Article

The Effects of Service Crises and Recovery Resources on Market Reactions: An Event Study Analysis on Data Breach Announcements

Journal of Service Research
2023, Vol. 26(1) 44–63

DOI: 10.1177/10946705211036944
journals.sagepub.com/home/jsr


Shahin Rasoulian[1], Yany Grégoire[1], Renaud Legoux[1] and Sylvain Sénécal[1]

Abstract

Building on the literatures on service failure and crisis seriousness, we develop a framework to understand the effects of a specific type of service crisis (i.e., data breaches) and organizational recovery resources on the reactions of the stock market. To do so, we conduct an event study analysis with a sample of 217 data breach announcements, as our empirical context. Our analyses reveal that a firm suffers from negative abnormal stock returns when either the outcome of the breach (e.g., the breach of financial data) or its causal process (e.g., hacker attack) indicates a high level of seriousness. Moreover, considering organizational recovery resources, we find that in the case of financial data breaches, age, size, profitability, liquidity, and brand familiarity are the primary resources that can help a firm's recovery. For hacker attacks, these organizational recovery resources include size, profitability, and liquidity.

Keywords

crisis seriousness, data breach, event study, service crisis, service recovery, recovery process

Introduction

The rapid expansion of the information age and growing firms' tendency to invest in data-driven services has increased managers' concerns about data breach incidents (Bélanger and Crossler 2011; Smith, Dinev, and Xu 2011). Data breach is defined as the potential or actual malpractice of unauthorized access to private data of the stakeholders of an organization (Rasoulian et al. 2017). Data breaches have been described as major *service crises* needing managers' attention (Malhotra and Malhotra 2011; Rasoulian et al. 2017). Indeed, such incidents constitute a poor service performance in which firms fail to satisfy the basic requirements about data protection of a large group of customers and employees (Malhotra and Malhotra 2011). In addition, such incidents could receive major media coverage and attract public attention (Rasoulian et al. 2017). According to privacyrights.org, from 2005 to 2018 in North America, over 11 billion records were breached, and the number of firms affected by data breaches increased from 150 to over 640 annually (Data Breaches | Privacy Rights Clearinghouse 2019). Although data breaches are among managers' key concerns—and a large body of research has highlighted the importance of information protection (Culnan and Armstrong 1999; Rifon, LaRose, and Choi 2005; Sheehan and Hoy 2000)—the literature has not yet provided a comprehensive framework to evaluate the market-level effects of different types of breaches and to assess the role of organizational resources in attenuating these effects.

Accordingly, the general purpose of this research is to narrow this gap by proposing a framework that investigates the seriousness of different categories of data breaches and the role of organizational recovery resources. For this framework (Figure 1), we use stock market abnormal returns as the evaluation criterion to measure the effects of data breach seriousness and organizational recovery resources. Figure 1 highlights the two novel aspects of our framework: (1) a distinction between seriousness of outcome versus process for data breaches (and service crises) and (2) the moderation effects of organizational recovery resources. In addition, Table 1 defines our key constructs. Since data breach is a specific type of service crisis (Malhotra and Malhotra 2011; Rasoulian et al. 2017), constructing such a framework can deepen our understanding of the consequences of such crises.

As highlighted in prior research (Gijsenberg, Van Heerde, and Verhoef 2015), the phenomenon of service crisis (i.e., a poor service performance affecting a large number of stakeholders, and obtaining intensive media coverage) has received little attention, especially compared to rich streams on private service failure and product-harm crisis (Rasoulian et al., 2017).

[1]Department of Marketing, HEC Montreal, Montréal, QC, Canada

Corresponding Author:
Shahin Rasoulian, Department of Marketing, HEC Montreal, 3000, Chemin de la Côte-Sainte-Catherine, Montréal, QC H3T 2A7, Canada.
Email: shahin.rasoulian@hec.ca

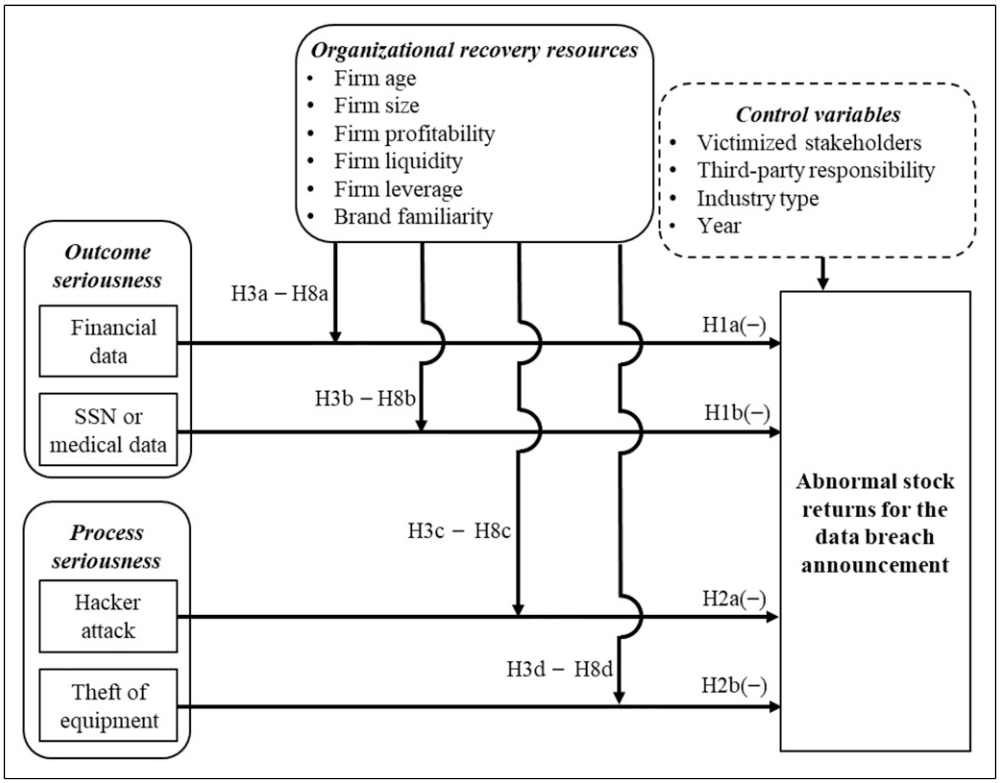

Figure 1. Conceptual framework for the market value loss of data breach announcement.

Table 1. Our Key Concepts and Their Corresponding Definitions.

Concept	Definition
1. Data breach	An event signaling the potential or actual malpractice of unauthorized access to personal data of a group of stakeholders (Culnan and Williams 2009; Rasoulian et al. 2017).
2. Outcome of a data breach	The outcome represents the type of data that are affected by the breach. According to the literature (see Table 2), the type of data refers to financial data, social security number, medical information, or general information.
3. Process leading to a data breach	The process represents the causal procedure at the origin of the data breach. According to the literature (see Table 3), the causal procedures (or processes) can be organized in the following categories: accidental disclosure, hacker attack, improper disposal, insider attack, misplaced data source, or theft of equipment.
4. Seriousness of a data breach	Seriousness is broadly defined as the extent to which the impact or the damages caused by a data breach are important and threaten the functioning of an organization. This research focuses on two types of seriousness: Outcome and process (Carr 2007; Seiders and Berry 1998).
5. Seriousness of outcome (for data breaches)	In our context, the seriousness of an outcome refers to the value of the breached data for firms and stakeholders. This notion refers to the "value of loss" of the crisis assessment literature (Billings, Milburn, and Schaalman 1980; Burnett 1999).
6. Seriousness of process (for data breaches)	In our context, the seriousness of a process refers to the importance of the causal process at the origin of the breach. It is determined on the basis of three criteria identified in the crisis assessment literature (Billings, Milburn, and Schaalman 1980; Burnett 1999): The probability of damage, the time pressure to solve the defective process, and the degree of control of a firm over the defective process.
7. Organizational recovery resources (for data breaches)	A firm's tangible and intangible resources that can be used for the recuperation efforts after a data breach (Esteve-Pérez and Mañez-Castillejo 2008; Grant 1991; Newbert 2008). In this research, we refer to six types of firm resources: age, size, profitability, liquidity, leverage, and brand familiarity.
8. Abnormal stock return (after data breach announcement)	The difference between the observed return and the return expected in the absence of the event (Binder 1998; MacKinlay 1997).

Accordingly, further examination of service crises is important because such situations markedly differ from product-harm crises and private service failures. Indeed, service crises are especially difficult to manage as they are not associated with clear recovery solutions, such as recalling defective products (Gijsenberg, Van Heerde, and Verhoef 2015). Service crises also differ from private service failures in terms of number of affected stakeholders and public attention; the former situation needs to be carefully managed given its public component (Rasoulian et al. 2017). The current research accounts for the particularities of service crises by developing a comprehensive framework that specifically applies to such situations. By doing so, we also answer recent calls that urge service researchers to take a firm perspective, to use quantitative models, and to integrate financial metrics (Grégoire and Mattila 2020; Khamitov, Grégoire, and Suri 2020).

Prior research concludes that the announcements of data breaches typically result in negative stock returns (Acquisti, Friedman, and Telang 2006; Campbell et al. 2003; Cavusoglu, Mishra, and Raghunathan 2004; Malhotra and Malhotra 2011). The current framework complements this literature by addressing two specific gaps. First, our knowledge remains limited about the key attributes of data breaches that affect changes in stock returns. For instance, we cannot decisively conclude that all types of data breaches *always* result in negative stock returns. Second, we pay special attention to understanding the effects of some resources that could help organizations recover from major data breaches. Depending on their initial situations, companies are not all equal when facing data breaches. The proposed framework addresses these two issues by making two corresponding contributions, as we explain next.

As a first contribution, we build a framework by integrating two literatures: service failure-recovery and crisis seriousness assessment. Using the distinction between outcome and process in service failure (Carr 2007; Seiders and Berry 1998), we argue that investors' reactions are explained by the *outcome seriousness* and *process seriousness* of such a service crisis. The seriousness of a crisis, or a data breach in our case, is broadly defined as the extent to which the damages caused by a crisis are important and threaten the functioning of an organization (Burnett 1999; Pearson and Mitroff 1993). We define our two types of seriousness—outcome and process (Table 1)—by referring to four dimensions identified in the literature on crisis assessment (Billings, Milburn, and Schaalman 1980; Burnett 1999). Here, the seriousness of an outcome refers to the sensitiveness of the breached data for the firm and the stakeholders. This notion refers to the "value of loss" identified in the crisis literature. In turn, the seriousness of a process refers to the importance of the causal process at the origin of the breach. It is determined on the basis of three criteria identified in the crisis literature: the probability of damage, the time pressure to solve the defective process, and the degree of control of a firm over the process.

Building on these conceptual foundations, we claim as our first contribution that *outcome seriousness* is enhanced when the breached data contain sensitive information, such as financial data, social security numbers (SSNs), or medical information. In a similar vein, the *process seriousness* becomes salient when the breach is caused by hacker attack or theft of equipment—that is, incidents involving external "thieves." By doing so, we specify the conditions for which the outcome or process of a data breach becomes more threatening and serious; such specifications represent the core of our first contribution. Then, we predict that outcome or process seriousness decreases a firm's future stock value (Malkiel and Fama 1970; Srivastava, Fahey, and Christensen 2001). We test such predictions by conducting an event study with a sample of 217 data breach announcements.

