THREE ESSAYS ON ORGANIZATIONAL DETERMINANTS OF DATA BREACH RISK

Qian WANG

PhD

The Hong Kong Polytechnic University

2021

The Hong Kong Polytechnic University
Department of Management and Marketing

Three Essays on Organizational Determinants of Data Breach Risk

Qian WANG

PhD

A thesis submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
November 2020

CERTIFICATE OF ORIGINALITY

I hereby declare that this thesis is my own work and that, to the best of my knowledge and belief, it reproduces no material previously published or written, nor material that has been accepted for the award of any other degree or diploma, except where due acknowledgement has been made in the text.

_____ _____ (Signed)

Qian WANG (Name of student)

Abstract

Given data breaches can bring firms significant financial and reputational damages, it should come as little surprise that information security has become the chief concern among corporate executives. Against this backdrop, it is important to investigate how data breach risk can be determined by organizational factors. My thesis intents to provide several new insights into this area.

The thesis includes three essays. The first essay empirically investigates two research questions: (1) How will firms' information technology (IT) innovativeness influence data breach risk? and (2) How will the relationship between IT innovativeness and data breach risk be contingent upon environmental uncertainty? I determine that firms' IT innovativeness will increase data breach risk. I further determine that the effect of IT innovativeness on increasing such a risk is mitigated if mangers are presented with high long-term incentives and is exacerbated when external environments are complex. This research is the first empirical attempt to analyze the security impact of IT innovation, highlighting the information security challenge and providing beneficial insights for organizations when they pursue proactive and innovative ITs.

In the section essay, I investigate how employee-related corporate social responsibility's (CSR) influence data breach risk. I determine that firms' employee-related CSR reduces data breach risk. I further find that the effect of employee-related CSR on reducing such a risk is pronounced when firms suffer from deteriorating economic performance, face turbulent environments, or encounter high product

similarity with their competitors. This research is among the first empirical attempts to analyze the security effectiveness of corporate CSR. Specifically, it highlights the information security benefits of employee-related CSR and provides beneficial managerial insights on making strategic decisions on these activities.

The third essay investigates (1) how firm diversity strategies influence data breach risks and (2) whether the relationship between firm diversity and data breach risk is moderated by managerial ability. I determine that firm diversity, particularly related diversity, can benefit firms by reducing their data breach risk. I also determine that the benefits of firm diversity in reducing data breach risk is exacerbated when managerial ability is high.

Acknowledgements

I would like to take this opportunity to express the deepest and sincere appreciation to all the people who helped me go through the Ph.D. journey.

First and foremost, I would like to express my heartfelt and immense gratitude to my chief supervisor, Prof. Eric W.T. NGAI, for his invaluable guidance, supervision, and support during my Ph.D. study! During the most difficult times when writing this thesis, he presented me considerable encouragement. It is absolutely impossible for me to overcome the rough road to finish this thesis without his constant guidance and help. It is my greatest honor to be one of his students.

I would like to express my immense appreciation for my BOE members, namely, Prof. Kai Lung HUI, Prof. Indranil BOSE, and Dr. Vincent CHO, for their valuable suggestions on my PhD thesis.

I would like to offer my special and big thanks to Dr. Chih-Hung PENG. He taught me a lot of valuable research techniques. He also presented me much encouragement and help during my depressed, and many constructive suggestions on my thesis.

Moreover, I would like to express the sincere appreciation to Dr. Jianghua SHEN, Dr. Lingmin XIE, and Mr. Shenyang JIANG, for their suggestions on my research and their long-term encouragement. They also provided considerable support and friendship that I needed.

I also would like to express many thanks to the talented scholars in PolyU, for their insightful suggestions on my research.

Finally, I want to express the utmost thanks to my father, Mather, and husband. I love them so much. I greatly appreciate for their constant believing in me and sticking by my side.

Contents

List of Tables

List of Figures

Chapter 1. Introduction

1.1.Introduction

Information is one of the utmost important non-tangible resources for organizations, and similar to other resources, organizations are responsible to appropriately protect it. The practice of defending information from unauthorized operations, such as access, use, theft, modification, and destruction is termed "information security" and the information that should be protected is termed "data," which is not limited in form (i.e., electronic or paper) (Whitman and Mattord 2011). Data breaches occur if confidential or private information is compromised by unauthorized parties (Sen and Borle 2015).[1]

Given the exponential growing of the volume of data and the severe business dependence upon the Internet, firms face larger-than-ever data breach risks. A variety of mega-breaches frequently make headlines all around the world. Based on the statistics from Norton, in the US, the first half of 2019 saw 3,800 breaches published and 4.1 billion records compromised, which are approximately 54 percent increase compared to the same time period of 2018.[2] Moreover, the Ponemon Institute's Cost of a Data Breach (2019) reports that, the percentage possibility of experiencing a security breach within two years had reached 29.6 percent in 2019 in the US, which increases from the 27.9 percent in 2018.[3]

[1] "Information security" is not synonyms to "IT security" and "cyber security" despite the substantial overlaps between the three terms. Information security is the general term used regardless of data form (digital or paper). IT security can be viewed as a sub-component of information security, in which digital forms of data are protected from unauthorized access. Lastly, cyber security represents the process of protecting or defending the use of cyberspace from cyber-attacks (CNSS, 2010) and intersects with information security. In particular, my thesis focuses on information security.

[2] https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html

[3] https://www.all-about-

Data breaches can bring firms serious aftermaths and are considerably expensive for firms to endure. Recent statistics (Ponemon 2019) suggest that the average cost of a data breach has reached $3.92 million, and for each compromised record, it takes a cost of $150. Beyond this, such a financial damage actually significantly underestimates the real cost of data breaches since the breaches can also tremendously damage the breached firms' brand and reputation (Gwebu et al. 2018; Janakiraman et al. 2018). Based on the Ponemon Institute's Cost of a Data Breach (2019), the average cost from customer turnover that engendered by a data breach is approximately 45 percent greater than the average total cost of such a breach.

Given the significant impact of data breaches for firms, security scholars in the past few decades have been continuously developing appropriate prevention measures. Traditionally, substantial technological measures against security threats have been proposed, such as sensitive data scanning (Shu et al. 2015), machine learning (Hart et al. 2011), collection intersection (Liu et al. 2015), and watermarking (Papadimitriou and Garcia-Molina 2011). Nevertheless, the solutions offered by these isolated improvements to technical tools are considerably limited because successful security controls should include improved techniques, enhanced security awareness, and proper enforcement of security policies (Colwill 2009). An over-reliance on technology without considering other factors can have disastrous consequences for information security.

Therefore, security scholars have recently increasingly called for further research

security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf

on data breach solutions from the organizational perspective (e.g., Cram et al. 2019; Cram et al. 2017; D'arcy and Herath 2011; Hedström et al. 2011). The extant data breach risk studies that utilizes secondary data sources have proposed several organizational determinants of data breach risks, such as information technology (IT) investment (Angst et al. 2017; Kwon and Johnson 2014; Sen and Borle 2015), managers' IT expertise (Haislip et al. 2021), information system (IS) application (McLeod and Dolezel 2018; Wang et al. 2015), and IT governance (Higgs et al. 2016; Kwon et al. 2012). However, note that the scope of the extant empirical literature on organizational determinants of data breach risk is relatively limited. Therefore, my thesis intends to further unpack the influence of organizational factors on data breach risk by utilizing secondary data sources.

To connect organizational factors to data breach risk, I direct my attention to the aspects of factors suggested by prior security research to influence firms' quality of security protection and security performance. First, IT-related factors are suggested to influence firm information security, given IT-related weaknesses and loopholes are among firms' biggest sources of security leakage (Alexander et al. 2013; Axelrod et al. 2009; Brotby 2009). Accordingly, in Essay 1 ("*Information Technology Innovativeness and Data Breach Risk: Moderating Roles of Executive Incentives and Environmental Uncertainty*"), I focus on the organizational factor of IT innovativeness, which refers to firms' propensity to adopt innovative ITs (Rogers 2003), and investigate its impact on data breach risks. I take an organizational learning perspective in the investigation, given literature has extensively investigated the impacts of IT innovations from the

organizational learning perspective (Attewell 1992; Fichman and Kemerer 1997; Jacobs et al. 2015). Based on organizational learning theory, I analyze the potential security problems in the different stages of an IT innovation. Then, on the basis of such knowledge, I investigate the following two research questions: (1) *How will firms' IT innovativeness influence data breach risk*? and (2) *How is relationship between IT innovativeness and data breach risk contingent upon long-term incentives and environmental uncertainty?* My empirical tests provide support for my hypotheses. That is, I find that IT innovativeness increases data breach risk. I further determine that while executives' long-term incentives help mitigate the effect of IT innovativeness on such risk, that complex external environments magnify the relationship between IT innovativeness and data breach risk.

Second, security research suggests that employee-related factors will influence information security, given firms' employees are constantly regarded as the "weakest link" in organizations' security equation (Bulgurcu et al. 2010; Colwill 2009; Jensen et al. 2017; Jensen et al. 2020; Lineberry 2007). Accordingly, in Essay 2 ("*Corporate Social Responsibility and Data Breach Risk: An Agency Perspective*"), the organizational determinant of data breach risk that I focus is employee-related Corporate Social Responsibility (CSR), which refers to firms' initiatives that are important to employees (Flammer and Luo 2017). In this study, I take a principal–agent perspective in theorizing since CSR literature (e.g., Crouch 2006; Ferrell et al. 2016; Flammer and Luo 2017; Krüger 2015; Petrenko et al. 2016) has extensively suggested that CSR is an important agency control mechanism to reduce agency

problems amongst shareholders. Within a principal–agent framework, I analyze how agency problems (e.g., shirking, adverse selection) lead to security concerns. Based on the knowledge, I investigate the following two research questions: (1) *How does corporate employee-related CSR influence data breach risk*? and (2) *How does negative performance, environmental dynamism, and product similarity individually moderate the association between employee-related CSR and data breach risk*? The obtained empirical results are substantially consistent with my hypotheses. That is, employee-related CSR will reduce data breach risk, particularly if organizations are operating in a loss domain, dynamic setting, or market with similar products.

Third, security research suggests that firm-structural related factors will influence firm information security (Calder and Watkins 2012; Kayworth and Whitten 2010; Peltier 2013). That is because, in the current digital era, the seamless Internet-connectivity in a firm entails information security to be controlled collaboratively among all its business units, thereby enabling firms' operating structure poses an influence on their manners of information security management. Accordingly, in Essay 3 ("*Firm Diversity, Data Breach Risks, and Moderating Role of Managerial Abilities*"), I focus on the organizational determinant of data breach risk, namely, firm diversity, which refers to firms' diversified operations in multiple industries (Tallman and Li 1996). I take a diverse learning perspective in the study given such a perspective has been extensively used to analyze the effectiveness of multiple sources of knowledge acquired (Beckman and Haunschild 2002; Hambrick et al. 1996; Schilling et al. 2003). Thus, within a diverse learning perspective, I analyze the difficulties of security

controls. Then, I analyze how the setting of multiple businesses influence firms' security controls. The investigates in this study is guided by the following two research questions: (1) *How does firm diversity influence data breach risk*? and (2) *How does managerial ability moderates the association between firm diversity and data breach risk*? The empirical results of the main analysis are highly support my hypotheses. That is, data breach risk is reduced as the level of operating diversity increases, particularly in the context of related diversified operations. Meanwhile, such a benefit of firm diversity to reduce data breach risk is strengthened when managerial ability is high.

1.2. Structure of the Dissertation

This dissertation consists of the following three studies:

- Chapter 2: *Information Technology Innovativeness and Data Breach Risk: Moderating Roles of Executive Incentives and Environmental Uncertainty*,
- Chapter 3: *Corporate Social Responsibility and Data Breach Risk: An Agency Perspective*, and
- Chapter 4: *Firm Diversity, Data Breach Risks, and Moderating Role of Managerial Abilities*.

The detailed structure of each study is summarized below.

Chapter 2 presents my first study, namely, "*Information Technology Innovativeness and Data Breach Risk: Moderating Roles of Executive Incentives and Environmental Uncertainty.*" Section 2.1 presents the introduction. In Section 2.2, I review the related literature. Then, I discuss the theoretical background, and propose

the corresponding hypotheses in Section 2.3. Section 2.4 introduces the detailed description of the data and variables, and Section 2.5 presents the empirical results. Section 2.6 concludes the study.

Chapter 3 presents my second study, namely, "*Corporate Social Responsibility and Data Breach Risk: An Agency Perspective.*" In Section 3.1, I provide the introduction. Section 3.2 reviews the related literature which is foundational to this study. I present my theoretical background in Section 3.3 and propose the hypotheses in Section 3.4. Section 3.5 provides the detailed description of the data and variables that used to test my hypotheses. Section 3.6 presents the empirical results. The last section of this chapter concludes this study with a discussion that highlights the contributions of this work.

Chapter 4 presents my third study, namely, "*Firm Diversity, Data Breach Risks, and Moderating Role of Managerial Abilities*." Section 4.1 provides the introduction of the study. The Section 4.2 briefly reviews the firm diversity and data breach literature streams. This is followed by a discussion that theorizes how firms' operating diversity can influence likelihood of data breaches, and how managerial ability moderates such an influence. Section 4.4 discusses the data and variables. Section 4.5 presents the empirical results. Section 4.6 concludes this study and discusses implications for research and practice.

Chapter 2. Information Technology Innovativeness and Data Breach Risk: Moderating Roles of Executive Incentives and Environmental Uncertainty

2.1.INTRODUCTION

"Emerging technologies frequently have unintended consequences, or may create one problem even as they solve another."

