said in a statement released Monday.

According to a report by WFSB-TV, of Hartford, Conn., a New Britain, Conn., man identified only as Justin received in his Gmail account an email containing information from the Ruby Tuesday payroll including names, bank accounts and Social Security numbers.

The report said Justin told the TV station that he had worked as a server at a West Hartford Ruby Tuesday until February.

The former employee said he emailed the company about receiving the confidential information and the company replied, "This information was erroneously sent to you. Please confirm that you have not forwarded the email or its attachment to anyone else."

The company said Monday that *it regretted that the error had occurred* and *adjustments had already been made to prevent it from occurring again*.

"The safety and security of our team members' personal information is of the utmost importance to us and we are committed to ensuring that it remains protected. *We apologize for any inconvenience this has caused to the team members involved*, and we have already contacted them to offer information and any assistance we can," the statement said.

"We will be providing formal written notice of the exposure to them soon, and we will be notifying certain state regulators in accordance with applicable laws."

Ruby Tuesday also said the company was *extending an offer for the affected team members to activate credit monitoring services for one year at the company's expense* "to ensure the integrity of their personal information."

Reference: *The Daily Times*. (2013, July 15). *Ruby Tuesday email mistakenly reveals personal data*. Retrieved March 1, 2014 from http://www.thedailytimes.com/business/ruby-tuesday-email-mistakenly-reveals-personal-data/article_ca46c117-7258-54ec-8e05-22c26e81e1e5.html

Full text of the WVLT TV local8now website, Tuesday July 16, 2013
Former Ruby Tuesday server gets emails with workers' information

KNOXVILLE, Tenn. (AP) -- Personal information on Ruby Tuesday employees was accidentally sent to a former company worker.

The Maryville-based company told the Knoxville News Sentinel the former employee has assured Ruby Tuesday officials the email was permanently deleted.

The company acknowledged the former worker's address had been copied on an internal communication last week regarding 78 company staff members.

A news report in Connecticut said the information accidentally went to a New Britain resident who had worked as a server at a Ruby Tuesday restaurant until February. The report said the information included employees' names, bank accounts and Social Security numbers.

The company did not say what information was disclosed, but *is paying for a year of credit monitoring for affected employees.*

Reference: WVLT.TV website. (2013, July 16). *Former Ruby Tuesday server gets email with workers' information*. Retrieved March 1, 2014 from http://www.local8now.com/home/headlines/Former-Ruby-Tuesday-server-gets-email-with-workers-information-215643341.html