As our second contribution, we explore the extent to which organizational recovery resources can buffer the negative effect of service crises seriousness (outcome and process) on firms' performance. Most of these recovery resources are reflected in a firm's size, age, brand familiarity, and three financial resources (i.e., liquidity, leverage, and profitability) (e.g., Esteve-Pérez and Mañez-Castillejo 2008; Grant 1991). The availability of these six recovery resources is expected to facilitate firms' recovery process after data breaches (Newbert 2008; Thornhill and Amit 2003). As a result, the cash flow prospects of a firm with strong recovery resources should be accompanied with less devaluation. To the best of our knowledge, our research examines the largest set of recovery resources ever considered in the literatures on data breaches and service crises; this comprehensive examination represents the core of our second contribution. By doing so, we contribute to the literature on service recovery by examining the role of firms' resources at a macro level. As highlighted by Van Vaerenbergh and Orsingher (2016), there is limited research that examines the antecedents and aspects of the recovery process at a macro level (see Smith, Fox, and Ramirez 2010; Smith and Karwan 2010 for exceptions). Indeed, most of the scholarly attention has been given to "micro" measures (e.g., apologies and compensation) that managers can use to recover service failures or crises. Addressing this gap, our research shows the role of "macro" recovery resources in buffering the negative impacts of specific service crises (i.e., data breaches) on investors' responses.

The remainder of this article is organized as follows. After reviewing the literature on the impact of data breaches on firms' abnormal stock returns, we integrate the literatures on service failure and crisis seriousness to formulate our hypotheses. Next, we explain our data collection and analyses. Finally, we present our results and discuss their implications.

Research Background

We identified six articles that examine the market-level consequences of data breaches viewed as service crises. We summarize this literature in Table 2. Two of these studies primarily focus on *information technology (IT) security breaches*—that is, a broad category in which data breach is only one of the possible instances (e.g., Campbell et al. 2003; Cavusoglu, Mishra, and Raghunathan 2004). Specifically, IT security breach is defined as a malicious electronic attempt—typically associated with

Table 2. Summary of the Major Literature on Data Breach and Stock Returns.

Study	Areas of Focus	Sample	Key Findings
Martin, Borah, and Palmatier, (2017)	The impacts of data breaches, firms' privacy policies (transparency of information practices and level of customers' control over their personal data), number of affected customers, firm size, and firm industry type (service vs. goods) on abnormal stock return of the focal firm and its rivals.	293 events of all possible types of customers' data breaches.	Data breaches result in negative abnormal returns for focal and rival firms. Customers' control over managing their data decreases the magnitude of return. High number of affected individuals will increase this magnitude for the focal firm and will decrease it for the rival firms. Firm size and firm industry type do not have a significant impact on abnormal returns.
Malhotra and Malhotra, (2011)	The impacts of data breaches, firm size, firm industry sector (financial or retail), number of affected customers, and type of breached data (financial vs. personal) on the net present value of corporations.	93 events of customers' data security breaches, including hacker attack, theft of equipment, and insider attack.	Data breaches result in negative abnormal returns, especially in the long run. Larger firms suffer greater market value loss than smaller firms, and larger firms suffer more from large breaches. There are no independent effects of number of affected customers and type of breached data on the net present value.
Gatzlaff & McCullough (2010)	The impacts of data breaches, firm size, market-to-book ratio, market capitalization, and subsidiary responsibility on abnormal stock return.	77 events of customers' and employees' data breaches, including data stolen, theft of equipment, and misplaced data sources.	Data breaches result in negative abnormal returns. This effect is larger for firms with higher market-to-book ratio and smaller for large firms and subsidiaries.
Acquisti, Friedman, and Telang, (2006)	The impacts of data breaches, number of affected individuals, industry sector, type of victimized stakeholder (customer vs. employee), and firm size on abnormal stock returns.	79 events of customers' and employees' data breaches, including hacker attack, theft of equipment, improper disposal, misplaced data source, and insider attack.	Data breaches result in negative abnormal returns. This impact is lesser for large firms and is greater for events affecting more than 100,000 individuals. There is no significant effect for the type of victimized stakeholders and industry sector.
Cavusoglu et al., (2004)	The impacts of IT security breaches (i.e., access attack, modification attack, and denial-of-service attack), firm type (online sellers vs. conventional sellers), and firm size on abnormal stock returns.	32 events of access attack and modification attack to customers' data and 34 events of denial-of-service attack to websites of firms.	Both access attack and denial-of-service attack result in negative abnormal returns. Smaller firms and online selling firms suffer more intensively from IT security breaches.
Campbell et al., (2003)	The impacts of IT security breaches, including data breach (data stolen) vs. denial-of-service attack (no data stolen) on abnormal stock returns.	11 events of data breach attack to customers' data and 32 events of denial-of-service attack to websites of firms.	Only data breach attacks (data stolen) result in negative abnormal returns.
Our contribution	The impacts of data breaches, type of breached data (financial, social security number, medical information, etc.), procedure of breach (hacker attack, theft of equipment, etc.), type of victimized stakeholder (customer vs employees), and the moderating role of organizational recovery resources on abnormal stock returns.	217 observations with 176 distinct firms of all possible types and processes of data breaches against both customers and employees.	Data breaches result in negative abnormal returns for firms. This diminishment is more pronounced for financial data breaches and hacker attacks. Firm size, profitability, and liquidity are the main resources that can help the firm to recover from data breaches. In the specific case of financial data breaches, firm age and brand familiarity also play a key role in recovery. Key contribution 1: Testing the individual effects of a detailed typology of breached data (outcome and procedure of breach (process)). Key contribution 2: Examining the moderating effect of a comprehensive list of six recovery resources.

Table 3. Definitions and Frequencies of the Causal Processes of Data Breaches.

Causal Processes	Definition	Frequency	
		N	(%)
1. Accidental disclosure	Posting data 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
2. Hacker attack	Electronic entry to networks or computers by an outside party (Hansman and Hunt 2005).	39	18
3. Improper disposal	Failing to dispose of paper documents securely, such as discarding them without shredding (Culnan and Williams 2009).	12	5.5
4. Insider attack	Intentional breach of data by someone with legitimate access, such as an employee or a contractor (Sarkar 2010; Schultz 2002).	66	30.5
5. Misplaced data source	Misplacing data sources, such as smartphones, portable memory devices, CDs, hard drives, and data tapes, inside or outside the firm (Sarkar 2010).	22	10
6. Theft of equipment	Illegal confiscation of equipment, such as laptops, computers, or other data sources, such as smartphones, portable memory devices, CDs, hard drives, and data tapes, by thieves inside or outside the firm (Whitman 2004).	44	20

hacker attacks—that aims to interfere with a company's information system (Cavusoglu, Mishra, and Raghunathan 2004). IT security breaches can result in several IT failures, including data breach (i.e., gaining unauthorized access to data), modification attack (i.e., inserting or deleting data), or denial-of-service (i.e. blocking the use of resources, applications, or information to legitimate users) (Campbell et al. 2003; Cavusoglu, Mishra, and Raghunathan 2004). These two studies show that IT security breaches lead to negative abnormal returns. Although these two studies are informative, they are not conducted in the same context as this current research. Here, we focus on data breaches that can be caused by a variety of reasons labeled causal processes. Our context is not limited to hacker attacks, and it incorporates other causal processes such as misplacing data sources, thefts of equipment, accidental disclosures, improper disposals, and insider attacks (see Table 3).

Consistent with our orientation, the four remaining articles focus on data breaches, and they have generated many important insights (see Table 2 for details). First, Acquisti, Friedman, and Telang (2006) examine the market-level consequences of data breaches with a diverse set of causal processes (i.e., misplaced equipment, theft of equipment, insider attack, bad security practices, and software flaws) involving customers and employees. Then, Malhotra and Malhotra (2011) investigate the effects of the number of affected customers, the type of breached data (financial vs. personal), and firm size on the net present value of corporations. In turn, (Gatzlaff & McCullough, 2010) explore the effects of book-to-market ratio, firm size, subsidiary responsibility, and three causal processes (i.e., data stolen, theft of equipment, and misplaced data sources) on abnormal returns. Finally, Martin, Borah, and Palmatier (2017) focus on the effects of firms' data protection policies (i.e., policy transparency and data control strength[1]), firm size, and industry type on investors' and consumer's responses. The dominant conclusion of these four studies is that the announcement of data breaches is almost always associated with negative firm value.

Building on these insights, the current research complements this literature by specifying the attributes of a data breach that enhance its seriousness, which would ultimately affect a firm's abnormal returns. Although some prior research examines the effect of a few causal processes or types of breached data, we are not aware of any research that simultaneously examines the effects of a large set of *both* causal processes and data types. In addition, prior research has somewhat overlooked the protective effects of organizational recovery resources. Some research includes some of these resources, but we are not aware of any prior work that formally examines a large set of organizational recovery resources. In the light of these important gaps, we develop a comprehensive framework that simultaneously investigates the effect of large sets of data breaches' attributes—in terms of causal processes and data types—and organizational recovery resources, as we see next.

Conceptual Framework

The Impact of Data Breach Announcements on Stock Returns

Prior research conceptualizes data breaches as service crises involving customers and employees (e.g., Malhotra and Malhotra 2011; Rasoulian et al., 2017). For customers, the security of information is a basic and necessary prerequisite for service quality (Lewis and Mitchell 1990; Martin and Murphy 2016; Rasoulian et al. 2017). For employees, firms must respect their right to safety, privacy, and fair treatment (Carroll 1991). Here, the literature on opportunism argues that firms' failure to fulfill their fundamental obligations toward customers or employees, either actively or passively, would lead to profound dissatisfaction (Seggie, Griffith, and Jap 2013; Wathne and Heide 2000). Thus, all stakeholders would view any violation of their privacy as a major service failure, which would represent a crisis when many individuals are affected, and the situation becomes public (Rasoulian et al. 2017).

Service crises threaten firms' survival, profitability, and stock returns (Larivière 2008; Pearson and Mitroff 1993). These repercussions stem from the damages that crises cause to organizations' tangible and intangible assets (Coombs and Holladay 2002). In the context of data breaches, these damages include loss of reputation, financial costs, and operational interruptions (Janakiraman, Lim, and Rishika 2018). In addition, many expenses are associated with data breaches (Hansman and Hunt 2005; Romanosky and Acquisti 2009; Romanosky, Telang, and Acquisti 2011; Sarkar 2010), such as the costs related to legal investigations, offering compensation, repairing damages (e.g., physical or digital), and improving current systems and processes (e.g., updating firewalls, training employees, and improving policies).

Since the negative impact of data breaches on stock returns is well established (Acquisti, Friedman, and Telang 2006; Martin, Borah, and Palmatier 2017), we do not formulate a formal hypothesis on this effect (although our results reconfirm it). The current research expands this key finding by examining the specific attributes of data breaches that amplify negative stock returns. As we see next, these attributes are assessed depending on their levels of seriousness.