(Ransbotham et al. 2016, p. 1)

In this digital era, firms have accelerated implementation of technology advancements (e.g., Internet of Things, mobility, and cloud computing) to compete in intense markets (Mithas and Rust 2016; Trantopoulos et al. 2017; Vial 2019). Although the implementation of innovative ITs presents profit opportunities for firms, such digital transformation also brings firms a number of challenges, one markedly crucial among which is information security (Hanelt et al. 2020; Qian et al. 2012; Sheng et al. 2008). For example, numerous firms have adopted cloud technologies to enhance their business operations. However, such a technology adoption has added billions of unsecure devices to these firms' network as well as considerably complexity to their operations (Singh and Malhotra 2015). Consequently, the benefits of such a cloud transformation have been accompanied by a range of security failures, such as, cyber-attacks, employee data theft, and loss of devices (Esposito et al. 2016; Takabi et al. 2010). Evidence from practical studies has further confirmed this phenomenon, with the Ponemon Institute (2020) reporting indicates that 82% of firms having experienced more than one data breach because of technology-driven transformation.[4]

[4] https://get.cybergrx.com/ponemon-report-digital-transformation-2020/

According to another survey by Fortinet (2018), 85% of chief information security officers regard security issues related to introducing technology applications as having a marked, significant, influence on their firms' data and physical security.[5]

Given evidence of such a close linkage between firms' technology innovations and security threats, there is a need to theoretically and empirically examine the relationship between the two aspects. However, to my knowledge, such research has been nearly disregarded by prior work, thereby suggesting that opportunities exist for the related investigations. In particular, note that ITs have become remarkably integrated into firm operations from web presence to back-end systems in the current digital era (Fichman 2001; Rogers 2003). In such *integrated and seamlessly-connected* technology environments, a vulnerability in any technology may jeopardize an entire enterprise IT system for failure, thereby remarkably distorting the boundaries of the security influence of any IT. Consequently, I focus on firm IT innovativeness, which refers to firms' propensity for IT innovations across a composite of multiple technologies (Rogers 2003), and investigate how it poses threats to firms' information security. Accordingly, I propose my first research question: (1) *How does firm IT innovativeness influence data breach risk (i.e., the likelihood of experiencing a data breach)*?

The interplay between IT innovativeness and information security is complex and multifold. Firms may *superficially* benefit in the security aspect from their IT innovations by realizing specific security protection function, improved capabilities in

[5] https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/Fortinet-2018-Security-Implications-of-Digital-Transformation-Report.pdf

computing speed, and data storage expansion (Bharadwaj 2000; Chae et al. 2014). However, their introduction of such digital and technological advancements leads to a surge in complex operations, requirement uncertainty, security-related workload, and network access which affords new entry points of attack (D'Arcy et al. 2014; D'Arcy and Teh 2019), thereby implying substantial internal and external security threats that may plague IT innovative firms.

To theoretically unpack the tension between firm IT innovativeness and information security performance, I draw on organizational learning theory (Huber 1991; Levitt and March 1988). Such a theory suggests that firms' insufficient organizational learning will lead to unfavorable operational performance, and has long emphasized the concepts of "knowledge barrier" and "learning burden" created by IT innovations (Attewell 1992; Fichman and Kemerer 1997; Jacobs et al. 2015). Drawing from the theory and certain common natures that inherently and universally present in IT innovations (e.g., IT-fashion, esoteric, digitalized, and newness), I propose that IT innovations can lead to firms' security knowledge barrier and security threats because of four security problems: (1) *uncertain security adoption*, (2) *error-prone routines*, (3) *insufficient external reference*, and (4) *more sources of leakage*. High IT innovative firms will particularly experience an extensive level of these security problems, thereby leading to high-level security vulnerabilities.

To understand the contextual factors and to test the causal mechanisms at play, I also consider a series of contextual factors that moderate this primary relationship. The efficiency of organizational learning processes is conditional on firms' internal (Carley

1992; Vera and Crossan 2004) and external (Jacobs et al. 2015; Sinkula 1994) contexts. Hence, I test the contingency perspective of organizational learning by introducing internal (i.e., *long-term incentives to leaders*) and external (i.e., *environmental uncertainty*) contingency factors into my models. Exploration in this aspect is guided by a second research question: (2) *How do long-term incentives and environmental uncertainty individually moderate the influence of IT innovation on data breach risk*?

In sum, within an organizational learning framework, I present a series of predictions on how firms' IT innovativeness (or *propensity for IT innovations*) influences their data breach risk and how this influence is contingent on other factors. Empirical tests are based on a unique longitudinal data set that contains 3,061 firm-year observations of listed firms in the U.S. across a four-year period (2012–2015). I adopt a systematic research design and conduct a comprehensive list of tests to unpack the impact of firms' IT innovativeness on data breach risks. Consistent with my expectation, I find that firms' IT innovativeness will increase data breach risk. Delving into such a relationship and in line with the theoretical evidence that the efficiency of organizational learning processes is conditional on firms' internal and external contexts (Carley 1992; Sinkula 1994), I find that the relationship between IT innovativeness and data breach risk is mitigated if leaders are long-term orientated and exacerbated when external environments are complex.

This research advances the literature primarily in three ways. First, although the positive aspects of firms' IT innovation adoptions have attracted extensive interest (Bharadwaj 2000; Karahanna et al. 2019; Saldanha et al. 2020), this study empirically

demonstrates the potential information security-related "dark side" of IT innovation. Thus, this research provides new insights into the existing IT innovation literature by introducing a novel operational outcome (i.e., data breach risk) that may accompany firms' IT innovation adoptions, and that sits outside of the traditional economic outcomes considered in the extant IS (Bharadwaj 2000; Karahanna et al. 2019; Mithas and Rust 2016), operations management (Bala 2013; Nagle 2019), or strategy (Chun et al. 2015; Koellinger 2008) research. Furthermore, given that firms have accelerated their digital transformation pace in the current digital era, my findings help complete their understanding of the potential risks of digital technology adoptions and caution firms to pay attention to information security in such a transformation journey.

Second, this study extends the limited scope of the information security research by shedding light on the security impact of a new organizational factor, namely, IT innovativeness. While many cybersecurity studies have directed attention to individuals' actions as posing security risk or firm policy as mitigating such risk, they are generally in an individual-level (Cram et al. 2017; Moody et al. 2018) and the extent organizational-level studies that investigate determinants of data breaches have been significantly limited in scope. Given the research gap, I pioneeringly direct attention to potential negative security impact of firms' overall propensity for IT innovations. By doing so, I extend and provide new insights that connect the broader organizational context to information security and data breach risk, thereby extending the limited research in the realm. In addition, I advance the security literature by applying organizational learning to offer rich theoretical explanation for why IT

innovations are replete with security vulnerabilities.

Finally, by providing a fine-grained look at the contingencies that intervene IT innovativeness and data breach risks, this research is among the first to empirically analyze how the interplay of firm internal and external contexts can influence security threats tied to IT innovations. I demonstrate that impact of IT innovativeness on data breach risk vary with firms' managerial and environmental factors. The findings help me gain insight into whether the security impact of IT innovations is most evident in certain conditions, and such findings also resonate with the extant insights from organizational learning literature (e.g., Jacobs et al. 2015; Vera and Crossan 2004), which suggests that certain organizational contexts and external uncertainties synergistically combine to further influence learning effectiveness.

2.2.Literature Review and Research Background

Data breaches, alternatively called IT security failures (Kwon and Johnson 2014), IT security breaches (Garg et al. 2003), or information security breaches (Kwon et al. 2012), are considered malicious or accidental leakages of confidential or private information to unauthorized parties (Cheng et al. 2017b; Sen and Borle 2015). As firms continuously turn to digitalization, their volume of data is increasing and their devices are increasingly connected through networks and the Internet. Thus, they actually face larger-than-ever risks of experiencing data breaches.[6] The consequences of data breaches can be extremely devastating through networks and the Internet, such as large

[6] https://www.ibm.com/downloads/cas/ON8MVMXW

financial penalties (Baldwin et al. 2017; Solove and Citron 2017), damage to brand and reputation (Gwebu et al. 2018; Janakiraman et al. 2018), disruption of productivity (Hilary et al. 2016; Makridis and Dean 2018), and decreases in stock values (Benaroch et al. 2012; Kamiya et al. 2020).

Data breaches can have internal (e.g., data theft by insiders or accidental disclosure) and external (e.g., virus, hacking, social engineering attacks, and malware) sources (Cheng et al. 2017b). Although data breaches that have historically made the news are commonly carried out by malicious outsiders, external data breach threats are relatively amenable to traditional security countermeasures (e.g., antivirus software, intrusion detection systems, and firewalls) (Colwill 2009; Cram et al. 2019). On the contrary, threats that originate from firm insiders are considerably more complex and difficult to defend against by merely adopting any one-size-fits-all security solutions (Bulgurcu et al. 2010; D'Arcy et al. 2009; Herath and Rao 2009a; Vance et al. 2013). The reason is that internal employees can easily use their intimate knowledge, physical proximity, and privileged access to firms' information to cover their tracks in order to steal sensitive information for personal profit (Colwill 2009).

Therefore, information security, apart from being a technical issue, is an operational and managerial issue as well. However, despite the long-existing calls for the research on data breach solutions from the organizational and managerial perspective (e.g., Cram et al. 2019; Cram et al. 2017; D'arcy and Herath 2011; Hedström et al. 2011), my review of prior studies (see Table 2.1) suggests that the extant literature that investigates the organizational or managerial determinants of data

breach risk remains relatively limited in terms of scope. Existing studies have proposed only a few organizational determinants: IT security investment (Angst et al. 2017; Kwon and Johnson 2014; Sen and Borle 2015), IT governance (Higgs et al. 2016; Liu et al. 2020), IT application (Wang et al. 2015), and social-facing activities (D'Arcy et al. 2020). Evidently, the number is incommensurate with the significance of data breach. As a result, my study intends to improve extant studies by focusing on a novel determinant of data breach, namely, *IT innovativeness*.

Table 2.1. Empirical Research on Organizational Determinants of Data Breach Risk

Literature	Organizational Determinant	Theoretical Background for Effect	Main Findings
Sen and Borle (2015)	IT security investment	Opportunity theory of crime, institutional anomie theory, and institutional theory	• Investment in IT security is correlated with an increased risk of data breach within state and industry sectors. • The strictness of state-level data breach disclosure laws significantly impacts data breach risk in the financial, educational, and medical industries and for the non-governmental organization sector.
Kwon and Johnson (2014)	IT security investment	Organizational learning theory	• Proactive security investments are positively related with data breach risk. • Proactive investments are more cost effective in healthcare security than in reactive investments
Angst et al. (2017)	IT security investment	Institutional theory	• IT security investment is not directly associated with data breach risk. • Institutional factors create conditions under which IT security investments can play a role in reducing data breach risk.
Higgs et al. (2016)	IT governance	Signaling theory	• Firms with technology committees are likely to be involved in reported breaches compared with those without.
Wang et al. (2015)	Features of IT applications	Routine activity theory	• The IT applications with large value, little application controls, high visibility and accessibility, and rare protection measures are highly likely to be targeted.
Mcleod and Dolezel (2018)	Technical facilitates, and organizational factors	Not specifically indicated	• Several technical facilitates (e.g., EMR system, neonatal intensive care unit, lab barcoding, and health information exchange initiative) are highly likely to experience data breaches. • Several organizational factors (e.g., Number of birth, staff beds, and surgical operations) is positively associated with the occurrences of data breaches.
D'Arcy et al. (2020)	Social performance	Shareholder theory	• Firms' peripheral social performance (e.g., philanthropy, community relations) tends to result in an elevated likelihood of data breaches. • Firms that are noted to have poor social performance records are with a reduced likelihood to experience a data breach. • Firms that simultaneously have peripheral social performance strengths along with high social performance concerns in other areas are at increased risk of breaches.
Liu et al. (2020)	IT governance	Not specifically indicated	• Universities with centralized IT governance experience a reduced number of data breaches. • Such an effect is moderated by the heterogeneity of universities, university type, and research intensity.
Haislip et al. (2021)	Executives' IT skills	Not specifically indicated	• Executives with IT expertise are associated with fewer data breach risks.

The present study focuses on IT innovativeness, which is an aggregated measure for IT innovations rather than a specific type of innovative technology. That is because, firms' systems are operated in highly collaborated and Internet-connected means, thereby remarkably distorting the boundaries of the security influence of any innovative IT. In this environment, similar to the case in which a hacker can move laterally through an entire firm's network once gaining access, the weakest point of one technology may also become the largest security vulnerability of another technology. In terms of the phenomenon, Rogers (2003, p. 15) commented that "past diffusion research generally investigated each innovation as if it were independent from other innovations. This simplification represents a dubious assumption…." Fichman (2001) similarly emphasized that ITs have become remarkably integrated, and he also empirically determined that such aggregated IT innovation measures across a class of technologies will "promote strong robust and generalization and can promote stronger predictive validity" (p. 427). Taken together, the afore-mentioned pieces of evidence all supports the necessity to consider firms' innovativeness across a composite of multiple technologies in the present study. In line with prior literature (e.g., Rogers 2003),[7] I here defined firms' IT innovativeness as firms' propensity for IT innovations, which are new to organizations and relative to their competitors.