Seriousness of Service Crises: Process and Outcome

Our conceptual framework (Figure 1) posits that the seriousness of a data breach—in terms of process and outcome—conditions firms' negative abnormal stock returns. When the attributes of a data breach indicate the presence of serious crises, firms should expect heightened damages to their resources and competitive advantage. As a result, investors will strongly devalue their performance and future cash flow.

As previously noted, we employ the literatures on service failure and crisis seriousness assessment to develop our framework (see Table 1 for definitions). A service failure can be assessed by referring to two dimensions: outcome and process (Carr 2007; Seiders and Berry 1998; Smith, Bolton, and Wagner 1999). An outcome refers to the "what" question and the object that is lost after a service failure. In our context, it represents the type of data that is affected during a data breach. In turn, a process refers to the "how" question and the deficient procedure that created the service failure. In our context, it refers to the causal process that was at the origin of the data breach (see Table 3). In the next subsections, we describe the different outcomes and processes considered in this research. Then, we explain why the level of seriousness varies for different outcomes and processes.

Outcome Seriousness: In our context, the outcome refers to the type of breached data, which we conceptualize as financial data (i.e., credit card, debit card, and bank account information), social security number, medical information, and identification information (i.e., name, driver's license number, date of birth, address, e-mail address, or phone numbers). These different categories are associated with different levels of outcome seriousness, which vary according to the sensitive nature of the given data (Table 1). The notion of outcome seriousness is drawn from the notion of *value of loss*, which is well established in crisis assessment (Billings, Milburn, and Schaalman, 1980; Burnett 1999). This concept refers to the importance of the losses resulting from the crisis for firms and their stakeholders.

Breached data could be used in several fraudulent ways—such as incurring charges on accounts as well as applying for credit cards, mortgages, and unemployment benefits—which could cause financial and psychological harm to the victims (Romanosky and Acquisti 2009; Romanosky, Telang, and Acquisti 2011). Also, the breach of data could cause reputational harm to victims, as in the case of medical information breaches (Kierkegaard 2012).

Above all, the breach of financial data, SSNs, and medical information are among the most threatening losses affecting firms and stakeholders (Romanosky, Hoffman, and Acquisti 2014). In the case of financial data, victims can easily file lawsuits against firms by alleging financial harm. Here, Romanosky et al. (2014) report that the odds of being sued are six times greater for firms when breaches include financial data.

In a similar vein, but to a lesser extent, the breaches of SSNs or medical information could imply a high value of loss for firms and stakeholders. According to legislations, such as the Identity Theft Prevention Act (ITPA) or the Health Information Portability and Accounting Act (HIPAA), firms are required to implement advanced protection for these two groups of data. Failing to protecting such data could cause firms to compensate the reputational, financial, or psychological losses of victims (Romanosky, Hoffman, and Acquisti 2014; Romanosky, Telang, and Acquisti 2011). Moreover, after the breach of these types of data, firms need to undergo criminal investigations and to notify victims about the loss of their data (Kierkegaard 2012). In sum, all the measures associated with these two types of data make the situations particularly serious for firms.

Given the above explanations, breached data that contain financial data, SSNs, or medical information—compared with other types of data—should lead to higher outcome seriousness. It should be noted that outcome seriousness should be especially important for breached financial data. Accordingly, these different levels of outcome seriousness, varying according to the type of data, should result in negative abnormal returns for firms.

> *H1*: The magnitude of negative abnormal returns for data breach is larger when the breached data contain (*a*) financial data (vs. other types of data) or (*b*) SSNs or medical information (vs. other types of data).

Process Seriousness: As previously noted, the current research focuses on six causal processes: accidental disclosure, hacker attack, improper disposal, insider attack, misplaced data sources, or theft of equipment. Table 3 provides specific definitions and the frequencies of occurrence of each process. To the best of our knowledge, there is no formal taxonomy of causal processes for data breaches. However, the suggested list incorporates most of the instances identified in prior work (Table 2), and it is the most exhaustive found in the literature. As

displayed in Table 3, insider attack (i.e., intentional breach of data by someone with legitimate access, such as employees) is the most frequent type reported in our databank, whereas improper disposal (i.e., failing to dispose of paper documents securely) is the least likely.

In our context, process seriousness captures the importance of a given causal process, and it is determined by referring to three key criteria established in crisis assessment—that is, the probability of damage, the time pressure to solve the defective process, and the degree of control of a firm over the defective process (Billings, Milburn, and Schaalman 1980; Burnett 1999). First, the *probability of damage* represents the likelihood that badly intentioned individuals would abuse the breached data. Second, the *time pressure* dimension refers to the amount of time available to the organization to formulate a satisfactory solution for the incident. Finally, *the degree of control* is the amount of firms' control over their internal and external environments to reduce the impacts of the defective process or to stop it completely. Using these criteria, we posit that a causal process is particularly serious when it is likely to result in abusing data, when a firm has limited time to fix its deficiencies, and when managers have limited control over its effects.

By using this tripartite conceptualization, we argue that hacker attack is a causal process associated with a high level of seriousness. Hacker attacks represent electronic entries to firms' computers by malicious outside parties (Hansman and Hunt 2005; Mookerjee et al. 2011). First, the likelihood of abusing the data is very high (i.e., probability of damage); the main motivation of hackers is to abuse the data or to sell them to other criminals (Mookerjee et al. 2011). Second, hacker attacks put serious time pressure on firms to restore the integrity of their information system and to regain their business continuity. Third, the degree of control to resolve the crisis and to retrieve the breached data is low because hackers are rarely identifiable (Hansman and Hunt 2005; Spitzner 2003). Overall, the occurrence of a hacker attack incident intensifies the three dimensions of process seriousness.

Using similar reasoning, theft of equipment is a second causal process associated with a high level of seriousness. Here, this process is defined as the illegal confiscation of equipment (such as laptops, computers, or other data storage sources), inside or outside the firm, by external thieves (Whitman 2004). Again, this causal process scores high on the three criteria of interest. First, the primary purpose of thieves is to resell the stolen equipment to other criminals. It is possible that malicious individuals would try to extract the data to abuse them (i.e., probability of damage). Second, the resulting absence of equipment can disrupt firms' operations (Spillan and Hough 2003), and firms would be under time pressure to regain their operational functionality. Third, since the thieves are unlikely to get caught (Bliss and Harfield 1998), the degree of firms' control to resolve the issue and to retrieve the data is low.

In sum, the announcement of hacker attacks or thefts of equipment intensifies the three dimensions of process seriousness. The other causal processes—accidental disclosure, improper disposal, insider attack, and misplaced data source—seem less serious because they would aggravate only a few dimensions of interest. Hence, the two former causal processes (i.e., hacker attacks or thefts of equipment) indicate high levels of process seriousness, which would result in substantial negative abnormal returns. Therefore:

H2: The magnitude of negative abnormal returns for data breach is larger when the breach is caused by *a)* hacker attack (vs. other causal processes) or *b)* theft of equipment (vs. other causal processes).

The Role of Organizational Recovery Resources in Service Crises

Organizational recovery refers to the process of firms' restoration and recuperation after crises, either to the same state or a different position as before the incident (Linnenluecke, Griffiths, and Winn 2012; Morrow et al. 2007). In such a process, firms' tangible and intangible resources play a key role because they affect firms' ability to restore themselves successfully (Esteve-Pérez and Mañez-Castillejo 2008; Grant 1991; Newbert 2008; Thornhill and Amit 2003; Tweneboah-Kodua, Atsu, and Buchanan 2018). Previous work on data breaches has investigated mainly the effect of firm size (Cavusoglu, Mishra, and Raghunathan 2004; Malhotra and Malhotra 2011). We extend this knowledge base by examining the moderating role of a wider set of organizational resources, including size, age, financial resources (i.e., profitability, liquidity, and leverage), and brand familiarity. All these resources are well documented in the resource-based theory of the firm (Grant 1991; Newbert 2008), and they are expected to support firms' recovery process at a macro level ((Van Vaerenbergh and Orsingher 2016).

Building on the direct effects exposed in H1 and H2, we hypothesize that the recovery resources of interest will attenuate the effects of serious outcomes (i.e., financial data and social security number/medical information) and serious processes (i.e., hacker attacks and theft of equipment) on firms' negative abnormal returns. To the best of our knowledge, the current research is among the first attempt to show how specific resources can play a direct role in helping firms' recovery process after service crises. In the next subsections, we explain the attenuating moderation effects of each organizational recovery resources.

Firm age: Older firms, compared to younger firms, have well-established resources and capabilities that make them better equipped to face environmental changes and organizational crises. During major data breaches, the experience of older firms should help them restore their operations and cope with the business uncertainties associated with the situation (Grant 1991; Thornhill and Amit 2003). Accordingly:

H3: The magnitude of negative abnormal returns for the following types of breaches—*a)* financial data, *b)* social security number or medical data, *c)* hacker attack, or *d)* theft

of equipment—is attenuated for older firms (compared to younger firms).

Firm size: Indeed, firm size contributes to the recovery of an organization after a crisis for two key reasons: economy of scale and reputation (Murphy et al., 2009). The reason associated with the economy of scale entails the following logic. If organizational crises impose new fixed costs, then the losses in percentage will be less for larger firms compared to smaller firms. Also, larger firms can allocate more tangible resources and employees to resolve a crisis. From a reputational perspective, larger firms with solid brand names may more easily counter the perceptual damage of a crisis, compared to smaller firms. Such a reputational advantage should reduce the impact of losses for larger firms, compared to smaller organizations.

H4: The magnitude of negative abnormal returns for the following types of breaches—*a)* financial data, *b)* social security number or medical data, *c)* hacker attack, or *d)* theft of equipment—is attenuated for larger firms (compared to smaller firms).

Firms' financial resources: Financial resources are important tangible assets that significantly influence the competitive advantage of a firm (Newbert 2008). They create a form of "safety cushion" to recover from random shocks (Cooper, Gimeno-Gascon, and Woo 1994). The access to strong financial resources directly helps a firm to meet its short-term and long-term financial obligations to overcome a crisis (Wiklund, Baker, and Shepherd 2010). During a crisis, a firm may undergo financial strain to provide compensations to its victims and to address its legal liabilities. In this context, the possession of solid financial resources can buffer the pressure of crises. A large number of financial ratios can be used as indicators of firms' financial solidity (Beaver 1966). Among this large selection, we choose three of the most currently used ones: profitability, liquidity, and leverage (Altman 1968; Wiklund, Baker, and Shepherd 2010).

Profitability is the ability of a firm to generate revenues in excess of expenses. It is a key indicator of the ability of the firm to repay its debts. It also acts as an internal buffer against crisis because it reflects a reliable financial process that could help firms recover from crises (Beaver, McNichols, and Rhie 2005; Wiklund, Baker, and Shepherd 2010). In turn, *liquidity*—or the availability of internal funds—is the ability of a firm to meet its short-term financial obligations (Wiklund, Baker, and Shepherd 2010). High liquidity indicates that the firm possesses enough cash to fulfill its short-term needs and to recover from the short-term effects of a crisis.