In reviewing the IT innovation literature, I note that IT innovation literature has

[7] IT innovativeness has been defined in different ways in the organizational literature. Hurley and Hult (1998) defined innovativeness as firms' openness toward innovations and measured such an openness as the number of new technologies accepted by firms. Bennett (1969) delineated innovativeness as a measure of how soon an individual or organization adopts a technology after its initial appearance. Bell (2005) and Damanpour (1991) defined innovativeness as firms' capability to introduce innovative technologies. In addition, Rogers (2003) explained innovativeness as the degree to which organizations are proactive at adopting technologies.

left unexplored how firms' IT innovations influence information security. Such a lack of attention is alarming because information security issues have become particularly salient when firms use emerging technologies to achieve digital transformation in their operations (Fortinet 2018).[8] Entering the unique year of 2020, the COVID-19 pandemic has forced firms worldwide to accelerate their pace to innovate and digitalize business and operations (Soto-Acosta 2020). However, such a rapid pace of digital acceleration has strained firms' security protections, as evidenced by a substantial increase in data breaches in this period.[9] Given such a close linkage between firm digital transformation and security threats, my research complements and extends the literature by explaining why and how firm propensity for IT innovations pertains to information security.

2.3.THEORETICAL FRAMEWORK AND HYPOTHESIS DEVELOPMENT

2.3.1. Organizational Learning Theory

The organizational learning framework helps to explain the relationship from IT innovativeness to data breach risks. Organizational learning theory represents a classical theory in organizational behavioral studies (Argote and Miron-Spektor 2011; Fiol and Lyles 1985; Huber 1991; Levitt and March 1988). This theory posits that organizations are considered entities of routines, such as procedures, policies, cultures, rules, norms, strategies, and conventions. The theory posits what firms learn to

[8] https://www.fortinet.com/demand/gated/Fortinet-2018-Security-Implications-of-Digital-Transformation-Report?utm_source=blog&utm_campaign=2018-q3-ciso-digital-transformation-report

[9] MonsterCloud (https://monstercloud.com/) reports that reports that ransomware attacks are up 800% during the COVID-19 pandemic.

improve outcomes becomes organizational knowledge (or simply knowledge), which is stored in a variety of routines that guide future organizational behaviors.

Organizational learning can proceed through multiple approaches. First, the *learning-by-doing* approach is widely accepted by scholars to interpret organizations' learning effort. This approach describes how organizations can learn from and implement changes in response to direct operational experiences (Levitt and March 1988; March 1991). That is, by encoding history inferences and experiences into routines, firms can accumulate knowledge to show effectiveness and promote successful outcomes. Through a series of transmitting behaviors, such as socialization, imitation, personnel movements, and education, acquired knowledge can also be accessed by organizational members who have yet to personally learn from experiences (Levitt and March 1988).

The learning-by-doing approach focuses on learning and acquiring knowledge within the organizational boundary; however, organizations can also learn by absorbing knowledge outside the organizational boundary through *learning-about* (Huber 1991; Wang and Ramiller 2009), which represents the second organizational learning approach. This approach indicates that learners can gain knowledge by making sense of available information (e.g., websites, books, rivals' experiences, trading partners, or consultancies) from sources outside organizations. That is, a learner can obtain the required knowledge by understanding information derived from what others have said, written, or experienced. In particular, Levitt and March (1988) described a notion that is similar to the learning-about approach as "ecologies of

learning," in which organizations can learn "*in an environment that consists largely of other collections of learning subun*its" (p. 331).

Although the learning-by-doing and learning-about approaches are defined separately, these methods are closely related. That is, whether organizations acquire knowledge through learning-by-doing or learning-about, knowledge is incrementally encoded into routines that guide behaviors that lead to favorable outcomes (Argote and Miron-Spektor 2011; Fiol and Lyles 1985; Levitt and March 1988). By contrast, firms' deficiency in organizational learning result in knowledge barriers and potentially unfavorable operational outcomes (Huber 1991; Tatikonda and Montoya-Weiss 2001).

2.3.2. Security Learning in IT Innovation

Firms' IT innovation adoptions disrupt the firms' original security equilibrium and raise new security vulnerabilities and learning contents. Security learning should pervade each IT innovation journey of firms to reduce their security knowledge barrier (Attewell 1992; Fichman and Kemerer 1997). Prior studies have suggested two main phases in an innovation process: *pre- IT adoption* (or initiation) and *post- IT adoption* (or implementation) phases (Rogers Everett 1995; Zaltman et al. 1973). I respectively analyze the involved aspects of security learning in either of the phases.

In the *pre-IT adoption* phase, an IT innovation has yet to become an organizational reality. By collecting and interpreting information from external environments, organizations can shape the preliminary attitude or stance toward security aspects that are involved in the technology (Fichman and Kemerer 1997). In

this phase, security learning in terms of ITs may involve the following contents:

- potential security vulnerabilities that can accompany new IT applications,
- countermeasures (e.g., regulatory policies and standards, technological tools, or security training) that can help mitigate security vulnerabilities,
- compatibility and interoperability of new technologies with the extant corporate security cultures and routines, and
- difficulties in mastering the operations in new technologies.

Note that organizational learning in this phase is mainly conducted through the *learning-about approach* by absorbing experience and knowledge from external sources (Wang and Ramiller 2009). A sufficient and effective accumulation of security knowledge through the learning-about approach before IT innovation adoptions will reduce the security knowledge barrier in making adoption decisions (Huber 1991; Stock and Tatikonda 2008; Tatikonda and Rosenthal 2000), thereby benefiting adopters to make wise preparations for potential security threats.

In the *post-IT adoption* phase, routines change when IT innovations have started to be materially recognized. That is, software and hardware are installed, and as the project life cycle progresses, business procedures are changed, employees are trained, awareness is updated, and related policies are enforced (Fichman and Kemerer 1997). The involved security learning mainly pertains to the following aspects:

- learning to adapt to new security routines (e.g., procedures, rules, systems, and regulatory policies) by learning new knowledge and operations,
- identifying security vulnerabilities in productions and operations,

- developing countermeasures to patch vulnerabilities and harden systems,
- logging security errors to avoid similar or repeat mistakes, and
- consolidating and disseminating organizational security awareness.

In particular, security learning in this phase is primarily conducted through the *learning-by-doing approach* by accumulating security knowledge within the organizational boundary (Argote and Miron-Spektor 2011). Beyond this aspect, the *learning-about approach* can also facilitate the advancement of learning through learning-by-doing (Levitt and March 1988). For example, an IT innovation adopter may encounter a new security problem that accompanies an innovative IT application. Apart from learning from experiences, the adopter could also consult external consultants regarding the threat. Learning obtained from either avenue can further guide the adopter's operations against the threat.

2.3.3. IT Innovativeness and Data Breach Risk

Nevertheless, security learning in IT innovation is vulnerable to a set of security problems which may engender security knowledge barrier and promise data breach threats. Fundamentally speaking, each of these problems inherently resides in the specific *common* nature of IT innovations. These security problems are discussed as follows.

First, given the *fashion-driven* nature of IT innovations (Swanson and Ramiller 2004; Wang and Ramiller 2009), IT innovation adopters may suffer from the security problem of *uncertain security adoption* prior to IT adoption. That is, the emergence of

an IT fashion will likely prompt organizational leaders to view an IT innovation as an efficient solution to key enterprise problems. Therefore, *firm leaders tend to promote technology adoption following a "me-too" trend but with insufficient deliberation on the potential security vulnerabilities and difficulties* (Abrahamson 1996). The direct consequence for the organization is that the new technology may be incompatible with organizations' remaining security routines or extremely difficult to handle, thereby presenting high-level security threats upon implementation (Cram et al. 2019; D'Arcy et al. 2014; D'Arcy and Teh 2019). *From the organizational learning perspective*, this problem can be viewed as insufficient security learning through the learning-about approach in the pre-IT adoption phase, thereby engendering a considerable security knowledge barrier. In particular, this security problem echoes the organizational learning concept of "superstitious learning;" that is, top executives provide an enthralling discourse to promote certain innovations as efficient solutions to important organizational problems but actually overestimate the organizations' abilities to control the accompanying risks (Levitt and March 1988).

Second, adopters in the post- IT adoption phase may face the security problem of *error-prone routines*, which are subject to the *esoteric* and *transformative* nature of IT innovation (Fleming 2001; King et al. 1994). That is, the adopters may encounter serious knowledge barriers between what they know and what the technology needs them to know upon IT implementation (Jacobs et al. 2015). Meanwhile, security routines (e.g., procedures, policies, or norms) in regard to the new technology are underdeveloped and jeopardize favorable security outcomes. This situation is further

confounded since IT infrastructures and services are commonly complex and not well understood (Stock and Tatikonda 2008). *From the organizational learning perspective*, this problem is caused by the adopters' insufficient security learning through either the learning-by-doing or learning-about approach in the implementation phase, and consequently, significant security knowledge barriers can lead to unfavorable security outcomes.

Third, fundamentally derived from the *innovative* and *newness* natures of IT innovation (Fleming 2001; Tatikonda and Montoya-Weiss 2001), adopters in the post-IT adoption phase may face the security problem of *insufficient external reference*. This is because, innovative ITs have yet to be pervasively diffused, and thus, the industry-wide discovery of their weak points is limited (Mitra and Ransbotham 2015). Consequently, firms' security professionals encounter difficulty in comprehensively keeping track of the threats to and vulnerabilities of IT innovations. In addition, collective safeguards (e.g., vulnerability management programs and software patching processes) for innovative technologies tend to be insufficiently developed, thereby providing additional potential for malicious actors to break firms' defenses (Angst et al. 2017). *From the organizational learning perspective*, this problem can be regarded as the insufficiency of security knowledge accumulation (i.e., security knowledge barrier) at an environmental level. Thus, external sources are limited and rare for IT adopters and inhibit learning that protects systems and improves security routines.

Fourth, given the *digital* and *Internet-connected* nature of IT innovations (Fichman 2004; Rogers 2003), IT innovation firms in the post-IT adoption phase may

suffer from the security problem of *increased sources of leakage*. This problem of IT innovations is caused twofold, namely, *intensive information* and *widened attack surface*. First, a surge of firm data processing, collection, storage, and analysis needs emerge upon new IT implementations (Gurbaxani and Whang 1991). As previously argued, operations in data activities that make up the new technology are prone to security threats, and therefore, such *intensive data activities in the context of IT innovations* will understandably increase information leaking possibilities. Second, firms' IT innovations will bring new IT applications into their infrastructure and systems, thereby leading to a *widened attack surface* and increased leakage sources (Gruschka and Jensen 2010).

Table 2.2 presents the four potential security problems of IT innovations (i.e., uncertain security adoption, error-prone routines, insufficient external reference, and increased sources of leakage). Each security problem represents a source of security knowledge barriers because of insufficient security learning and yields a certain level of security vulnerabilities of IT innovations. An integration of the four security problems leads to an increased security threats that accompany IT innovations. Therefore, the security problems and security threats encountered by highly innovative organizations are accentuated. The following hypothesis is presented on the basis of the preceding discussions:

HYPOTHESIS 2-1 (H2-1). *IT innovativeness is positively associated with data breach risks.*

Table 2.2. Security Problems of IT Innovations

IT Innovation Phase	Security Problem	Source IT Innovation Natures	Reasons of Security Knowledge Barrier	Accompanying Information Security Threats
Pre- IT adoption	*Uncertain security adoption*	• IT-fashion (Swanson and Ramiller 2004; Wang and Ramiller 2009)	Insufficient security learning-about prior to adoption	• Incompatible security routines • Difficult to master
Post- IT adoption	*Error-prone routines*	• Esoteric • Transformative (Fleming 2001; King et al. 1994)	Insufficient accumulation of security learning.	• Prone to maloperation • Prone to maladaptation
	Insufficient external reference	• Innovative • Newness (Fleming 2001; Tatikonda and Montoya-Weiss 2001)	Insufficient security learning sources	• Difficult to catch vulnerabilities • Weak safeguards
	Increased sources of leakage	• Digitalized • Internet-connected (Fichman 2004; Rogers 2003)	More security vulnerabilities	• Increased sources of information leaks

2.3.4. Moderators: Managerial Ability and Environmental Uncertainty

I have theoretically predicted the potential impact of firm IT innovativeness on data breach risk. Despite the theoretical justifications and corresponding prediction, I understand that no unconditional or universal relationship exists (Donaldson 2001; Drazin and Van de Ven 1985). Thus, I use a contingency perspective germane to organizational learning (Carley 1992; Gnyawali and Stewart 2003; Sinkula 1994; Vera and Crossan 2004) and consider the following internal and external contingency factors respectively: long-term incentives and environmental uncertainty.

2.3.4.1.Moderating Role of Long-Term Incentives

I consider the moderating role of *long-term incentives* to leaders from an internal contingency perspective. The reasoning is that leaders are "the guiding forces behind organizational learning" (Vera and Crossan 2004, p. 222), and their time preference can directly determine their incentives to proactively search for information and facilitate organizational learning (Amit 1986; Flammer and Bansal 2017; Flammer and Kacperczyk 2016; Lin et al. 2019).

Firm leaders tend to be myopic and hold a "here-and-now" mindset in decision

making (Eisenhardt 1989). Firms can foster top mangers' long-term orientation by providing long-term incentives, such as linking compensation to firms' long-run performance (Carpenter and Sanders 2004; Currim et al. 2012; Flammer and Bansal 2017; Seo et al. 2015). Long-term oriented managers may have a high propensity to focus on factors that may remotely affect the firms' future. Consequently, they are highly likely to engage in a thorough information processing going beyond the vicinity of the problems on hand in making decisions (Carpenter and Sanders 2004; Currim et al. 2012; Flammer and Bansal 2017; Wang and Bansal 2012). Lin (2019) empirically determined that long-term orientated managers are associated with a high comprehensiveness in decision-making.

Focusing this rationale into my context (i.e., IT innovation and security), given the security investments to prevent the occurrences of future failures and tend to be unable to materialize in the short run (Colwill 2009), such investments should be regarded as long-term orientated. It is reasonable to expect that the managers with sufficient long-term incentives have high motivations to further focus on information security issues and have a high tendency to create a long-term information security environment in the pre- and post- IT adoption phases. That is, they are highly likely to proceed with a comprehensive security-related information searching to avoid long-run security concerns that accompany firms' IT innovations. Consequently, I expect that security problems of IT innovation ameliorates in this situation, thereby weakening the influence of corporate IT innovativeness on data breach risk. Thus, I propose the following hypothesis:

HYPOTHESIS 2-2 (H2-2). *High long-term incentives weaken the relationship between corporate IT innovativeness and data breach risk.*

2.3.4.2.Moderating Role of Environmental Uncertainty

I analyze the moderating role of environmental uncertainty from the environmental contingency perspective, given management scholars have extensively suggested that firms' external environment significantly influences the efficiency of

organizational learning (Argote and Miron-Spektor 2011; Jacobs et al. 2015; Jansen et al. 2006; Ojha et al. 2018; Sinkula 1994). Duncan (1972) particularly identified two dimensions of environmental uncertainty, namely, environmental dynamism and complexity. Such a two-dimensional topology of environment has been extensively adopted by the later research (e.g., Bourgeois III 1980; Jansen et al. 2006; Tian and Xu 2015). Thus, I follow these studies and discuss the moderating role of environmental uncertainty along both the dimensions (i.e., environmental dynamism and complexity).

Environmental Dynamism. Environmental dynamism refers to the volatility, unpredictability, and instability prevalent in firms' external environments (Dess and Beard 1984; Keats and Hitt 1988). Jansen et al. (2006, p. 1664) described dynamic environments as being characterized by "*changes in technologies, variations in customer preferences, and fluctuations in product demand or supply of materials.*"

I postulate that environmental dynamism will exacerbate the security problems of IT innovativeness from three aspects. First, Mendelson and Pillai (1998) found that technological changes in a highly dynamic environment occur at a rapid pace and with a significant magnitude. Such extensive and accelerated IT changes will compel firms to accept IT innovations even in an unprepared manner to minimize the threat of obsolescence (Sabherwal et al. 2019; Tushman and Anderson 1986), thereby reducing the IT innovative firms' time and attention to search security information before the adoptions. Therefore, in this environment, the uncertain security adoption problem of IT innovation magnifies.

Second, a dynamic environment will likely complicate firms' operational change assessments, and impact forecasts (Azadegan et al. 2013; Milliken 1987; Sabherwal et al. 2019). Thus, firms' operational uncertainties in adapting new ITs are further aggravated. This situation may be further complicated with insiders' increased levels of stress and anxiety caused by considerable environmental ambiguity (Jansen et al. 2009; Waldman et al. 2001), since highly stressful employees tend to be associated

with considerable negligence when operating new ITs, and they are also relatively incapable of dedicating persistent and effortful security learning to reduce security barriers (Ratnawat and Jha 2014). Therefore, the *error prone routines* problem of IT innovation magnifies in situations in dynamic environments.

Third, under relatively unstable environments, firms face immense information-processing requirements and heavy IT-related workload (e.g., intensive business information update) caused by highly dynamic customer needs and fluctuated product demand (Sabherwal et al. 2019; Tian and Xu 2015). This condition exacerbates the security problem of *increased sources of leakage* upon IT adoptions.

In summary, security problems of IT innovations amplify when external environments are highly dynamic. Hence, the relationship between IT innovativeness and data breach risk is positively moderated. Thus, I formulate the following hypothesis:

HYPOTHESIS 2-3 (H2-3). *High environmental dynamism strengthens the relationship between corporate IT innovativeness and data breach risks.*

Environmental Complexity. Complexity originates from the diversity of external competitors that a firm should cope with (Dess and Beard 1984; Keats and Hitt 1988). High heterogeneity of competitors indicates increased environmental complexity, where firms encounter numerous competitors. Correspondingly, "intensive competition" represents a salient feature of complex environments (Xue et al. 2012).

I contend that the presence of environmental complexity strengthens the security problems of IT innovations for a number of reasons. First, fierce competition compels firms to be aptly agile to respond to competitors' initiatives and remain ahead of the competition (Milliken 1987). Thus, firms in the environment *face enormous pressure* to be IT innovative to boost competitiveness and to maintain their competitive advantage, resulting in a high tendency to disregard considerable security knowledge barriers they encounter when preparing to adopt new ITs. Thus, the *uncertain security adoption* problem of IT innovation is highly serious for such firms.

Second, firms in complex markets have complex inputs (e.g., venders) and outputs (e.g., customers) (Dess and Beard 1984). Multiple inputs and outputs and firms' complex interrelationships increase the types of security routines in IT operations, thereby increasing the complexity and uncertainties of security learning (Daft and Macintosh 1981; Tushman and Nadler 1978). Consistent with the comment of Schneier (2015, p. 354) that "Complexity is the worst enemy of security," I argue that employees in complex environments tend to experience additional operational difficulties and complexities in securely implementing new ITs. Hence, *error-prone routines* problem of IT innovation is heightened.

Third, Keats and Hitt (1988) indicated that in highly complex environments, the organizational information processing requirement increases with the number and heterogeneity of industry competitors and high uncertainties. Thus, when innovative IT are adopted in highly complex environments, firms' information workload tends to further increase. In the situation, the *increased sources of leakage* problem of IT innovation intensifies.

To summarize, security problems that typically accompany an IT innovation intensifies when external environments are highly complex. This situation positively moderates the relationship between IT innovativeness and data breach risks. Accordingly, I propose the following hypothesis:

HYPOTHESIS 2-4 (H2-4). *High environmental complexity strengthens the relationship between corporate IT innovativeness and data breach risks.*

Table 2.3 summarizes the examined moderators and their respective moderating mechanisms (i.e., intervening security problems).

Table 2.3. Moderating Mechanism

Contingency Perspective	**Hypothesis**	**Moderator**	**Intervening Security Problems (be weakened/be strengthened)**
Internal	*H2-2*	*Long-Term Incentives*	• Mindless adoption (*be weakened*) • Error-prone routines (*be weakened*) • Insufficient external reference (*be weakened*)
External	*H2-3*	*Environmental Dynamism*	• Uncertain security adoption (*be strengthened*) • Error-prone routines

			(*be strengthened*) • *Increased sources of leakage* (*be strengthened*)
	H2-4	*Environmental Complexity*	• Uncertain security adoption (*be strengthened*) • Error-prone routines (*be strengthened*) • *Increased sources of leakage* (*be strengthened*)

Figures 2.1 illustrates my conceptual model.

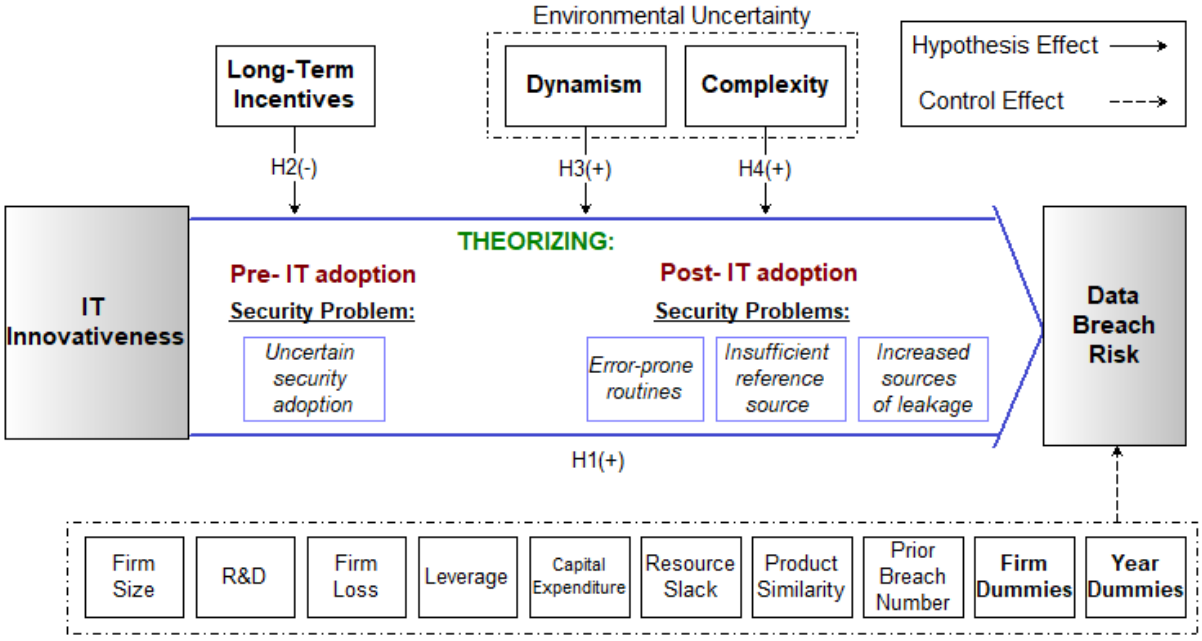

Figure 2.1. Research Conceptual Model

2.4.DATA AND VARIABLES

2.4.1. Data Description

To test the research model, I compiled a variety of data from five primary public sources. These public sources are the Privacy Rights Clearinghouse (PRC) (data breach data), Identity Theft Resource Center (ITRC) (data breach data), Computer Intelligence (CI) database (IT implementation data), Execucomp (compensation data), and COMPUSTAT (accounting data).

My data collection started with PRC[10] and ITRC[11]. I note empirical information security research (e.g., D'Arcy et al. 2020; Higgs et al. 2016; Kamiya et al. 2020), that specifically focuses on me publicly traded firms, commonly adopts a single data breach source of PRC. However, the data breach report in PRC is limited. So, to offer a more robust representation of data breaches, I *also* collected data breach data from ITRC. I totally identify 4,016 (3,632) reported data breaches from 2012 to 2016 in PRC/ITRC. If one data breach occurred in a US-listed firm and was reported in either PRC or ITRC from 2012 to 2016, then such a breach is counted as one in my sample. In particular, I manually matched the firm names in my data breach data with the firm names in COMPUSTAT to achieve the information on ticker code.[12] If the names reported in PRC or ITRC were similar to but could not entirely matched with the ones in COMPUSTAT, I searched the firms' websites and other sources to further ensure a proper matching. This approach eventually yielded 622 data breaches involving 385 different firms. Panel A (Table 4) shows the information on my data breach data and Panels B (Table 4) shows the sample selection process.

Table 2.4. Information on data breach data and sample selection

Panel A: Information on data breach data

Year	Number of the breaches that were included in my sample	Number of the breaches that were reported by PRC	Number of the breaches that were reported by ITRC
2012	127	886	470
2013	129	890	619
2014	133	868	783
2015	112	547	780
2016	121	825	980

[10] Established in 1992, PRC (https://privacyrights.org/) functions as a nonprofit organization for consumer privacy rights.

[11] ITRC (http://www.idtheftcenter.org/) is a nonprofit organization that has publicly provided data breach reports since 2005. The data breaches reported in ITRC are based on confirmed breaches reported by various media sources and notifications from government agencies.

[12] When data breaches occurred in the unlisted subsidiaries of listed firms, I considered such breaches as having occurred in their listed parent firms.

Total	622	4,016	3,632

Panel B: Sample selection step	
Number of data breaches from 2012 to 2016 reported by PRC or ITRC	7,648
Less: Number of data breaches that cannot be merge with COMPUSTAT	(*7,026*)
Number of data breaches occurred in a US-listed firm.	622
Less: Number of breaches without necessary data from CI database and Execucomp.	(*447*)
Number of data breaches with necessary data from all other datasets.	175
Final Sample: number of the firm-year observations	3,061

I used CI database to derive a proxy for IT innovativeness. CI database records the information on IT infrastructure annually across over 10,000 firms in the me and Canada. As for its details, this database has been extensively regarded as an authoritative source of firm-level IT data and used in numerous studies (Chwelos et al. 2010; Kleis et al. 2012; Tian and Xu 2015; Xue et al. 2011; Xue et al. 2013; Xue et al. 2017). In particular, the CI database records firms' IT implementations annually. I collected these IT implementation data from the CI database on me public firms from 2012 to 2015. I then restricted the sample to the public firms which are available in COMPUSTAT. These procedures yielded a final sample of 8,821 firm-years. Then, I collected all accounting data (79,493 firm-years) from COMPUSTAT between 2007 and 2015. These data measured environmental uncertainty and the control variables. I also collected compensation data from Execucomp to calculate the moderator of long-term incentive. Consistent with prior work (e.g., Erickson, Hanlon and Maydew, 2006; Feng, Ge, Luo and Shevlin, 2011; Armstrong et al. 2013), I focused on the long-term incentive of corporate top management team. I collected equity holdings data for the top executives (including the CEO) of each firm from Execucomp for the measurement.

2.4.2. Variable Descriptions

2.4.2.1.Dependent Variable

I calculated the dependent variable of data breach risks (*BREACH_DUMMY*) as a dummy variable that equals 1 if a firm has a reported breach in the current or next fiscal year, and 0 if otherwise.[13] These data were collected from PRC and ITRC.

2.4.2.1.Independent Variable

This study measures IT innovativeness (*INNO*) using the Saidin index. An appropriate measure of IT innovativeness should capture two aspects, namely, (1) the number of adopted ITs and (2) innovative degree of each adopted technology. For example, Rogers (1995) measures IT innovativeness as *a composite score* comprising multiple ITs, and in this composite score, the rare and leading adoptions are presented large weights. Therefore, in consistent with the concept and prior literature, I measure IT innovativeness as a weighted sum of a portfolio of firms' ITs, where the less diffused and rare ones are assigned with higher weights. In particular, Saidin index (Karahanna et al. 2019; Spetz and Maiuro 2004), which is calculated as a weighted sum of a firm's adopted ITs, *with the weight of each IT being the percentage of firms that do not implement the technology,* is an ideal aggregated IT index to achieve the current objectives. Obviously, in calculating the Saidin index, the weights of the extensively diffused ITs are low, whereas those of rare ITs are high.