Finally, *leverage*—which represents the long-term debts and liabilities—refers to the extent to which non-equity capital is used in a firm (Opler and Titman 1994). Higher levels of debt suggest a reduced ability for firms to generate new, reasonably priced debt (Opler and Titman 1994; Wiklund, Baker, and Shepherd 2010). Therefore, high leverage is associated with firms' financial vulnerability and risk of default. Since crises could impose new long-term liabilities, the combination of new and current liabilities could degrade the future financial health of the firm. Building on these explanations, we predict the following hypotheses for the three financial resources of interest:

H5: The magnitude of negative abnormal returns for the following types of breaches—*a)* financial data, *b)* social security number or medical data, *c)* hacker attack, or *d)* theft of equipment—is attenuated for firms with greater profitability (vs. firms with less profitability).

H6: The magnitude of negative abnormal returns for the following types of breaches—*a)* financial data, *b)* social security number or medical data, *c)* hacker attack, or *d)* theft of equipment—is attenuated for firms with greater liquidity (vs. firms with less liquidity).

H7: The magnitude of negative abnormal returns for the following types of breaches—*a)* financial data, *b)* social security number or medical data, *c)* hacker attack, or *d)* theft of equipment—is attenuated for firms with less leverage (vs. firms with greater leverage).

Brand familiarity: Brand familiarity reflects consumers' direct or indirect experiences with the brand (Benedicktus et al. 2010; Dawar and Lei 2009). There is evidence that brand familiarity positively impacts the attitude and trust of customers toward the brand (Benedicktus et al. 2010). In crises, brand familiarity may act as a buffer against the adverse impact of negative information on brands (Dawar and Lei 2009). Upon receiving new information that challenges a prior attitude, people usually try to defend their initial perception. Accordingly, consumers could perceive familiar brands to carry less responsibility for crises, and such perceptions would translate into lower negative impacts on brand evaluations. The marketing-finance literature also provides evidence that firms with greater brand familiarity experience a more stable financial performance (Rego, Billett, and Morgan 2009). Formally:

H8: The magnitude of negative abnormal returns for the following types of breaches—*a)* financial data, *b)* social security number or medical data, *c)* hacker attack, and *d)* theft of equipment—is attenuated for firms with greater brand familiarity (vs. firms with less brand familiarity).

Research Design

Data and Sample

We used records and announcements from several sources (e.g., Privacy Rights Clearinghouse, Factiva and web search engines, and Standard & Poor's COMPUSTAT database) to construct our dataset. We started by randomly collecting the announcements of data breach events from the Privacy Rights Clearinghouse[2] database. Our initial sample consisted of 340 observations, involving publicly traded firms, from 2005 to

Table 4. Cross-Tabulation of Serious Data Breaches and Organizational Recovery Resources.

	Firm Age		Firm Size		Firm Profitability		Firm Liquidity		Firm Leverage		Brand Familiarity	
	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High
Financial data	46	49	49	46	61	34	78	20	59	36	41	54
SSN/medical data	62	61	68	55	65	58	78	45	80	43	64	59
Hacker attack	17	22	22	17	21	18	26	13	23	16	19	20
Theft of equipment	16	28	20	24	23	21	23	21	29	15	21	23

2013. Next, we checked these announcements through the Factiva database and web search engines to verify the precise announcement dates and obtain the details of events. Afterward, we dropped cases with confounding announcements within 1 week before and after the event to make sure that the announcements about each case were not affected by other announcements (McWilliams and Siegel 1997). We considered the following types of news as confounding announcements: earning announcements, mergers and acquisitions, and large profit announcements. Our final sample consists of 217 observations with 176 distinct publicly traded companies. Out of the 217 cases, 140 affected only customers, 69 only employees, and the rest both the employees and customers. Overall, our sample contains 79.5% service firms versus 20.5% manufacturing firms. It should be noted that data breach is a specific type of service crisis that could occur in any industry collecting personal data. For data breaches, the service failure involves an inability at protecting the data or information of stakeholders, and such events could occur in both manufacturing and service industries.

Finally, we classified each event by the type of breached data (i.e., financial, social security number or medical information, and others, such as name and address) and the causal processes (i.e., hacker attack, theft of equipment, and others, such as accidental disclosure and improper disposal) according to our definitions (Table 3). To perform this task, two independent coders were hired to categorize the different types of breaches. We used dummies to codify each of the four categories of "hacker attack," "theft of equipment," "financial data," and "SSNs and medical information." For instance, if the event happens through a hacker attack, it takes the value 1 and 0 otherwise; or if the event breaches the financial data of stakeholders, it takes the value 1 and 0 otherwise. The inter-coder agreement, using (Perreault Jr & Leigh, 1989) reliability index,[3] was 0.975 for hacker attacks (39 observations), 0.981 for theft of equipment (44 observations), 0.941 for financial data (95 observations), and 0.932 for SSNs/medical information (123 observations). Overall, these scores signal high inter-coder agreement and reliability of classification of events.

We computed firm-level accounting data using Standard & Poor's COMPUSTAT database. Table 4 contains the number of different types of serious data breaches across different levels of recovery resources (low vs. high). As this table shows, these different events happened almost equally to organizations with different levels of recovery resources.

Abnormal Stock Return Measurement

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

For each event announcement, we estimated Equation 1 using OLS regression over a 120-trading-day period ending 10 days before the event so as not to overlap the event period.

Using Equation 2, we estimated abnormal returns of stock i on day t during the event period

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

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 abnormal return (CAR) for each stock had to be computed for an appropriate event window. Following a well-established method in the literature of marketing-finance (Karniouchina, Uslay, and Erenburg 2011; Wiles and Danielova 2009), we determined the appropriate event window on the basis of the graph of the aggregated cumulative average abnormal return (CAAR). This graph illustrates the time period in which the stock market reacts to the target event. Figure 2 shows this graph from 5 days before to 10 days after the event. According to this graph, the negative trend starts from day 0 (i.e., the day of announcement) and continues to day 3, with no leakage before day 0. Although there are negative noises after day 3, we cannot confidently associate them with our event of interest because of the time gap. In sum, the window [0, 3] covers the majority of the negative reactions of the stock market to the announcement of the data breach.

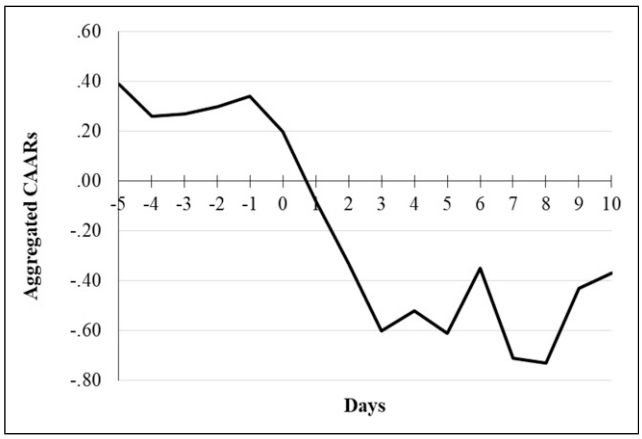

Figure 2. Aggregated CAARs over time.

In order to further verify the appropriateness of our event window, we examined the CAAR for several possible windows around the event date. The results show that the window [0, 3] is significant with the highest amount of CAAR (see Table 6, which is presented in the next section).

Moderating and Control Variables

To test the moderating effect of recovery resources, we measured firm age as the logarithm of the number of months that elapsed since the stock's inclusion in CRSP (McAlister, Srinivasan, and Kim 2007). Firm size was measured as the logarithm of the total value of assets (Kalaignanam, Shankar, and Varadarajan 2007). We measured profitability as the return on total assets. Liquidity was measured as cash and short-term investment in relation to total assets, and leverage was computed as the ratio of long-term debt to total assets (Beaver 1966).

Brand familiarity was measured as the number of the *New York Times* mentions during the year preceding the event (Karniouchina, Uslay, and Erenburg 2011). To this end, a Python web crawler was developed to count the number of articles from the *New York Times* in which the name of the firm was mentioned.

In addition, we controlled for important industry and event level covariates in our analyses to regulate the extent to which the data breach announcement can explain the movements in the stock returns of firms.

Victimized stakeholders: Using a three-level nominal variable, we controlled for the type of victimized stakeholders (customers, employees, or both) to explore if this variable would impact abnormal stock returns in response to the data breach announcement.

Third-party responsibility: We coded whether the event 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 type: North American Industry Classification System (NAICS) codes were used to control the industry-level changes. Natural financial performance varies in different industry sectors (Campbell et al. 2001), and different sectors have varied potentials in dealing with data breaches (Tweneboah-Kodua, Atsu, and Buchanan 2018). We used dummies for this variable.

Year: Dummies for the year when the event happened were also considered. This market-level variable calibrates for yearly macroeconomic performances (McGahan and Porter 1997).

Results

Descriptive Statistics

Table 5 shows the descriptive statistics of our variables and Pearson's correlations between each pair of variables used in our research. This table reveals that pairwise correlations are all below 0.40, which suggests that multicollinearity is not an issue in our regression analyses. Variance inflation factors are below 1.5 (i.e., substantially below the 10 guideline), thus illustrating no issue of multicollinearity (O'brien 2007).

Event Study Analysis

Results of the impact of a data breach announcement on the stock returns are reported in Table 6 for several windows. CAARs of windows [−1, 0] and [−2, 0] are not significant, demonstrating that there is no leakage before the date of announcements in our study. As we discussed earlier, window [0, 3] significantly covers the majority of market reactions to the event announcement.

The Cowan generalized sign test (Generalized Sign Z)—a nonparametric test (Cowan 1992)—and the 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 the 4-day period, starting from the date of the announcement, the stocks of firms lost on average 0.94% as a result of the data breach announcement. This finding is comparable to that of prior studies (Acquisti, Friedman, and Telang 2006; Martin, Borah, and Palmatier 2017). Considering the average market capitalization of corporations in our sample (US$35,563 million), the 0.94% loss means that firms lost on average US$335 million in market capitalization within 4 days per breach event.

Cross-Sectional Regression Results

Table 7 presents the main results of our analyses. Model 1 estimates the direct effect of different types of serious data breaches on abnormal stock returns. Model 2 investigates the individual impact of serious data breaches, six organizational recovery resources, and control variables. Model 3 examines the interactions between organizational recovery resources and serious data breaches to assess the recovery effectiveness of a firm's resources.

Table 5. Descriptive Statistics and Correlation Matrix (N = 217).

Variables	M	SD	VIF	1	2	3	4	5	6	7	8	9	10	11
1. Abnormal return	−0.01	0.05	—	—	—–	—	—	—	—	—	—	—	—	—
2. Financial data	0.44	0.50	1.27	−0.10	—	—	—	—	—	—	—	—	—	—
3. SSN and medical data	0.56	0.50	1.49	0.04	−0.38***	—	—	—	—	—	—	—	—	—
4. Hacker attack	0.18	0.38	1.31	−0.12	0.05	−0.34***	—	—	—	—	—	—	—	—
5. Theft of equipment	0.20	0.40	1.28	0.01	−0.17**	0.35***	−0.23***	—	—	—	—	—	—	—
6. Firm age	5.27	0.95	1.14	0.10	0.01	0.01	0.02	0.10	—	—	—	—	—	—
7. Firm size	9.92	2.46	1.28	0.11	0.07	−0.10	−0.13*	−0.05	0.08	—	—	—	—	—
8. Firm profitability	0.04	0.08	1.22	0.21**	−0.19	0.09	−0.15**	0.03	0.16*	−0.08	—	—	—	—
9. Firm liquidity	0.11	0.12	1.26	0.05	−0.20***	0.08	0.10	0.16**	−0.20**	−0.17**	0.17**	—	—	—
10. Firm leverage	0.19	0.19	1.11	0.01	0.10	−0.10	−0.01	−0.09	−0.03	−0.15**	0.11*	−0.11	—	—
11. Brand familiarity	4.53	2.26	1.19	0.19***	0.05	−0.12*	−0.07	0.01	0.05**	0.36***	0.01	0.03	0.05	—
12. Third-party responsibility	0.22	0.41	1.18	0.03	−0.15*	0.21**	−0.24***	0.26***	−0.02	0.01	0.20**	0.13	−0.06	−0.13**

* p<0.1; ** p<0.05; *** p<0.01.

Table 6. CAARs for Data Breach Announcement (N = 217).

Event Window	CAAR	Number of Events with Negative Abnormal Returns	Patell z	Generalized Sign Z
(−2,0)	−0.07	117 (100)	−0.357	−0.670
(−1,0)	−0.10	110 (97)	−0.591	−1.077
(0,0)	−0.14	116 (101)	−0.859	−0.534
(−1,+1)	−0.38	131 (86)	−1.572	−2.572**
(0,+1)	−0.42	132 (85)	−1.942*	−2.707**
(0,+2)	−0.67	127 (90)	−2.558**	−2.028*
(0,+3)	−0.94	128 (89)	−2.355**	−2.164*
(−1,+2)	−0.62	130 (87)	−2.204*	−2.436**
(−1,+3)	−0.90	126 (91)	−2.096*	−1.892*

* $p < 0.05$; ** $p <$ .01; *** $p < 0.001$.

To check for the existence of outliers, we used the minimum covariance determinant (MCD) method. This method revealed the existence of 18 outliers in our dataset. 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

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

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. Here, the cutoff value is equal to the square root of the 97.5% quantile of the chi-square distribution.

To alleviate the issue of existence of outliers and to reduce the concern about heteroscedasticity, we applied the M-estimator robust regression method to examine our hypotheses (Maronna, Martin, and Yohai 2006; Rousseeuw and Leroy 1987). This method minimizes the influence of outliers on the parameter estimation (Equation 4)

$$\min \Sigma_i \rho(r_i(X)) \quad (4)$$

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

$$\rho(t) = \begin{cases} \frac{t^2}{2}, & |t| \le c \\ c|t| - \frac{c^2}{2}, & \text{otherwise} \end{cases} \quad (5)$$

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

The estimation results of Model 1 and Model 2 show that financial data breaches (β = −0.013, SE = 0.004, chi-square = 7.41, $p < 0.01$) and hacker attacks (β = −0.017, SE = 0.005, chi-square = 8.50, $p < 0.01$) explain a significant number of the changes in investors' reactions following data breach announcements. These results support H1*a* and H2*a*. However, results for breaches of SSNs/medical information and breaches caused by theft of equipment either are weak or do not persist throughout our validation check. Hence, we could not find enough evidence to support H1*b* and H2*b* with the current dataset.

To fully capture the extent to which financial data breaches and hacker attacks constitute the 0.94% wealth loss that was found in our event study analysis, we computed CAARs for each of these two groups of events separately. We found that hacker attacks are significantly associated with 2.22% value loss (CAAR = −2.22%, Z_{gsign} = −2.984, $p < 0.01$), while other causes of data breaches do not on average lead to a significant loss (CAAR = −0.61%, Z_{gsign}= 0.506, not significant). Also, financial data breaches result in 1.52% significant value loss (CAAR = −1.52%, Z_{gsign}= −2.225, $p < 0.05$), yet non-financial data breaches do not show a significant loss (CAAR = −0.43%, Z_{gsign}= −0.348, not significant) in the current context. Translating these results to average loss on market capitalization, the corporations in our databank would have lost US$712 million and US$577 million as a result of hacker attacks and financial data breaches, respectively, within 4 days. These results seem to signal that hacker attack incidents are viewed by investors as being more serious and damaging.

The Model 2 estimation reveals that the interactions of financial data breaches and firm age (β = 0.009, SE = 0.004, chi-square = 4.79, $p < 0.05$), firm size (β = 0.004, SE = 0.002, chi-square = 3.89, $p < 0.05$), firm profitability (β = 0.267, SE = 0.061, chi-square = 19.38, $p < 0.01$), firm liquidity (β = 0.086, SE = 0.039, chi-square = 4.86, $p < 0.05$), and brand familiarity (β = 0.005, SE = 0.002, chi-square = 7.36, $p < 0.01$) are significant. So, H3*a*, H4*a*, H5*a*, H6*a*, and H8*a* are supported, but not H7*a* (i.e., the moderating impact of firm leverage).

In addition, interactions of hacker attacks and firm size (β = 0.005, SE = 0.002, chi-square = 3.06, $p < 0.05$), firm profitability (β = 0.199, SE = 0.056, chi-square = 12.84, $p < 0.01$), and firm liquidity (β = 0.107, SE = 0.044, chi-square = 5.79, $p <$ 0.05) are significant. Hence, H4*c*, H5*c*, and H6*c* are supported. The interactions between hacker attacks and the rest of organizational resources are not significant, or they do not survive our robustness tests.

Table 7. Results of the Impact of Data Breach on Abnormal Stock Return (Market Model).

		Model 1 (Main Model)		Model 2 (Individual Effects)			Model 3 (Interactions)		
Variables		Coefficients		Coefficients		Std. Coef.	Coefficients		Std. Coef.
Main effects									
Financial data (FD)	H1a (−)	−0.013***	(0.004)	−0.011***	(0.004)	−0.011***	−0.138***	(0.031)	−0.008**
SSN or medical data (SSN/MED)	H1b (−)	−0.006*	(0.004)	−0.007	(0.004)	−0.007	−0.131***	(0.031)	−0.008*
Hacker attack (HA)	H2a (−)	−0.017***	(0.005)	−0.013***	(0.005)	−0.013***	−0.029	(0.039)	−0.003
Theft of equipment (TE)	H2b (−)	−0.007	(0.004)	−0.005	(0.005)	−0.005	−0.024	(0.035)	−0.001
Firm age	—	—	—	−0.001	(0.002)	−0.001	−0.012***	(0.004)	−0.011***
Firm size	—	—	—	0.001	(0.001)	0.003	−0.003	(0.002)	−0.006
Firm profitability	—	—	—	−0.022	(0.027)	−0.002	−0.281***	(0.070)	−0.024***
Firm liquidity	—	—	—	0.034**	(0.015)	0.004**	−0.122***	(0.037)	−0.015***
Firm leverage	—	—	—	0.001	(0.010)	0.001	−0.056**	(0.026)	−0.011**
Brand familiarity	—	—	—	0.001*	(0.001)	0.003*	0.001	(0.002)	0.002
Interaction effects									
(FD) × Firm age	H3a (+)	—	—	—	—	—	0.009**	(0.004)	0.009**
(FD) × Firm size	H4a (+)	—	—	—	—	—	0.004**	(0.002)	0.009**
(FD) × Firm profitability	H5a (+)	—	—	—	—	—	0.267***	(0.061)	0.023***
(FD) × Firm liquidity	H6a (+)	—	—	—	—	—	0.086**	(0.039)	0.011**
(FD) × Firm leverage	H7a (−)	—	—	—	—	—	0.015	(0.021)	0.003
(FD) × Brand familiarity	H8a (+)	—	—	—	—	—	0.005***	(0.002)	0.011***
(SSN/MED) × Firm age	H3b (+)	—	—	—	—	—	0.013***	(0.004)	0.012***
(SSN/MED) × Firm size	H4b (+)	—	—	—	—	—	0.002	(0.002)	0.005
(SSN/MED) × Firm profitability	H5b (+)	—	—	—	—	—	0.286***	(0.066)	0.024***
(SSN/MED) × Firm liquidity	H6b (+)	—	—	—	—	—	0.172***	(0.042)	0.021***
(SSN/MED) × Firm leverage	H7b (−)	—	—	—	—	—	−0.004	(0.022)	−0.001
(SSN/MED) × Brand familiarity	H8b (+)	—	—	—	—	—	0.002	(0.002)	0.004
(HA) × Firm age	H3c (+)	—	—	—	—	—	−0.003	(0.006)	–0.003
(HA) × Firm size	H4c (+)	—	—	—	—	—	0.005**	(0.002)	0.012**
(HA) × Firm profitability	H5c (+)	—	—	—	—	—	0.199***	(0.056)	0.017***
(HA) × Firm liquidity	H6c (+)	—	—	—	—	—	0.107**	(0.044)	0.013**
(HA) × Firm leverage	H7c (−)	—	—	—	—	—	−0.003	(0.032)	−0.001
(HA) × Brand familiarity	H8c (+)	—	—	—	—	—	−0.002	(0.002)	−0.005
(TE) × Firm age	H3d (+)	—	—	—	—	—	−0.002	(0.005)	−0.002
(TE) × Firm size	H4d (+)	—	—	—	—	—	0.004*	(0.002)	0.009*
(TE) × Firm profitability	H5d (+)	—	—	—	—	—	0.096	(0.095)	0.008
(TE) × Firm liquidity	H6d (+)	—	—	—	—	—	−0.040	(0.036)	−0.005
(TE) × Firm leverage	H7d (−)	—	—	—	—	—	0.085***	(0.029)	0.016***
(TE) × Brand familiarity	H8d (+)	—	—	—	—	—	−0.004**	(0.002)	−0.010**
Controls									
Victimized stakeholders[a]	—	—	—	0.006	—	0.006	−0.011	(0.008)	−0.001
Victimized stakeholders[b]	—	—	—	−0.007	—	−0.007	−0.001	(0.005)	−0.011
Victimized stakeholders[c]	—	—	—	0[d]	—	.0[d]	0[d].		0[d]
Third-party responsibility	—	—	—	0.001	(0.004)	—	0.002	(0.004)	0.002
Industry type dummies	—	—	—	—	Included	—	—	Included	—
Year dummies	—	—	—	—	Included	—	—	Included	—

* $p < 0.1$; ** $p < 0.05$; *** $p < 0.01$.
[a]Employees.
[b]Employees and customers.
[c]Customers (reference category).
[d]This parameter is set to zero because it is redundant.

Table 8. Results of the Impact of Data Breach on Abnormal Stock Return (Fama–French).