CI database contains adoption data for 61 types of ITs used by general US-listed

[13] In one of my robustness checks, I changed the dependent variable *BREACH* into *BREACH_NUM*, which represents the accumulated number of data breaches reported by firm *i* in the current fiscal year *j* and *j+1*.

firms (see Appendix B) over my sample period.[14] I consider all the types of ITs that recorded by CI database in calculating the Saidin index. In particular, to avoid the situation that such a "rare" and "less diffusion" is caused by "outdated," I have manually checked that the adoption rate of each included IT to ensure that such a rate does not constantly decrease. By calculating the Saidin index of each observation in my sample, I found that an example of the majority of the rare and innovative ITs is software-as-a-service ERP software with under 1% adoption rate. An example of the most widely diffused ITs in my sample is Phone System (with an average 73% adoption rate).

2.4.2.2.Moderator of Long-Term Incentive

Given stock options has been extensively regarded as a predominant form of long-term incentive compensation contract (Flammer and Bansal 2017; Hite and Long 1982; Nagar et al. 2003; Peng and Röell 2014; Sanders 2001), I derived a proxy for the variable of long-term incentive (*INCENTIVE*) as the average value of stock and option grants presented to top executives during the fiscal year.

2.4.2.4.Moderator of Environmental Uncertainty

Environmental Dynamism (*DYN*). I followed voluminous literature (e.g., Dess and Beard 1984; Keats and Hitt 1988) and computed *DYN* by regressing industry sales on a five-year period and standardizing the resulting standard error of the regression coefficient by the average industry sale for each three-digit SIC code. The high values

[14] I did not consider the two items of "Laptop PCs are more than 3 years old" and "Desktop PCs are more than 3 years old" as recording firms' IT applications.

of *DYN* indicate increased industry volatility and environmental dynamism.

Environmental Complexity (*COM*). I followed the empirical tradition (e.g., Boyd 1995; Dess and Beard 1984; Keats and Hitt 1988) to use industry concentration multiples minus one to measure *COM*.[15] I followed Hou and Robinson (2006) and Mithas et al. (2013), and I measured industry concentration in each three-digit NAICS industry as follows:

$HHI = \sum_i s_{ij}^2,$

where s_{ij} is the market share of firm i in industry j. A low *HHI* or high *COM* implies increased complexity and competition.

2.4.2.5.Control Variable

Following prior literature (e.g., Chen et al. 2011; Higgs et al. 2016; Kwon et al. 2012), I controlled for a vector of firm characteristics that may influence a firm's data breach risk, including, firm size, research and development (R&D) expense, loss position, firm leverage, capital expenditure, resource slack, product similarity with competitors, previously accumulated number of breaches. Given that large firms have many opportunities to be involved in data breaches, the first control variable is firm size (*SIZE*), which is the natural logarithm of the value of the total assets (in $millions) in a fiscal year. Second, firms with substantial R&D expenses are likely to possess intellectual property, thereby increasing their vulnerability of being targeted by hackers. Therefore, I included R&D expense (*R&D*) as another control, which is

[15] Industry concentration is extensively accepted to be the opposite to the extent of the environmental complexity that arises from the number and diversity of external entities faced by a firm (Boyd 1995; Dess and Beard 1984; Keats and Hitt 1988; Palmer and Wiseman 1999; Wiengarten et al. 2017).

calculated as the log of the R&D expenses (in $millions). Third, the severe economic problems encountered by loss listed firms will decrease the firms' attentions on information security issues (Higgs et al. 2016). Thus, another control that I included is whether a firm is in a loss position (*LOSS*), which is an indicator variable equal to 1 if the firm reported negative net income or 0 if otherwise. Fourth, firms' capital can determine whether these entities have sufficient resources or capital to invest in information security if needed. Hence, I controlled for firm leverage (*LEVERAGE*), which is the division between initial total liabilities and initial total assets (Aivazian et al. 2005). Fifth, larger capital expenditure provides more security investment opportunities (Carpenter and Guariglia 2008), and thus, I controlled for firms' capital expenditure (*CAPITAL_EXPENSE*). Sixth, I control for firms' resource slack (*SLACK*) given firm excess resource tends to play as a buffer to mitigate firm risks (Mishina et al., 2004; Lungeanu et al., 2016). I followed Wiengarten et al. (2017) and measured *SLACK* as the ratio of selling, administrative, and general expenses to sales. Seventh, I controlled for total product similarity (*SIMILARITY*) given this variable can directly determine firms' organizational learning possibility from their competitors. I measured this variable with the total product similarity variable in Hoberg-Phillips Textual Network Industry Classification (TNIC) dataset[16] provided by Hoberg and Phillips (2010, 2016), as in Kim et al. (2016) and Li and Zhan (2018). Last, I controlled firms' total number of previous breaches (*BREACH_PRE*) since this variable can largely index the endogenous factors of firms' security vulnerabilities.

[16] http://hobergphillips.tuck.dartmouth.edu/

Panel A in Table A presents the variable descriptions, in which *i* and *j* index firm and year, respectively. Table 2.5 reports the descriptive statistics and correlations.

Table 2.5. Descriptive Statistics and Correlations

	Variable	Mean	S.D.	1	2	3	4	5	6	7	8	9	10	11	12
1	*BREACH_DUMMY*	0.05	0.21	1.00											
2	*INNO*	13.23	10.15	0.14	1.00										
3	*INCENTIVE*	7.81	0.94	0.17	0.28	1.00									
4	*DYN*	0.13	0.10	-0.09	0.04	-0.04	1.00								
5	*COM*	-0.19	0.17	-0.02	-0.12	0.02	-0.27	1.00							
6	*SIZE*	7.31	1.92	0.22	0.47	0.68	-0.03	0.05	1.00						
7	*R&D*	0.03	0.07	-0.01	-0.17	-0.06	-0.14	0.16	-0.25	1.00					
8	*LOSS*	0.22	0.41	-0.04	-0.15	-0.25	0.01	0.06	-0.30	0.28	1.00				
9	*LEVERAGE*	0.56	0.26	0.08	0.19	0.21	0.00	0.00	0.32	-0.10	0.09	1.00			
10	*CAPITAL_EXPENSE*	0.04	0.05	-0.04	-0.07	-0.02	0.03	0.02	0.03	-0.11	-0.03	0.03	1.00		
11	*SLACK*	0.27	0.48	0.00	-0.09	-0.07	-0.06	0.09	-0.16	0.30	0.18	-0.03	0.07	1.00	
12	*SIMILARITY*	3.12	4.98	0.07	-0.08	0.15	-0.05	0.16	0.16	0.23	0.10	0.10	0.09	0.07	1.00
13	*BREACH_PRE*	0.08	0.39	0.67	0.14	0.17	-0.09	0.00	0.23	-0.01	-0.05	0.06	-0.05	0.00	0.07

2.4.3. Endogeneity Concern and Analysis Strategy

I estimated all of the models with *firm-level fixed-effect* models to test the hypotheses. The firm-fixed effects further account for unobserved heterogeneity, thereby reducing the concerns associated with time-invariant omitted firm characteristics that are correlated with firms' data breach risks. The year-fixed effects control for any systematic differences across these years that could influence a firm's security risk.

I recognize that IT innovativeness and security risks might be ***endogenous***. For example, certain unobserved time-variant factors might drive both firms' IT innovations and occurrences of data breach. In the situation, certain omitted variables will be significantly correlated with both the independent variable and the error term in my models.

To further ameliorate endogeneity concerns, I followed the approach in an increasing number of business research (e.g., Gamache et al. 2020; Guillén and Capron 2016; Li et al. 2018; Maksimov et al. 2019; Turner and Rindova 2018) and used the IT

innovativeness of peer firms (i.e., firms operating in the same industry) as an instrument variable to test the relationships among IT innovation, contextual factors and firm security. The averaged IT innovativeness from peer firms is a good *instrument* because it can influence the focal firm's IT innovativeness via mimetic isomorphism (DiMaggio and Powell 1983; Maksimov et al. 2019), but it would not directly cause firms' data breach incidences.

With the instrument variables, I performed regressions by using a two-stage residual inclusion (2SRI) approach (Terza et al. 2008). Such an approach is similar to a two-stage least-squares approach in the sense that the second stage in either approach is linear (Hausman 1978; Maksimov et al. 2019). I adopted an 2SRI approach in my analysis given such an approach is "particularly advantageous for estimating my two-step model with interaction terms" (Maksimov et al. 2019, p. 10). Following past studies (Guillén and Capron 2016; Maksimov et al. 2019), I employed 2SRI in all my models because, unlike 2SLS approach, such an approach does not require the steps to create additional instruments for testing interactions and helps clearly analyze the effect through the processes of sensing and reconfiguring. Specifically, in the first stage of my tests, I calculated the average IT innovativeness of peer firms and used the value as an instrument to test the effect of IT innovativeness. In the second stage, I adopted the residual from the first stage (*RESIDUAL_INNO*) as an additional control in my models.

2.5. RESULTS

2.5.1. Baseline Analysis

Tables 2.6 and 2.7 presents the baseline analysis results on the basis of a sample of 3,061 firm-year observations. Table 2.6 reports the results for the main effects. In particular, my panel regression model is as follows:

$$BREACH_{ij} = \beta_0 + \beta_1 INNO_{ij} + \sum \alpha_r Control_{ij} + v_i + w_j + RESIDUAL\_INNO_{ij} + \epsilon_{ij} \quad (1)$$

where β_1 is the coefficient of the independent variable; α_n, $n \in$ [1, 2,…, 8] reflect the effects of my controls; *RESIDUAL_INNO* is the residual from innovation, v_i and w_j represent the firm- and year-fixed effects, respectively; and ϵ_{ij} is the error term.

First, I conducted my analyses by using *fixed-effect logit* models given my dependent variable (*BREACH*) is a binary variable and I collected the data in multiple years. Models 1 and 2 report the related results. Model 1 (Table 2.6) only introduces the control variables. The results show that firms' accumulated number of previous data breaches (*BREACH_PRE*) is positively related to their subsequent data breach risks. In addition, as expected, firms' product similarity with their competitors can help defend against security threats. Model 2 (Table 2.6) introduces the independent variable (*INNO*) and also includes the moderators as additional controls. The coefficient of *INNO* is positive and significant ($\beta = 0.290$, $p < 0.05$), thereby indicating that a one-unit increase in IT innovativeness increases a firm's likelihood of data breach by approximately 29%. Thus, H2-1 is supported.

Second, to mitigate the concern that the application of fixed-effect logit model considerably reduces the sample size by dropping the observations where firms had

not experienced a data breach during my sample period (Haislip et al. 2021), I followed prior data breach risk literature (D'Arcy et al. 2020; Haislip et al. 2021) and adopted a *fixed-effect ordinary least squares* (OLS) regression. The related results are presented in Models 3 and 4, supporting H2-1.

Table 2.6. Baseline Regression Results (Main Effect)

	Fixed-effect logit using 2SRI (*BREACH_DUMMY*)		Fixed-effect OLS using 2SRI (*BREACH_DUMMY*)	
	Model 1	Model 2	Model 3	Model 4
INNO		**0.290****		**0.006***
		(2.06)		**(1.90)**
INCENTIVE		−0.098		-0.000
		(−0.32)		(-0.01)
DYN		−13.902		0.014
		(−0.13)		(0.08)
COM		1.159		0.033
		(0.33)		(0.38)
SIZE	0.644	−0.143	0.016	-0.002
	(0.86)	(−0.17)	(1.05)	(-0.10)
R&D	−8.370	−6.304	-0.041	-0.140
	(−0.56)	(−0.35)	(-0.24)	(-0.44)
LOSS	−0.351	0.280	-0.004	-0.000
	(−0.58)	(0.40)	(-0.44)	(-0.01)
LEVERAGE	−3.346	−2.934	-0.048	-0.054
	(−1.63)	(−1.30)	(-1.40)	(-1.12)
CAPITAL_EXPENSE	−6.937	0.309	-0.098	-0.039
	(−0.71)	(0.03)	(-0.74)	(-0.20)
SLACK	4.598	8.205	0.009	0.036
	(0.72)	(1.07)	(0.18)	(0.51)
SIMILARITY	−0.332**	−0.346*	-0.004**	-0.004*
	(−1.97)	(−1.88)	(-2.03)	(-1.78)
BREACH_PRE	1.230***	1.232***	0.230***	0.213***
	(3.92)	(3.68)	(12.86)	(10.31)
RESIDUAL_INNO	0.022	−0.225	0.001	-0.003
	(0.32)	(−1.61)	(0.61)	(-0.93)
Firm Dummies	Yes	Yes	Yes	Yes
Year Dummies	Yes	Yes	Yes	Yes
Number of observations	280	280	3,061	3,061

Notes. t statistics in parentheses (* p < 0.1, ** p < 0.05, *** p < 0.01).

Next I examine the moderating effects of managerial ability (*MA*), environmental dynamism (*DYN*), and complexity (*COM*). Table 2.7 reports the results in terms of the moderating effects. The following empirical models are implemented:

$$BREACH_{ij} = \beta_0 + \beta_1 INNO_{ij} + \beta_2 MF_{ij} + \beta_3 INNO_{ij} * MF_{ij}$$

$$+\sum\alpha_r Control_{ij} + v_i + w_j + PEER\_INNO_{ij} + \epsilon_{ij} \qquad (2)$$

where MF_{ij} are the moderating factors (i.e. *INCENTIVE*, *DYN*, and *COM*).