Variables		Model 1 (Main Model)		Model 2 (Individual Effects)			Model 3 (Interactions)		
		Coefficients		Coefficients		Std. Coef.	Coefficients		Std. Coef.
Main effects									
Financial data (FD)	H1a (−)	−0.014***	(0.004)	−0.015***	(0.005)	−0.015***	−0.188***	(0.033)	−0.015***
SSN or medical data (SSN/MED)	H1b (−)	−0.008*	(0.004)	−0.005	(0.005)	–0.005	−0.115***	(0.032)	−0.008*
Hacker attack (HA)	H2a (−)	−0.013**	(0.005)	−0.011**	(0.006)	−0.011**	−0.046	(0.038)	−0.009*
Theft of equipment (TE)	H2b (−)	−0.001	(0.005)	−0.002	(0.006)	−0.002	−0.003	(0.039)	−0.005
Firm age	—	—	—	−0.001	(0.002)	−0.001	−0.013***	(0.004)	−0.013***
Firm size	—	—	—	0.002**	(0.001)	0.005**	−0.004*	(0.002)	−0.009*
Firm profitability	—	—	—	−0.044	(0.030)	−0.004	−0.211***	(0.070)	−0.018***
Firm liquidity	—	—	—	0.039**	(0.017)	0.005**	−0.096**	(0.039)	−0.012**
Firm leverage	—	—	—	0.007	(0.011)	0.001	−0.010	(0.026)	−0.002
Brand familiarity	—	—	—	0.001	(0.001)	0.002	0.002	(0.002)	0.005
Interaction effects									
(FD) × Firm age	H3a (+)	—	—	—	—	—	0.015***	(0.004)	0.015***
(FD) × Firm size	H4a (+)	—	—	—	—	—	0.005***	(0.002)	0.013***
(FD) × Firm profitability	H5a (+)	—	—	—	—	—	0.233***	(0.061)	0.020***
(FD) × Firm liquidity	H6a (+)	—	—	—	—	—	0.091**	(0.042)	0.011**
(FD) × Firm leverage	H7a (−)	—	—	—	—	—	−0.014	(0.021)	−0.003
(FD) × Brand familiarity	H8a (+)	—	—	—	—	—	0.005***	(0.002)	0.012***
(SSN/MED) × Firm age	H3b (+)	—	—	—	—	—	0.013***	(0.005)	0.012***
(SSN/MED) × Firm size	H4b (+)	—	—	—	—	—	0.002	(0.002)	0.005
(SSN/MED) × Firm profitability	H5b (+)	—	—	—	—	—	0.224***	(0.065)	0.019***
(SSN/MED) × Firm liquidity	H6b (+)	—	—	—	—	—	0.144***	(0.044)	0.018***
(SSN/MED) × Firm leverage	H7b (−)	—	—	—	—	—	−0.012	(0.023)	−0.002
(SSN/MED) × Brand familiarity	H8b (+)	—	—	—	—	—	−0.001	(0.002)	−0.002
(HA) × Firm age	H3c (+)	—	—	—	—	—	−0.014**	(0.006)	−0.014**
(HA) × Firm size	H4c (+)	—	—	—	—	—	0.005**	(0.002)	0.012**
(HA) × Firm profitability	H5c (+)	—	—	—	—	—	0.113**	(0.054)	0.010**
(HA) × Firm liquidity	H6c (+)	—	—	—	—	—	0.083*	(0.048)	0.010*
(HA) × Firm leverage	H7c (−)	—	—	—	—	—	−0.038	(0.034)	−0.007
(HA) × Brand familiarity	H8c (+)	—	—	—	—	—	−0.004*	(0.002)	−0.009*
(TE) × Firm age	H3d (+)	—	—	—	—	—	−0.008	(0.006)	−0.007
(TE) × Firm size	H4d (+)	—	—	—	—	—	0.004**	(0.002)	0.011**
(TE) × Firm profitability	H5d (+)	—	—	—	—	—	0.106	(0.104)	0.009
(TE) × Firm liquidity	H6d (+)	—	—	—	—	—	−0.065*	(0.039)	−0.008*
(TE) × Firm leverage	H7d (−)	—	—	—	—	—	0.082***	(0.030)	0.016***
(TE) × Brand familiarity	H8d (+)	—	—	—	—	—	−0.002	(0.002)	−0.005
Controls									
Victimized stakeholders[a]	—	—	—	0.002	(0.005)	—	−0.008 (0.009)	—	0.2
Victimized stakeholders[b]	—	—	—	−0.008	(0.010)	—	−0.002 (0.004)	—	0.74
Victimized stakeholders[c]	—	—	—	0[d]	—	0[d]	0[d].	—	0[d]
Third-party responsibility	—	—	—	−0.004	(0.005)	—	−0.007	(0.004)	2.69
Industry type dummies	—	—	—	—	Included	—	—	Included	—
Year dummies	—	—	—	—	Included	—	—	Included	—

* $p < 0.1$; ** $p < 0.05$; *** $p < 0.01$.
[a]Employees.
[b]Employees and customers.
[c]Customers (reference category).
[d]This parameter is set to zero because it is redundant.

In terms of control variables, we do not observe any significant effect of victimized stakeholders; the type of victimized group (customers or employees) does not seem to influence investors' reactions. Also, industry class does not display any significant effect; this result shows the generalizability of our findings across industry sectors. Furthermore, the effect of third-party responsibility is not significant, which indicates that the focal firm is considered the primary party responsible for a data breach from the investors' viewpoint.

Robustness Tests

To assure the robustness of our results, we analyzed their sensitivity to alternative computational approaches of abnormal stock returns. We computed stock returns using the Fama–French approach with equally weighted index as well as the Market Model with the GARCH (1, 1) estimation approach. The Fama–French approach estimates the expected returns and abnormal returns of each stock on each day by regressing the stock returns against the daily returns on the CRSP equally weighted index, the difference between daily returns of small and big stocks, and the difference between daily returns of high and low book-to-market stocks (Fama and French 1996). The Market Model with GARCH (1, 1) estimation approach estimates the parameters of expected returns by assuming that the residuals of the regressions of the Market Model approach can be conditionally heteroscedastic and then corrects this issue by modeling the variance of residuals as a function of the error term with a constant unconditional variance (Corhay and Rad 1997; Engle 2001).

The results of the two approaches mirrored the key results that we obtained from the Market Model approach. Table 8 shows the results of our analyses using the Fama–French approach. The results of Model 1 and Model 2 remained almost unchanged, so the impacts of financial data breaches and hacker attacks are persistent. According to Model 3, in the cases of financial data breaches and hacker attacks, the significance and direction of the moderating roles of age, size, profitability, liquidity, and brand familiarity are persistent.

Additional Analyses

It is of high practical value to investigate whether the occurrence of financial data breaches and hacker attacks can simultaneously impose more event cost on affected firms, compared to the individual occurrence of these events. Therefore, we examined the interaction effect of these two variables on abnormal returns. While this interaction is negative for both the Market Model ($\beta = -0.016$, SE = 0.008, chi-square = 3.52, $p = 0.06$) and the Fama–French approach ($\beta = -0.013$, SE = 0.01, chi-square = 1.7, $p = 0.192$), it does not consistently achieve significance across approaches. Therefore, we lack evidence to confirm with confidence that this interaction is significant. The combination of hacker attacks and breaches of financial data is not necessarily more serious than these two events considered individually.

Furthermore, we tested the impact of the number of affected victims with a subsample of our dataset for which this variable was reported (i.e., 121 cases out of 217 cases). The effect of this variable was not significant ($\beta = 0.001$, SE = 0.001, $p = 0.40$); this result is consistent with prior studies (Acquisti, Friedman, and Telang 2006; Malhotra and Malhotra 2011).

Discussion

The service literature has paid limited attention to service crises (see Malhotra and Malhotra (2011) and Gijsenberg et al. (2015) for exceptions), and it has overlooked the effects of specific crises attributes and organizational recovery resources on stock devaluation. The development of specific frameworks for service crises is important because such phenomena differ from the well-documented situations of private service failures and product-harm crises (see Rasoulian et al. (2017) for a detailed discussion). As a response, employing data breaches as an empirical context for service crises (Rasoulian et al. 2017), we present a comprehensive framework that examines the effects of crisis seriousness (outcome and process) and recovery resources on abnormal stock returns. By doing so, we also answer recent calls asking for more research at the firm level, using quantitative models and financial metrics (Khamitov, Grégoire, and Suri 2020; Van Vaerenbergh and Orsingher 2016).

Building on the literatures on service failure and crisis seriousness, our results highlight that outcome seriousness (i.e., financial data) and process seriousness (i.e., hacker attacks) have considerable effects on investors' reactions and stock valuation. In the current databank, outcome seriousness is enhanced when the breach contains financial data (H1a), whereas process seriousness is intensified for hacker attacks (H2a). Otherwise, the other categories of breach events seem much less costly for firms. Such findings shed new light on the results previously reported in this area by being more specific about the effect of different types of data breaches.

Considering organizational recovery resources, our findings suggest that, for breaches involving financial data, older (H3*a*), larger (H4*a*), more profitable (H5*a*), more liquid (H6*a*), and better-known (H8*a*) firms can attenuate the negative impact of an event. When firms possess these resources, they can recover more successfully after breaches of financial data. Our current results do not provide evidence of the buffering effect of firm leverage for breaches involving financial data. In turn, the recovery resources attenuating the effects of hacker attacks on stock devaluation are firm size (H4*c*), firm profitability (H5*c*), and firm liquidity (H6*c*). For hacker attacks, the results were not significant for the following resources: age, leverage, and brand familiarity. We do not find any attenuating moderation effect for these last three resources.

Importantly, these last nonsignificant interaction effects should be carefully interpreted by referring to the context of the study. For instance, these nonsignificant effects could be linked to the greater seriousness of hacker attack incidents compared to

financial data breaches. Indeed, our findings show that the average size of negative abnormal returns is greater for hacker attacks than for financial data breaches. This finding is aligned with prior work that argues that events targeting the functionality of firms are perceived as more serious than those targeting only the data (Goldstein et al., 2011). This last conclusion comes from the fact that interruptions in routine functionalities are more costly than other crises. In addition, we highlight that the effects of firm age and brand familiarity should not be underestimated in the context of major data breaches; these effects should be further examined with additional market-level and behavioral investigations.

Finally, the results of our control variables indicate that our findings are persistent across different industry sectors and groups of victimized stakeholders. Also, the involvement of an external contractor in a breach event does not seem to diminish the responsibility of the parent company in our databank.

Implications for Theory

Broadly speaking, the current research contributes to the literatures on service failure-recovery, crisis seriousness assessment, data breaches, and service crises. Our framework integrates the attributes of service failures (i.e., outcome and process) with the dimensions of crisis seriousness assessment (i.e., value of loss, probability of damage, time pressure, and degree of control) to determine the conditions under which a specific service crisis (in terms of data breaches) have a greater effect on stock devaluation. In addition to the determination of these conditions, our framework considers the role of organizational resources in firms' recovery process. This last aspect of our framework is important because it answers a recent call asking for more research on the "macro" and firm-level aspects of the recovery process (Van Vaerenbergh and Orsingher 2016). Accordingly, our research identifies the organizational resources that support a firm's recovery process, and the circumstances under which these resources vary in effectiveness (depending on the attributes of a crisis). In sum, we present evidence that the reactions of investors to different service crises are not identical; such reactions are influenced by different drivers, such as outcome seriousness, process seriousness, and the presence of organizational recovery resources.

We also generate new insights about the financial consequences of data breach announcements. Our framework distinguishes between the outcome and process dimensions of data breaches, and it uses this distinction to determine the seriousness of such unfortunate events. Our results indicate that data breaches that signal seriousness, in terms of outcome or process, are costly for firms. Precisely, we identify two attributes—one related to outcome (financial data) and one to process (hacker attacks)—that make data breaches more serious, in turn depreciating firms' stock value. Stated differently, we found that data breaches that signal serious crises are more costly for firms from a market-level perspective. Finally, we explain the key role of attenuation that recovery resources can play during data breaches. From an investor's standpoint, it seems that age, size, profitability, liquidity, and brand familiarity are important resources than can help firms recover from serious data breaches.

Implications for Managers

For managers, the current research highlights that service crises, such as data breaches, are not always accompanied with substantial wealth losses for shareholders. In fact, wealth losses depend on the seriousness of an outcome (i.e., financial data) or a causal process (i.e., hacker attacks). Moreover, some firm resources (e.g., age, size, profitability, liquidity, and brand familiarity) can protect shareholders' wealth and ultimately support firms' performance after service crises. Importantly, our framework can guide firms with different resources and restoration potentials to recognize the most threatening events and to take actions to prevent the occurrence of impactful service crises.

For instance, data breaches are costly for shareholders when they are caused by hacker attacks or when they involve financial data. Such conclusions hold for breaches of employees' or customers' data and for several industry sectors. These findings suggest that firms should invest massively against the occurrence of these two categories of breaches. Firms should prioritize, in term of investments, the security of their information systems to prevent hackers' intrusions. Furthermore, firms that collect the financial data of their stakeholders (e.g., credit card or bank account information) should invest in highly secure systems that enhance the confidentiality of this type of information.

Finally, firms that are smaller, less profitable, or less liquid should pay particular attention to data breaches. Such firms should consider this threat seriously since they may have difficulty recovering immediately after data breaches. Our results confirm the importance for firms to maintain a strong portfolio of resources. In our context, resources associated with firm size, profitability, and liquidity appear especially important because they attenuate the effects of both breached financial data and hacker attacks on stock devaluation.

Limitations and Further Research

Our conclusions are subject to some limitations that suggest avenues for future research. First, as is the case with other event studies, the generalizability of our study is limited to publicly traded US firms. Also, the method of an event study cannot detail the mechanism that underlies the reactions of investors to announcements in the media. We assume that relevant theories and our statistical analyses can explain the movements in firms' stock value following data breach announcements. Keeping this in mind, future behavioral studies can enhance the internal validity of our conceptual framework by using surveys, experiments, and interviews to explore how investors react to outcome or process seriousness. In addition, it would be of high theoretical and practical value to investigate the impact of data breaches on non-publicly traded firms and to investigate whether stakeholders react in a similar way in such a context. Second, future studies would benefit from testing the

applicability of our suggested framework in other crisis contexts, such as product-harm crisis or disasters and environmental crises (Dutton 1986), to examine the generalizability of our perspective.

Third, one key variable that has not been directly examined in this study is the number of breached records per event. It is worth noting that data breaches usually do not affect all stakeholders of a firm. Moreover, this variable is not always disclosed in the announcements of data breaches; that is why we did not include it in our main analyses. However, we used the number of affected victims as a proxy, and we did not find any significant effect of this variable (see the subsection "Additional Analyses"). Theoretically, we believe that a large number of breached records do not necessarily signal a major crisis. Indeed, according to crisis seriousness assessment, a large number of breached records should mainly intensify the dimension of time pressure; this unique dimension may not be sufficient to signal a serious crisis. In addition, large numbers of breached records should be correlated with the size of the corporation, which was identified as an effective attenuating recovery resource. However, we encourage future researchers to verify these speculations by including this variable in their analyses.

Fourth, we selected our six organizational resources after conducting an extensive review of previous work. We also focused on resources for which public information was available and relatively easy to collect. However, future research could benefit from extending this list by employing more recent data collection tools (e.g., web scraping, artificial intelligence, or text analysis applications). In addition, a potentially interesting resource refers to the number of distribution channels associated with a given firm. It would be interesting to examine how data breaches affect the different channels of a firm in different manners, and how channel diversity could affect firms' recuperation after serious data breaches.

Author's Note

This article is based on the second essay of the first author's dissertation. This article has been written and revised by the first author in collaboration with the second author. The third and fourth authors were the co-supervisors of this dissertation, and they initially helped the first author to identify the general topic, context, and methodology.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article. The research was funded by the Omer DeSerres Chair of Retailing at HEC, Montreal.

ORCID iDs

Shahin Rasoulian https://orcid.org/0000-0003-4362-7797
Yany Gregoire https://orcid.org/0000-0001-6939-4798

Notes

1. These two variables did not show enough variations in our databank to be included in the analyses. Out of 217 observations, 203 possessed similar transparency and control policies.
2. "Privacy Rights Clearinghouse" (accessed 10 January 2014) [available at https://www.privacyrights.org/data-breach].
3. Ir = {[(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.

References

Acquisti, Alessandro, Allan Friedman, and Rahul Telang (2006), "Is There a Cost to Privacy Breaches? An Event Study," ICIS 2006 Proceedings.

Altman, Edward I. (1968), "Financial Ratios, Discriminant Analysis and the Prediction of Corporate Bankruptcy," *Journal of Finance*, 23 (4), 589–609.

Beaver, William H. (1966), "Financial Ratios as Predictors of Failure," *Journal of Accounting Research*, 4 (1), 71–111.

Beaver, William H, Maureen F. McNichols, and Jung-Wu Rhie (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, France and Robert E. Crossler (2011), "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly*, 35 (4), 1017–42.

Benedicktus, Ray L., Michael K. Brady, Peter R. Darke, and Clay M. Voorhees (2010), "Conveying Trustworthiness to Online Consumers: Reactions to Consensus, Physical Store Presence, Brand Familiarity, and Generalized Suspicion," *Journal of Retailing*, 86 (4), 322–35.

Billings, Robert S., Thomas W. Milburn, and Mary Lou Schaalman (1980), "A Model of Crisis Perception: A Theoretical and Empirical Analysis," *Administrative Science Quarterly*, 25 (2), 300–316.

Binder, John (1998), "The Event Study Methodology Since 1969," *Review of Quantitative Finance and Accounting*, 11 (2), 111–137.

Bliss, Andy and Clive Harfield (1998), "The Threat of Computer Crime: Identifying the Problem and Formulating a Response at Force Level," *The Police Journal*, 71 (1), 25–34.

Burnett, John J. (1999), "A Strategic Approach to Managing Crises," *Public relations review*, 24 (4), 475–488.

Campbell, John Y., Martin Lettau, Burton G. Malkiel, and Yexiao Xu (2001), "Have Individual Stocks Become More Volatile? An Empirical Exploration of Idiosyncratic Risk," *Journal of Finance*, 56 (1), 1–43.

Campbell, Katherine, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou (2003), "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," *J. Comput. Secur*, 11 (3), 431–48.

Carr, Christopher L. (2007), "The Fairserv Model: Consumer Reactions to Services Based on a Multidimensional Evaluation of Service Fairness," *Decision Sciences*, 38 (1), 107–130.

Carroll, Archie B. (1991), "The Pyramid of Corporate Social Responsibility: Toward the Moral Management of Organizational Stakeholders," *Business horizons*, 34 (4), 39–48.

Cavusoglu, Huseyin, Birendra Mishra, and Srinivasan Raghunathan (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.

Coombs, W. Timothy and Sherry J. Holladay (2002), "Helping Crisis Managers Protect Reputational Assets: Initial Tests of the Situational Crisis communication theory," *Management Communication Quarterly*, 16 (2), 165–186.

Cooper, Arnold C., F. Javier Gimeno-Gascon, and Carolyn Y. Woo (1994), "Initial Human and Financial Capital as Predictors of New Venture Performance," *Journal of Business Venturing*, 9 (5), 371–95.

Corhay, Albert and A. Tourani Rad (1997), "Conditional Heteroskedasticity Adjusted Market Model and an Event Study," *The Quarterly Review of Economics and Finance*, 36 (4), 529–38.

Cowan, Arnold Richard (1992), "Nonparametric Event Study Tests," *Review of Quantitative Finance and Accounting*, 2 (4), 343–58.

Culnan, Mary J. and Pamela K. Armstrong (1999), "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science*, 10 (1), 104–15.

Culnan, Mary J. and Cynthia Clark Williams (2009), "How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches," *MIS Quarterly*, 33 (4), 673–87.

"Data Breaches/Privacy Rights Clearinghouse" (2019), (accessed November 17, 2019), [available at https://privacyrights.org/categories/data-breaches].

Dawar, Niraj and Jing Lei (2009), "Brand crises: The Roles of Brand Familiarity and Crisis Relevance in Determining the Impact on Brand Evaluations," *Journal of Business Research*, 62 (4), 509–16.

Dutton, Jane E. (1986), "The Processing of Crisis and Non-Crisis Strategic Issues," *Journal of Management Studies*, 23 (5), 501–17.

Engle, Robert (2001), "GARCH 101: The Use of ARCH/GARCH Models in Applied Econometrics," *The Journal of Economic Perspectives*, 15 (4), 157–68.

Esteve-Pérez, Silviano and Juan A. Mañez-Castillejo (2008), "The Resource-Based Theory of the Firm and Firm Survival," *Small Business Economics*, 30 (3), 231–49.

Fama, Eugene F. and Kenneth R. French (1996), "Multifactor Explanations of Asset Pricing Anomalies," *The journal of finance*, 51 (1), 55–84.

Gatzlaff, Kevin M., and Kathleen A. McCullough (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review*, 13(1), 61-83.

Gijsenberg, Maarten J., Harald J. Van Heerde, and Peter C. Verhoef (2015), "Losses Loom Longer Than Gains: Modeling the Impact of Service Crises on Perceived Service Quality Over Time," *Journal of Marketing Research*, 52 (5), 642–56.

Goldstein, James, Chernobai Anna, and Benaroch Michel (2011). An event study analysis of the economic impact of IT operational risk and its subcategories. *Journal of the Association for Information Systems*, 12(9), 606-631.

Grant, Robert M. (1991), "The Resource-Based Theory of Competitive Advantage: Implications for Strategy Formulation," *California management review*, 33 (3), 114–35.

Grégoire, Yany and Anna S. Mattila (2020), "Service Failure and Recovery at the Crossroads: Recommendations to Revitalize the Field and its Influence," *Journal of Service Research*, 1094670520958073.

Hansman, Simon and Ray Hunt (2005), "A Taxonomy of Network and Computer Attacks," *Computers & Security*, 24 (1), 31–43.

Huber, Peter J. (1973), "Robust Regression: Asymptotics, Conjectures and Monte Carlo," *The Annals of Statistics*, 1, 799–821.

Janakiraman, Ramkumar, Joon Ho Lim, and Rishika Rishika (2018), "The Effect of a Data Breach Announcement on Customer Behavior: Evidence From a Multichannel Retailer," *Journal of Marketing*, 82 (2), 85–105.