Models 5 to 8 report the results by using fixed-effect logit models. Model 5 introduces the interaction term (*INNO* × *INCENTIVE*) into Equation (1). The coefficient of *INNO* × *INCENTIVE* is significantly negative ($\beta = -0.073$, $p < 0.01$). In particular, the increasing effectiveness of firm IT innovativeness on their data breach risk will be decreased by approximately 7% given a one-unit positive increase in leaders' long-term incentive. Thus, H2-2 is supported. Model 6 (Table 2.7) introduces the interaction term (*INNO* × *DYN*) into Equation (1). The coefficient of *INNO* × *DYN* is significantly negative ($\beta = -3.310$, $p < 0.05$). Such a result is counter to my baseline hypothesis (H2-3) regarding the moderating role of environmental dynamism. Thus, H2-3 is not supported by my results. Model 7 (Table 2.7) introduces the interaction term (*INNO* × *COM*) into Equation (1). The coefficient of the interaction term is significant and positive ($\beta = 0.528$, $p < 0.05$), thereby indicating that the relationship between *INNO* and *BREACH* is strong when *COM* is high. In particular, the effect of *INNO* on increasing *BREACH* will be particularly strengthened by approximately 53% with a one-unit positive change in *COM*. Therefore, H2-4, which states that high environmental complexity will weaken the security effectiveness of IT innovativeness is supported. At last, Model 8 (Table 2.7) includes all the moderators and shows entirely consistent moderating effects.

Thereafter, I followed prior data breach risk literature (D'Arcy et al. 2020; Haislip et al. 2021), which adopted OLS regression in the analyses, and repeated the

aforementioned tests. The results (see Models 9 to 12) are entirely consistent and support my hypotheses.

Table 2.7. Baseline Regression Results (Moderating Effects)

	Fixed-effect logit using 2SRI (*BREACH_DUMMY*)				Fixed-effect OLS using 2SRI (*BREACH_DUMMY*)			
	Model 5	Model 6	Model 7	Model 8	Model 9	Model10	Model11	Model12
INNO	**0.881*****	**0.633*****	**0.441*****	**1.292*****	**0.022*****	**0.009****	**0.010*****	**0.028*****
	(3.21)	**(2.68)**	**(2.65)**	**(3.81)**	**(3.21)**	**(2.28)**	**(2.84)**	**(3.82)**
INNO×INCENTIVE	**−0.073*****			**−0.075****	**-0.002*****			**-0.002*****
	(−2.60)			**(−2.55)**	**(-2.63)**			**(-2.66)**
INNO×DYN		**−3.310****		**−2.369**		**-0.018**		**-0.013**
		(−2.01)		**(−1.36)**		**(-1.26)**		**(-0.87)**
INNO×COM			**0.528****	**0.537****			**0.014****	**0.013****
			(2.12)	**(2.18)**			**(2.44)**	**(2.25)**
INCENTIVE	−0.098	1.062*	−0.092	−0.109	-0.000	-0.002	-0.001	0.001
	(−0.32)	(1.94)	(−0.29)	(−0.35)	(-0.02)	(-0.11)	(-0.05)	(0.03)
DYN	−13.902	−23.451	31.942	−15.610	-0.144	-0.137	-0.109	-0.113
	(−0.13)	(−0.22)	(0.28)	(−0.12)	(-0.45)	(-0.43)	(-0.34)	(-0.36)
COM	1.159	0.635	1.482	−6.461	-0.001	0.000	-0.000	-0.001
	(0.33)	(0.18)	(0.44)	(−1.35)	(-0.07)	(0.02)	(-0.03)	(-0.07)
SIZE	−0.025	−0.311	−0.065	−0.082	-0.052	-0.055	-0.062	-0.060
	(−0.03)	(−0.38)	(−0.08)	(−0.10)	(-1.08)	(-1.14)	(-1.29)	(-1.25)
R&D	−3.220	−3.319	−1.545	3.840	-0.043	-0.037	-0.004	-0.009
	(−0.18)	(−0.18)	(−0.08)	(0.21)	(-0.23)	(-0.19)	(-0.02)	(-0.05)
LOSS	0.208	0.306	0.105	0.113	0.216***	0.213***	0.213***	0.216***
	(0.29)	(0.44)	(0.15)	(0.16)	(10.46)	(10.30)	(10.31)	(10.46)
LEVERAGE	−4.203*	−3.143	−3.724	−5.282**	-0.005*	-0.004*	-0.005*	-0.005**
	(−1.80)	(−1.37)	(−1.59)	(−2.15)	(-1.92)	(-1.78)	(-1.82)	(-1.96)
CAPITAL_EXPENSE	0.151	0.134	1.079	1.767	0.037	0.036	0.035	0.036
	(0.01)	(0.01)	(0.10)	(0.17)	(0.52)	(0.51)	(0.49)	(0.51)
BREACH_PRE	1.380***	1.260***	1.286***	1.480***	-0.003	-0.003	-0.004	-0.004
	(3.96)	(3.69)	(3.78)	(4.07)	(-0.93)	(-1.00)	(-1.34)	(-1.35)
SIMILARITY	−0.359**	−0.414**	−0.398**	−0.456**	-0.000	-0.002	-0.001	0.001
	(−1.97)	(−2.18)	(−2.06)	(−2.33)	(-0.02)	(-0.11)	(-0.05)	(0.03)
SLACK	5.495	8.479	6.922	4.182	-0.144	-0.137	-0.109	-0.113
	(0.70)	(1.11)	(0.91)	(0.54)	(-0.45)	(-0.43)	(-0.34)	(-0.36)
RESIDUAL_INNO	−0.255*	−0.281*	−0.267*	−0.338**	-0.001	0.000	-0.000	-0.001
	(−1.78)	(−1.85)	(−1.77)	(−2.07)	(-0.07)	(0.02)	(-0.03)	(-0.07)
Firm Dummies	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year Dummies	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Number of observations	280	280	280	280	3,061	3,061	3,061	3,061

Notes. t statistics in parentheses (* p < 0.1, ** p < 0.05, *** p < 0.01).

2.5.2. Robustness Checks

2.5.2.1.Heckman Correlation

I exerted effort to mitigate the concern which is raised because firm's IT implementation information can be not randomly covered by CI database. I adopted a two-step method proposed by Heckman {1977 #20453} to mitigate the potential

sample selection bias concerns. The primary purpose of such a method is to construct an *inverse Mill's ratio* (IMR) for each observation, thereby further serving as an additional control to correct the possibility of selection bias.[17]

I included the generated variable (i.e., *IMR*) as an additional control into Equations (1) and (2) and repeated my baseline analysis. These procedures enable me to obtain the results (please see Table 2.8) that are entirely consistent with those in my baseline analysis, thereby alleviating the sample selection bias concern.

Table 2.8. Heckman Correlation

	Fixed-effect logit using 2SRI (*BREACH_DUMMY*)				Fixed-effect OLS using 2SRI (*BREACH_DUMMY*)			
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
INNO	0.288**	0.879***	0.623***	0.443***	0.006*	0.022***	0.009**	0.010***
	(2.05)	(3.20)	(2.64)	(2.67)	(1.90)	(3.21)	(2.28)	(2.83)
INNO×INCENTIVE		-0.072***				-0.002***		
		(-2.59)				(-2.63)		
INNO×DYN			-3.241**				-0.018	
			(-1.97)				(-1.27)	
INNO×COM				0.539**				0.014**
				(2.17)				(2.44)
IMR	-428.986	-424.771	-318.330	-562.765	0.825	2.429	1.445	0.258
	(-0.64)	(-0.60)	(-0.49)	(-0.78)	(0.07)	(0.22)	(0.13)	(0.02)
RESIDUAL_INNO	-0.222	-0.253*	-0.277*	-0.265*	-0.003	-0.003	-0.003	-0.004
	(-1.59)	(-1.76)	(-1.83)	(-1.76)	(-0.94)	(-0.93)	(-1.00)	(-1.34)
Moderators	Included	Included	Included	Included	Included	Included	Included	Included
Controls	Included	Included	Included	Included	Included	Included	Included	Included
Firm Dummies	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year Dummies	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Number of observations	280	280	280	280	3,061	3,061	3,061	3061

Note. The settings on IT innovativeness measure (i.e., Saidin index), breach risk measure, sample period (i.e., 2012−2015), and control variables strictly followed the baseline analysis. Following the baseline analysis, the models in the test are twofold, namely, a fixed-effect logit one with using the 2SRI approach (see Cols. 1 to 4) and a fixed-effect OLS one with using the 2SRI approach (see Cols. 5 to 8). An additional control (i.e., *IMR*) is involved in the regression. t statistics in parentheses (* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$).

2.5.2.2.An Alternative Measure of the Dependent Variable

I used an alternative measure in terms of the dependent variable (i.e., data breach risks). That is, I replaced *BREACH_DUMMY* with *BREACH_NUM*, which represents

[17] Implementing Heckman's self-selection model requires the utilization of at least one predictor related to firms' relative performance and exogenous to focal firms. *Environmental dynamism* and *complexity* are two ideal choices. In addition, I followed Wiengarten et al. (2019) and included certain basic corporate economic indexes (i.e., *Firm size*, *Leverage*, *R&D*) as additional predictors. The aforementioned predictors enabled me to generate IMRs by using a probit model.

the accumulated number of data breaches within a year. Given *BREACH_NUM* is a count variable, I used *fixed-effect Poisson* and *fixed-effect OLS* regressions combined with the *2SRI* approach and achieved nearly consistent results (see Table 2.9).

Table 2.9. An Alternative Measure of Data Breach Risk (Dependent Variable)

	Fixed-effect Poisson using 2SRI (*BREACH_DUMMY*)				Fixed-effect OLS using 2SRI (*BREACH_DUMMY*)			
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
INNO	0.146*	0.514***	0.261**	0.203**	0.007*	0.035***	0.010*	0.012**
	(1.80)	(3.10)	(2.14)	(2.25)	(1.93)	(3.80)	(1.93)	(2.39)
INNO×INCENTIVE		-0.043**				-0.003***		
		(-2.53)				(-3.32)		
INNO×DYN			-1.333				-0.014	
			(-1.21)				(-0.71)	
INNO×COM				0.257				0.013*
				(1.48)				(1.72)
RESIDUAL_INNO	-0.125	-0.140*	-0.126	-0.135	-0.003	-0.003	-0.003	-0.004
	(-1.59)	(-1.71)	(-1.51)	(-1.63)	(-0.94)	(-0.93)	(-1.00)	(-1.34)
Moderators	Included	Included	Included	Included	Included	Included	Included	Included
Controls	Included	Included	Included	Included	Included	Included	Included	Included
Firm Dummies	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year Dummies	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Number of observations	309	309	309	309	3,061	3,061	3,061	3061

Note. The settings on IT innovativeness measure (i.e., Saidin index), sample period (i.e., 2012−2015), and control variables strictly followed the baseline analysis. In the test, data breach risk measure is updated into *BREACH_NUM* (please see the measure description of *BREACH_NUM* in Table A in Appendix A), and I firstly use a fixed-effect Poisson model with using the 2SRI approach (see Cols. 1 to 4). To allay the concerns that the application of fixed-effect Poisson model significantly reduces the sample size, I also provide the analyses by using a fixed-effect OLS model with 2SRI (see Cols. 5 to 8). t statistics in parentheses (* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$)

2.5.2.3.Alternative Measure of the Independent Variable: IT Leader List

An additional concern in my baseline analysis is whether IT innovativeness and security risk relationship can be accurately determined by using the Saidin index. Therefore, my first robustness check attempts to mitigate this concern by adopting an alternative measure of IT innovativeness (*INNO_DUMMY*) that is constructed using the InformationWeek (IW) 500 IT leader list. That is, for over 30 years, IW has identified and honored the US' most innovative IT users as "IT leaders" through its annual list.[18] Prior academic research (e.g., Bharadwaj 2000; Chae et al. 2014; Lu and

[18] Editors of IW 500 have noted that inclusion on the IW 500 IT list is by invitation only (See the website of

Ramamurthy 2010) has widely perceived IW 500 as an authoritative and credible source to identify IT leading firms.[19]

In particular, using the IT leader list to measure IT innovativeness raises the *selection bias issue*. I mitigated the selection bias concern by employing the coarsened exact matching (CEM) approach, which is a monotonic imbalance-reducing matching method and has recently received increasing attention in the field of business (e.g., Adbi et al. 2019; Bapna et al. 2016; Damaraju and Makhija 2018; Greenwood and Gopal 2017; Kolympiris et al. 2019).[20] Thereafter, I used the updated sample achieved with CEM and repeated my main analyses by replacing *INNO* with *INNO_DUMMY*, thereby enabling me to obtain results (please see Table 10) that are relatively consistent with those in my baseline analysis. Appendix B shows the imbalance analysis for the CEM approach.

Table 2.10. An alternative measure of IT innovativeness (independent variable)

	Logit model using the CEM approach (*BREACH_DUMMY*)			
	(1)	(2)	(3)	(4)
INNO_DUMMY	0.857**	1.349**	0.975	0.785
	(2.36)	(2.38)	(1.31)	(1.41)
INNO_DUMMY×INCENTIVE		-0.149*		
		(-1.87)		
INNO_DUMMY×DYN			-1.264	
			(-0.18)	
INNO_DUMMY×COM				-0.474
				(-0.17)
Controls	Included	Included	Included	Included
Industry Dummies	Yes	Yes	Yes	Yes
Year Dummies	Yes	Yes	Yes	Yes
Constants	-10.785***	-10.712***	-10.736***	-11.010***
	(-11.77)	(-11.71)	(-11.70)	(-11.93)

http://www.informationweek.com/iw500/2010/qualify.jhtml). The ranking methodology is based on a proprietary weighting system developed by the IW panel of experts, including industry analysts, IT executives, IT academics, and other practitioners.

[19] In the test, *INNO_DUMMY* is calculated as an indicator variable that is equal to 1 if a firm is ranked on IW 500 for the current fiscal year, which indicates high IT innovativeness; and 0 otherwise, which indicates a common level of IT innovativeness.

[20] CEM represents a new approach to improve the causal effect estimation by reducing the imbalance in covariates between the treated and control groups. My CEM estimation followed the *imb* and *cem* routines in Stata. I used firm size (*SIZE*), IT spending (*IT_SPEND*), business scope (*BUSI_SCOPE*), and year (*YEAR*) as pretreatment covariates because they are highly related with firms' IT innovation behaviors. In addition, I used the values of *IT_SPEND* to create coarsening. Appendix B shows the imbalance analysis for the CEM approach.

Number of observations	3,113	3,113	3,113	3,113

Note. The settings on data breach risk measure, sample period (i.e., 2012−2015), and control variables strictly followed the baseline analysis. I updated IT innovativeness measure by adopting the *IT leader list* one (*INNO_DUMMY*), and please see the measure description of *INNO_DUMMY* in Table A (Panel A) in Appendix A. Given the further constraint sample size after such an update, I adopted Logit model and employed the CEM approach to mitigate the selection bias issue that raised by adopting *INNO_DUMMY*. t statistics in parentheses (* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$).

2.5.2.4.Subsample Analysis

I further analyzed the security influence of IT innovativeness in terms of different data breach types. A common approach is to classify data breaches as either internal or external on the bases of the parties involved in the leakage (e.g., Cheng et al. 2017b; Hua and Bapna 2013; Kwon and Johnson 2014; Miller and Tucker 2011). Internal breaches are often caused by either malicious actions (e.g., corporate espionage) or accidental mistakes (e.g., incorrect placements or inadvertent sharing or disclosing by employees). By contrast, external breaches are typically caused by hacking, malwares, and social engineering attacks. I followed such classification criteria and characterized the data breaches in my sample into two subsamples of internal and external breaches. Thereafter, I individually tested the relationship between IT innovativeness and data breach risk in either subsample. Table 2.11 shows the relevant results.

Table 2.11 shows that the results for the internal breaches have similar significant patterns to those for the total data breaches. Nevertheless, the results for the external breaches exhibit weak evidence on the security influence of IT innovativeness. Thereafter, a t-test for the difference between the coefficients of the two terms (i.e., internal and external breaches) was performed (Wooldridge 2003, p. 139−142). The results (see Table 2.11) show that the difference is significant ($p < 0.01$). Therefore, I found that the influence of IT innovativeness is more evident on the internal than on

the external data breach risk.

Table 2.11. Subsample Analysis

	BREACH_IN				*BREACH_OUT*			
	Fixed-effect Logit		Fixed-effect OLS		Fixed-effect Logit		Fixed-effect OLS	
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
INNO	0.119	1.268**	0.003**	0.019***	0.110	0.589*	0.001	0.008
	(1.39)	(2.55)	(2.14)	(3.74)	(1.05)	(1.66)	(0.67)	(1.46)
INNO×INCENTIVE		-0.075*		-0.002***		-0.044		-0.001
		(-1.69)		(-2.75)		(-1.47)		(-1.30)
INNO×DYN		-5.696*		-0.013		-1.586		-0.006
		(-1.87)		(-1.15)		(-0.68)		(-0.47)
INNO×COM		0.294		0.008*		-0.033		-0.001
		(0.44)		(1.91)		(-0.09)		(-0.17)
Moderators	Included	Included	Included	Included	Included	Included	Included	Included
Controls	Included	Included	Included	Included	Included	Included	Included	Included
Firm Dummies	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year Dummies	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Number of observations	173	173	3322	3322	218	218	3322	3322

Note. The settings on IT innovativeness measure (i.e., Saidin index), sample period (i.e., 2012−2015), and control variables strictly followed the baseline analysis. Following the baseline analysis, the models in the test are twofold, namely, a fixed-effect logit one (see Cols. 1 to 4) and a fixed-effect OLS one (see Cols. 5 to 8). Please see the measure descriptions of *BREACH_IN* and *BREACH_EX* in Table A in Appendix A t statistics in parentheses (* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$).

I proposed two interpretations of this finding. First, external breaches can be more easily detected and defended than internal breaches because numerous technologies (e.g., firewalls and intrusion detection systems) are available for firms to effectively defend against external attacks. Thus, despite the information security and operational changes upon IT implementations, firms, particularly the IT-innovative ones, are capable of rapidly responding and enforcing effective technical measures to thwart external threats. By contrast, internal breach defenses and controls are relatively difficult and complex (Axelrod et al. 2009). They require firms to exert extensive effort to adjust and balance security routine changes upon IT adoptions, thereby causing additional security threats. Second, despite the extensive debate on internal security threats, firms are insufficiently focused on internal breaches compared with external attacks. In general, firms substantially invest in security technologies but commonly

disregard the improving of their non-technical human security measures. Firms also invest minimally in the protection against insider threats when compared with that against external threats. Thus, firms' defenses against internal threats tend to be weaker than against external breaches upon IT innovations. In summary, both reasons help explain why IT innovativeness has a stronger influence on internal breach risk than on external breach risk.

2.6. DISCUSSION AND IMPLICATIONS

I investigated the relationship between IT innovativeness and data breach risk. I used a sample of US firms from 2012 to 2015 and obtained empirical results that are nearly consistent with my predictions. That is, consistent with H2-1, I validated that firm IT innovativeness is positively associated with data breach risk. Consistent with H2-2, I proved that the aforementioned positive relationship can be significantly and negatively moderated by long-term incentives. In addition, I corroborate that environmental complexity can considerably and positively moderate the relationship between IT innovation and data breach risk, which supports H2-4.

Unlike H2-4, H2-3 is not empirically supported by the results. A partial explanation for this result may lie in the *inherent differences* between dynamism and complexity. That is, both the dimensions of dynamism and complexity can superficially reflect specific environmental uncertainties; however, their sources of uncertainties differ remarkably. Uncertainties under environmental dynamism originate from *continuously changing customer demands and technologies* (Dess and

Beard 1984). That is, the primary features of such an environment is *multiple changes but limited attentions of firms.* Attention-based view suggests that firms in the environment have to pay the particular attention to solve the ever-changing customers' preferences, product demand, technologies, and supply of materials, but have insufficiently focus on making themselves different from other rivals (Ocasio 2011; Sullivan 2010). Therefore, heterogeneities among entities are not highlighted among the firms under high dynamism (Downey et al. 1975). Consequently, the relative *homogeneities* among firms enable them to achieve security experiences through information searching from other members of their industry. By so doing, the threats that arise from other security problems can be counteracted.

By contrast, the uncertainty source of environmental complexity is *diversity of external competitors that a firm should cope with* (Dess and Beard 1984). Prior literature suggests that the primary features of such an environment is "heterogeneity" and "intensive competition" (Dess and Beard 1984; Keats and Hitt 1988). Therefore, firms under complexity can *rarely* absorb the compatible information and experiences from other members of their industry owing to the diverse *heterogeneities* among other entities. Hence, security threats that accompany firms' IT innovations are more pernicious in complex environments. In particular, this finding echoes the words of Schneier and Siegal (2003) that "Complexity is the worst enemy of security" (p. 354).

2.6.1. Theoretical Implications

The study offers several theoretical contributions. First, to the best of my

knowledge, this research represents the earliest, or among the earliest, empirical attempt to investigate the security consequence of IT innovativeness. In particular, the central notion that this study proposed and empirically validated is that IT innovation adoptions may cause substantial drawbacks in terms of security performance. Although such notions have been implied in studies on information security (e.g., Alexander et al. 2013; Axelrod et al. 2009; Brotby 2009), to my best knowledge, the present study is the first to provide empirical support of this idea.

Second, despite the long-standing call for security research from an organizational perspective (e.g., Cram et al. 2019; Cram et al. 2017; D'arcy and Herath 2011; Hedström et al. 2011), the related empirical efforts are considerably limited, most often looking at firm security policy and not focusing on broader firm characteristics that affects information security. Accordingly, the current study extends the prior security research by using an organizational perspective to identify and test a new organizational determinant (i.e., IT innovativeness) of data breach risk beyond those directly related to firm security policy.

Third, this research introduces the concepts of "security learning" and "security knowledge barrier" within an organizational learning framework. Accordingly, I model IT innovativeness as a driver of data breaches from the perspective that insufficient security learning causes security knowledge barrier in ways that increase data breach risks. That is, along with IT innovation adoptions, firms introduce a variety of immature security routines into the operations to update previously well-developed security routines. Such changes relatively disrupt the adopted firms' original security

equilibrium and cause security knowledge barrier and security vulnerabilities as well. Such notions may resonate with the security technostress literature (D'Arcy et al. 2014; D'Arcy and Teh 2019; Ho-Jin and Cho 2016; Hwang and Cha 2018), which suggests security requirements and infrastructures tend to increase employees' stress in operations.

Fourth, this research empirically connects firm leaders' time preference or external environments to firms' security performance. While most prior work has directed attention to chief information security officers (e.g., Haislip et al. 2020) or information security policies (Cram et al. 2019), this research is among the first undertakings that explore the role of leaders' time value systems or external environments in affecting data breach risk in the context of IT innovation.

2.6.2. Practical Implications

Several meaningful practical implications can be drawn from this study. First, my findings serve as a reminder that firms should prioritize information security as they accelerate their pace of digital transformation. Firms should realize that, although their IT innovations are economically beneficial because they can change social attitudes and increase operational efficiency, such innovations may simultaneously embody substantial security problems and threats. Thus, a balance between the economic benefits and security risks of IT innovations is required for managers to enhance firms' competitive advantage. As a precaution, managers should also formulate a deliberate plan and enforce the appropriate post-supervision in firms' digital transformation

journey. In addition, firms are typically over-reliant on traditional and monotonous technical security controls for their information security protection (Colwill 2009). My findings may also serve as a warning that technical security effort may potentially harms firms' information security given security IT adoption also tend to disrupt the adopted firms' original security equilibrium.

Second, my findings indicate that providing leaders additional long-term profits will strategically incentive leaders to pay further attention to security issues when fast-tracking firms' move to digitalization and in the big hurry to deploy a variety of innovative technologies. In addition, I may remind firms that long-term orientated managers tend to make great efforts to solve security threats that posted by firms' IT innovative adoptions.

Third, my findings can remind firms to incorporate their industry environments into their decisions related to IT innovations. In particular, if the industry where firms belong is high in complexity, then they should pay the particular and substantial attention on security risk of being a first mover in IT adoptions in the environment. The reason is that, in such a complex environment, firms' proactive adoption of new ITs may yield a highly substantial data breach risk.

2.6.3. Limitations and Future Research

Similar to other empirical studies, my results are also subject to limitations, thereby possibly providing avenues for future research. First, while my findings indicate that a high IT innovativeness is likely to increase data breach risk in the short

run, they do not imply that IT innovations, in particular security IT ones, remain damaging enterprise security in the long-run. Clearly, IT security innovations are important to firm information security protection as well. Absent such protection, firms are highly vulnerable to external attacks. Such arguments are consistent with the empirical findings in Angst et al. (2017) and Sen and Borle (2015) that *security IT investments* are likely to *increase* firms' data breach risks in the short-run, but tend to reduce such risks in the long-run. Accordingly, making ground on my topic, a possible avenue for future research is to investigate the long-term influence of IT innovations on data breach risks.

Second, despite my introduction of the "security learning" concept into the information security context, the scope of the related analysis only extended to the occurrences of data breaches rather than after breach incidences. However, I contend that security learning in the two stages (i.e., prior to and after data breaches) are consistent. That is because, comparing with the limited number of data breaches disclosed, firms' daily operations actually involve a larger number of security errors, and a majority of which fortunately do not lead to any breach; however, firms can still learn a lot from such "unmaterialized" errors. Accordingly, I suggest that future studies may consider the possible extensions in three directions: (1) the roles of IT innovations to influence the security learning after experiencing data breaches and (2) how IT innovations impacts firms' potential negative impact of data breaches.

Third, although the present study has brought the factor of managerial ability and environmental uncertainty in the security context, I only focused on the moderating

roles of these factors. Therefore, future studies may consider investigating the direct influence of managerial ability or environmental uncertainty on data breach risks.

Chapter 3. Corporate Social Responsibility and Data Breach Risk: An Agency Perspective

3.1.INTRODUCTION

"He that does good for good's sake seeks neither paradise nor reward but is sure to find both in the end"

(William Penn).

As firms implement digital strategies, an exponential surge has been observed in internet-connected devices and data traffic across networks (Cheng et al. 2017a). This explosion of traffic, often fueled by employee internet use, presents firms with larger-than-ever data breach risks that merit the attention of top managers, because even a single data breach can cause firm-level challenges, from the inconvenience of a network outage (Khan et al. 2019) to a major catastrophe such as a substantial decrease in stock values (Kamiya et al. 2020). To prevent data breaches, protect sensitive data, and secure strategic information, firms have found it necessary to increase investments in security- and assurance-related countermeasures (Colwill 2009).