Kalaignanam, Kartik, Venkatesh Shankar, and Rajan Varadarajan (2007), "Asymmetric New Product Development Alliances: Win-Win or Win-Lose Partnerships?," *Management Science*, 53 (3), 357–74.

Karniouchina, Ekaterina V., Can Uslay, and Erenburg Grigori (2011), "Do Marketing Media Have Life Cycles? The Case of Product Placement in Movies," *Journal of Marketing*, 75 (3), 27–48.

Khamitov, Mansur, Yany Grégoire, and Suri Anshu (2020), "A Systematic Review of Brand Transgression, Service Failure Recovery and Product-Harm Crisis: Integration and Guiding Insights," *Journal of the Academy of Marketing Science*, 1–24.

Kierkegaard, Patrick (2012), "Medical Data Breaches: Notification Delayed is Notification Denied," *Computer Law & Security Review*, 28 (2), 163–83.

Larivière, Bart (2008), "Linking Perceptual and Behavioral Customer Metrics to Multiperiod Customer Profitability: A Comprehensive Service-Profit Chain Application," *Journal of Service Research*, 11 (1), 3–21.

Lewis, Barbara R. and Vincent W. Mitchell (1990), "Defining and Measuring the Quality of Customer Service," *Marketing intelligence & planning*, 8 (6), 11–17.

Linnenluecke, Martina K., Andrew Griffiths, and Monika Winn (2012), "Extreme Weather Events and the Critical Importance of Anticipatory Adaptation and Organizational Resilience in Responding to Impacts," *Business Strategy and the Environment*, 21 (1), 17–32.

MacKinlay, A. Craig (1997), "Event Studies in Economics and Finance," *Journal of economic literature*, 35 (1), 13–39.

Malhotra, Arvind and Claudia Kubowicz Malhotra (2011), "Evaluating Customer Information Breaches as Service Failures: An Event Study Approach," *Journal of Service Research*, 14 (1), 44–59.

Malkiel, Burton G. and Eugene F. Fama (1970), "Efficient Capital Markets: A Review of Theory and Empirical Work," *The journal of Finance*, 25 (2), 383–417.

Maronna, R. A., Douglas Martin, and Victor Yohai (2006), *Robust Statistics: Theory and Methods*, John Wiley & Sons, Chichester.

Martin, Kelly D., Abhishek Borah, and Robert W. Palmatier (2017), "Data Privacy: Effects on Customer and Firm Performance," *Journal of Marketing*, 81 (1), 36–58.

Martin, Kelly D. and Patrick E. Murphy (2016), "The Role of Data Privacy in Marketing," *Journal of the Academy of Marketing Science*, 45, 135–155.

McAlister, Leigh, Raji Srinivasan, and MinChung Kim (2007), "Advertising, Research and Development, and Systematic Risk of the Firm," *Journal of Marketing*, 71 (1), 35–48.

McGahan, Anita M. and Michael E. Porter (1997), "How Much Does Industry Matter, Really?" *Strategic Management Journal*, 18 (1), 15–30.

McWilliams, Abagail and Donald Siegel (1997), "Event Studies in Management Research: Theoretical and Empirical Issues," *Academy of Management Journal*, 40 (3), 626–657.

Mookerjee, Vijay, Radha Mookerjee, Alain Bensoussan, and Wei T. Yue (2011), "When hackers talk: Managing Information Security Under Variable Attack Rates and Knowledge Dissemination," *Information Systems Research*, 22 (3), 606–623.

Morrow, J. L., David G. Sirmon, Michael A. Hitt, and Tim R. Holcomb (2007), "Creating Value in the Face of Declining Performance: Firm Strategies and Organizational Recovery," *Strategic management journal*, 28 (3), 271–283.

Murphy, Deborah L., Ronald E. Shrieves, and Samuel L. Tibbs (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, Scott 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, Robert M. (2007), "A Caution Regarding Rules of Thumb for Variance Inflation Factors," *Quality & Quantity*, 41 (5), 673–690.

Opler, Tim C. and Sheridan Titman (1994), "Financial Distress and Corporate Performance," *Journal of Finance*, 49 (3), 1015–1040.

Patell, James M. (1976), "Corporate Forecasts of Earnings Per Share and Stock Price Behavior: Empirical Test," *Journal of Accounting Research*, 14 (2), 246–76.

Pearson, Christine M. and Ian I. Mitroff (1993), "From Crisis Prone to Crisis Prepared: A Framework for Crisis Management," *The Academy of Management Executive*, 7 (1), 48–59.

Perreault Jr, William D., and Leigh Laurence E. (1989). Reliability of nominal data based on qualitative judgments. *Journal of marketing research*, 26(2), 135-148.

Rasoulian, Shahin, Yany Grégoire, Renaud Legoux, and Sylvain Sénécal (2017), "Service Crisis Recovery and Firm Performance: Insights From Information Breach Announcements," *Journal of the Academy of Marketing Science*, 45, 789–806.

Rego, Lopo L., Matthew T. Billett, and Neil A. Morgan (2009), "Consumer-Based Brand Equity and Firm Risk," *Journal of Marketing*, 73 (6), 47–60.

Rifon, Nora J., Robert LaRose, and Sejung Choi (2005), "Your Privacy is Sealed: Effects of Web Privacy Seals on Trust and Personal Disclosures," *Journal of Consumer Affairs*, 39 (2), 339–62.

Romanosky, Sasha and Alessandro Acquisti (2009), "Privacy Costs and Personal Data Protection: Economic and Legal Perspectives," *Berkeley Technology Law Journal*, 24 (3), 1061–1101.

Romanosky, Sasha, David Hoffman, and Alessandro Acquisti (2014), "Empirical Analysis of Data Breach Litigation," *Journal of Empirical Legal Studies*, 11 (1), 74–104.

Romanosky, Sasha, Rahul Telang, and Alessandro Acquisti (2011), "Do Data Breach Disclosure Laws Reduce Identity Theft?" *Journal of Policy Analysis and Management*, 30 (2), 256–286.

Rousseeuw, Peter J. and Annick M. Leroy (1987), "Related Statistical Techniques," In Robust Regression and Outlier Detection, John Wiley & Sons, Inc. 248–291.

Sarkar, Kuheli Roy (2010), "Assessing Insider Threats to Information Security Using Technical, Behavioural and Organisational Measures," *information security technical report*, 15 (3), 112–133.

Schultz, E. Eugene (2002), "A Framework for Understanding and Predicting Insider Attacks," *Computers & Security*, 21 (6), 526–531.

Seggie, Steven H., David A. Griffith, and Sandy D. Jap (2013), "Passive and Active Opportunism in Interorganizational Exchange," *Journal of Marketing*, 77 (6), 73–90.

Seiders, Kathleen and Leonard L. Berry (1998), "Service Fairness: What it is and Why it Matters," *Academy of Management Executive*, 12 (2), 8–20.

Sheehan, Kim Bartel and Mariea Grubbs Hoy (2000), "Dimensions of Privacy Concern Among Online Consumers," *Journal of Public Policy & Marketing*, 19 (1), 62–73.

Smith, Amy K., Ruth N. Bolton, and Janet Wagner (1999), "A Model of Customer Satisfaction with Service Encounters Involving Failure and Recovery," *Journal of Marketing Research*, 36 (3), 356–72.

Smith, H. Jeff, Tamara Dinev, and Heng Xu (2011), "Information Privacy Research: An Interdisciplinary Review," *MIS quarterly*, 35 (4), 989–1016.

Smith, Jeffery S., Gavin L. Fox, and Edward Ramirez (2010), "An Integrated Perspective of Service Recovery: A Sociotechnical Systems Approach," *Journal of Service Research*, 13 (4), 439–52.

Smith, Jeffery S. and Kirk R. Karwan (2010), "Empirical Profiles of Service Recovery Systems: The Maturity Perspective," *Journal of Service Research*, 13 (1), 111–25.

Spillan, John and Michelle Hough (2003), "Crisis Planning in Small Businesses: Importance, Impetus and Indifference," *European Management Journal*, 21 (3), 398–407.

Spitzner, Lance (2003), "The Honeynet Project: Trapping the Hackers," *IEEE Security & Privacy*, 1 (2), 15–23.

Srivastava, Rajendra K., Liam Fahey, and H. Kurt Christensen (2001), "The Resource-Based View and Marketing: The Role of Market-Based Assets in Gaining Competitive Advantage," *Journal of Management*, 27 (6), 777–802.

Thornhill, Stewart and Raphael Amit (2003), "Learning About Failure: Bankruptcy, Firm Age, and the Resource-Based View," *Organization Science*, 14 (5), 497–509.

Tweneboah-Kodua, Samuel, Francis Atsu, and William Buchanan (2018), "*Impact of Cyberattacks on Stock Performance: A Comparative Study*," Information & Computer Security.

Van Vaerenbergh, Yves and Chiara Orsingher (2016), "Service Recovery: An Integrative Framework and Research Agenda," *Academy of Management Perspectives*, 30 (3), 328–46.

Wathne, Kenneth H. and Jan B. Heide (2000), "Opportunism in Interfirm Relationships: Forms, Outcomes, and Solutions," *Journal of marketing*, 64 (4), 36–51.

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

Wiklund, Johan, Ted Baker, and Dean Shepherd (2010), "The Age-Effect of Financial Indicators as Buffers Against the Liability of Newness," *Journal of Business Venturing*, 25 (4), 423–37.

Wiles, Michael A. and Anna Danielova (2009), "The Worth of Product Placement in Successful Films: An Event Study Analysis," *Journal of Marketing*, 73 (4), 44–63.

Author Biographies

Shahin Rasoulian is a data scientist at Manulife Financial Corporation and a post-doctoral fellow at HEC Montréal. His research interests revolve around business quantitative methods, marketing strategy, financial risk and return, and text analysis. His previous research has been published in Journal of the Academy of Marketing Science.

Yany Grégoire is a full professor at HEC Montréal, and the Chairholder of the Omer DeSerres Chair of Retailing at the same institution. He has published extensively on the issues of customer revenge, online public complaining, and service failure in major journals, including Journal of Marketing, Journal of the Academy of Marketing Science, and Journal of Service Research, among others. He is also interested in other managerial issues such as customer experience, B2B marketing, and sales. He sits on the editorial boards of several journals, including Journal of Service Research and Journal of the Academy of Marketing Science.

Renaud Legoux is Full Professor of Marketing at HEC Montréal. He holds the Professorship on big data for the arts and culture; he is also scientific director at Synapse C. Before his academic career, he worked as a manager in the cultural field. He has contributed to the publication of research on arts marketing, the marketing/finance interface and service failures in major journals, including: Journal of Marketing, Journal of Business Ethics, Journal of the Academy of Marketing Science, and International Journal of Research in Marketing.

Sylvain Sénécal is Professor of Marketing, RBC Financial Group Chair of E-Commerce, and Co-director of the Tech3Lab at HEC Montreal. His research focuses on online consumer behavior and consumer neuroscience. It has been published in journals such as Journal of the Academy of Marketing Science, Journal of Retailing, and Journal of the Association for Information Systems. Before joining academia, he held marketing positions at Arcelor Mittal.