While preventing data breaches caused by external agents has attracted substantial attention, employees are frequently the root cause of security problems (Cram et al. 2019). In practical terms, *even external attacks (e.g., malware or spyware attacks) often exploit firm insiders to create data breaches (e.g., employees responding to phishing messages)* (D'Arcy et al. 2009; Liang et al. 2019; Yoo et al. 2020). As a result, Shane Sims, director of advisory forensics practice of PricewaterhouseCoopers (PwC), noted that information security is "not really an ominous cyber problem; it's

actually a people problem."[21] Against such a backdrop, academics have directed substantial attention to individual security behaviors (Bulgurcu et al. 2010; Posey et al. 2015; Posey et al. 2013; Vance et al. 2015; Warkentin and Willison 2009; Willison and Warkentin 2013) and has generally reached a consensus that employees' ideologies (e.g., attitude, commitment, conscious activity, and moral obligation) determine their security behaviors, thereby exerting influence on firms' susceptibility to information security threats (Cram et al. 2019; Crossler et al. 2013). Consequently, a key research issue that has emerged is understanding how firm strategies that shape employees' positive ideologies can reduce data breach risk. Such understanding is critical because it could offer firms insight into how to design firmwide strategies and policies that enhance information security. Employee-related CSR has been extensively shown to significantly foster employees' positive behaviors and ideologies (Farooq et al. 2017; Flammer 2015; Flammer and Luo 2017; Gubler et al. 2018; Mory et al. 2016). Thus, to connect organizational strategy to data breach risk, I direct my attention to firms' employee-related CSR, which refers to which refers to firms' responsible efforts to manage workplace and employee issues (Barber 2004; Flammer and Luo 2017; Garel and Petit-Romec 2020). Accordingly, I propose my first research question: (1) *How does corporate employee-related CSR influence data breach risk*?

To answer the first research question, I draw on agency theory (Eisenhardt 1989; Fama 1980; Ross 1973), which has been extensively used in business literature to study CSR's effectiveness (e.g., Crouch 2006; Ferrell et al. 2016; Flammer and Luo 2017;

[21] https://www.complianceweek.com/human-error-not-hackers-cause-most-data-breaches/4048.article

Krüger 2015; Petrenko et al. 2016), and I also position data breach risk as entirely or partially originating from agency problems. Consistent with the agency view that agency controls (i.e., incentives and monitoring) can solve agency problems (Tosi et al. 1997; Zajac and Westphal 1994), I propose in my context that, employee-related CSR acts as agency controls to reduce data breach risks by pulling three levers: (1) *alignment incentives*: aligning employee and firm goals; (2) *informal monitoring*: providing security peer monitoring and aftercare; and (3) *differentiation*: attracting candidates and retaining employees. These levers help align employees' goals of members in terms of information security and foster informal monitoring on employees' security behavior, thereby engendering substantial security benefits (Cram et al. 2019; Cram et al. 2017) and leading to my prediction that employee-related CSR reduces data breach risks.

Given the CSR–security nexus, I intend to further achieve a refined understanding of where and when such a nexus is reinforced or alleviated. Prior literature (e.g., Hull and Rothenberg 2008; Li and Simerly 1998; Sung et al. 2017) suggests that efficacy of agency controls may vary with specific firms' economic, industry, and market environments. In addition, in my theory, the plausible mechanism that underlies the CSR–security link is that employee-related CSRs can play as agency controls to mitigate agency problems. Therefore, I attempt to examine the CSR–security link in the following contexts: (1) organizations with deteriorating economic performance (*economic* environment), (2) organizations located in turbulent environments (*industry* environment), and (3) organizations' products are highly similar to those of their

competitors (*market* environment). That is, I consider whether the CSR–security relationship occurs as a function of (i.e., is moderated by) negative performance, environmental dynamism, and/or product similarity. Accordingly, I propose my second research question: (2) *How do negative performance, environmental dynamism, and product similarity individually moderate the association between employee-related CSR and breach risk*?

I examine these research questions through an empirical analysis of a unique longitudinal data set of US-listed firms across a nine-year period (i.e., 2005–2013). I adopt a systematic research design to unpack the relationship among employee-related CSR, firm contexts, and data breach risks. Consistent with my expectations, I find that firms' employee-related CSR reduces their data breach risk, particularly if these firms are operating in a loss position, dynamic industry, or market with similar products. The findings survive a battery of robustness tests, including alternative measures and models, Heckman correlation, and two-stage residual inclusion (2SRI) approach. In particular, I included firm- and year-fixed effects in nearly all the aforementioned tests to further account for any unobserved heterogeneity and systematic differences across years.

My study contributes to the literature in several ways. First, the present study advances security literature. When investigating organizational determinants of firm data breach risks, scholars have primarily focused on IT or IS specific variables. My study initially shed light on the security *benefits* of a new nontechnical and well-being strategy, namely, employee-facing CSR. By doing so, I extend and provide new

insights that connect the broader organizational context to data breach risk. Moreover, research on individual behavior and information security (i.e., behavioral security literature) has generally left unexamined how non-security-related organizational strategies incentive employees to protect information security (Cram et al. 2019). This lack of attention is concerning because such non-security-related strategies could be important potential determinants of employees' security behaviors (Hedström et al. 2011). This study is among the first, to the authors' knowledge, to provide fresh insights into the behavioral security literature by highlighting how firm strategies (i.e., employee-related CSR), that lies outside of the security domains, serves to *protect* firms' information security. I also contribute to the emerging security research that utilizes secondary data sources and focuses on publicly traded US firms. That is, I note that nearly all related studies (e.g., D'arcy et al. 2020; Higgs et al. 2016; Kamiya et al. 2020) have adopted a single data breach source of Privacy Rights Clearinghouse (PRC), while the data breaches reported by PRC is significantly limited. To the best of my knowledge, the current study is among the first to manually integrate data breach information from PRC and Identity Theft Resource Center (ITRC), thereby offering a substantially robust representation of data breaches. The implication is that future data breach research may consider using a similar approach to further collect data breach information in such a comprehensive manner.

Second, the present study contributes to CSR literature by refocusing CSR's benefits from the domain of traditional firm outcomes (e.g., financial performance) to information security outcomes (e.g., data breach risk). My findings resonate with

positive findings on CSR, such as employee incentives (Russo and Fouts 1997), employee governance (Flammer and Luo 2017), candidate attraction (Albinger and Freeman 2000), and risk mitigation (Shiu and Yang 2017). To my knowledge, my study is the first to empirically demonstrate that CSR benefits firmwide information security.

Third, my boundary condition analysis complements the potential "missing link" in applying agency theory and CSR to information security research. I are the first, to my knowledge, to determine that the security agency controlling functions of employee-related CSR vary in economic, industry, and market contexts. This finding offers support for applying insights from the agency literature, which has proposed that the effectiveness of agency controls differs across contexts (e.g., Li and Simerly 1998). Additionally, Gond et al. (2017) conducted a literature review and analysis of 268 CSR studies at the microlevel. They indicated that extant knowledge on situational moderators in the association between CSR and employee reactions is remarkably limited. Thus, my investigation on moderating influences advances the agency, CSR, and information security literatures by showing that firms' performance, industry environment, and product similarity intervene in the association between CSR and employee reactions.

3.2.LITERATURE REVIEW

Two major streams of literature are directly related to my study: employee-related CSR literature and information security research. The two streams are reviewed as

follows.

3.2.1. Employee-Related CSR Literature

CSR are firms' responsible initiatives that engage in "actions that appear to further some social good, beyond the interests of the firm and that which is required by law" (McWilliams and Siegel 2001, p. 117). In recent years, academic scholars have shown increasing interest in microlevel CSR and have extensively debated the effects of employee-related CSR, which refers to firms' responsible initiatives that are important to employees, such as investments in work–life balance (e.g., career breaks and flextime), growth and development (e.g., support for professional qualifications), pay and benefits (e.g., childcare, eldercare, and insurance), health and safety (e.g., health screening), and employee involvement (e.g., consultation and communication) (Barber 2004; Flammer and Luo 2017; Garel and Petit-Romec 2020). Flammer and Luo (2017) proposed that firms tend to use employee-related CSR as an internal governance tool to align employees' incentives and enhance their attentiveness, commitment, and compliance. They found that this type of CSR plays a significant role in countering employees' adverse behaviors. Flammer (2015) emphasized that having strong employee-related CSR programs enables firms to motivate, attract, and maintain the most talented workforce. Gubler et al. (2018) focused on one specific form of employee-related CSR, namely employee-related corporate wellness programs, and determined that CSR can assist firms in increasing productivity by enhancing workers' motivations and capabilities. Farooq et al. (2017) and Mory et al. (2016)

focused on internal CSR (i.e., CSR that focuses on employee welfare) and found that firms' internal CSR efforts can enhance employees' perceived respect and organizational commitment. Beyond these aspects, employee-related CSR has been found to play a significant role in attracting candidates (Albinger and Freeman 2000), providing an insurance-like effect (Shiu and Yang 2017) and mitigating knowledge leakage (Flammer and Kacperczyk 2019).

In summary, the extant literature has shown the significant impact of employee-related CSR on employees' ideologies and behaviors (e.g., attentiveness, commitment, compliance, and motivations). While these related theories have yet to be applied in an information security context, where academic evidence exists that firms' information security performance is significantly influenced by employees' ideologies and behaviors (Boss et al. 2015; Bulgurcu et al. 2010; Cram et al. 2019; Johnston and Warkentin 2010; Posey et al. 2015; Vance et al. 2015). Therefore, I turn to explaining the association between firms' employee-related CSR and information security.

3.2.2. Information Security Literature

Information security refers to the practices of preventing access, use, theft, inspection, modification, and destruction of information.[22] Information that should be protected is called data and can be either in physical or electronic form. Moreover, data breaches ensue once confidential or private information has been accessed by unauthorized parties (Sen and Borle 2015). The consequences of data breach can be

[22] SANS Institute: Information Security Resources (https://www.sans.org/security-resources/).

extremely devastating. Data breaches can negatively affect companies in many ways, such as huge financial penalties, loss of customers, damage to reputation, and post-breach share price decreases (Janakiraman et al. 2018; Kamiya et al. 2020; Whitler and Farris 2017).

Data breaches can occur in a variety of manners perpetrated by either internal or external actors, and with either malicious or inadvertent intent.[23] However, a noteworthy phenomenon is *each type of firm data breach is highly likely to be related with firm insiders*. On the one hand, *insider errors* (e.g., sensitive information leakage owing to the use of a wrong email address), negligence (e.g., leaving smartphones in taxis, or misplacing USBs), and *malicious behaviors* (e.g., employee information theft or fraud), are directly caused by firm insiders (Cheng et al. 2017a; Colwill 2009). On the other hand, *external attacks* often exploit firm insiders to create data breaches. For example, employees' negligence or noncompliance can easily open the "back doors" of systems for external attacks, thereby potentially causing data breaches (Guo 2013; Herath and Rao 2009b). Evidence also suggests a myriad of ways that insiders cause data breaches by affording access to hacking or introducing malware to the enterprise (Colwill 2009; Siponen and Vance 2010).

Against such a backdrop, behavioral security literature has directed substantial attention on how employees' behaviors can influence firms' security performance by gleaning insight from theoretical lenses such as protection motivation (Boss et al. 2015; Johnston and Warkentin 2010), deterrence (D'Arcy et al. 2009), neutralization

[23] Egress (2019) reports that approximately 60% of data breaches that occurred during 2019 resulted from human errors.

(Siponen and Vance 2010), and accountability (Vance et al. 2013), among others. The literature has suggested that firms' information security performance is significantly influenced by employees' ideologies and behaviors, such as attentiveness (Vance et al. 2015), commitment (Posey et al. 2015), compliance (Bulgurcu et al. 2010; Cram et al. 2019), and motivation (Boss et al. 2015; Johnston and Warkentin 2010).

Furthermore, the past decade has witnessed emerging studies on investigating how organizational factors can influence firms' data breach risks (i.e., the likelihood of experiencing a data breach). However, these studies have proposed only a limited number of organizational determinants of data breach risks, such as, such as IT security investment (Angst et al. 2017; Kwon and Johnson 2014; Sen and Borle 2015), IT governance (Higgs et al. 2016; Liu et al. 2020), IS application (McLeod and Dolezel 2018; Wang et al. 2015), and IT expertise (Haislip et al. 2021), consequently suggesting that there are opportunities to expand the scope of the extant literature by going beyond examining factors within the IT, IS, or information security domains. In particular, by linking findings *from* behavioral security literature *to* the findings of the employee-related CSR literature, I find that there is potential to expand the scope of the extant literature on organizational determinants of data breach risks to consider the impact of employee-related CSR.

In particular, my research is mostly related to that of D'Arcy et al. (2020), which studied the security impact of *corporate social* ***inresponsibility*** (i.e., CSR concerns) and *the corporate social inresponsibility in the context of undertaking "society-facing*

activities"[24], and this study found that society-facing activities can be accepted by shareholders as "greenwashing" tools to mask firms' poor social performance (i.e., corporate social inresponsibility) in ways that increase firms' data breach risks. However, the preceding research has primarily focused on security impact of corporate social inresponsibility rather than CSR. In addition, investigating the security effect of firms' employee-facing responsible initiatives is entirely beyond the scope of their study. By contrast, I focus on the security effectiveness of firms' employee-related CSRs, thereby suggesting that the research scopes in the two studies do not coincide entirely.

3.3.THEORETICAL BACKGROUND

3.3.1. Principal–Agent Framework

This study uses a principal–agent framework to link CSR and data breaches (Eisenhardt 1989; Ross 1973). In particular, I take such a principal–agent perspective as CSR literature has extensively suggested that CSR is an important agency control mechanism to reduce agency problems amongst shareholders (e.g., Crouch 2006; Ferrell et al. 2016; Flammer and Luo 2017; Krüger 2015; Petrenko et al. 2016). Similarly, in the context of information security, I propose that employee-related CSR can act as agency controls to reduce agency problems. In a so-called principal–agent relationship, one party (i.e., "principal") turns authority and duties over to another party (i.e., "agent"). If the agent and principal's goals are misaligned, then the former

[24] D'Arcy et al. (2020, p. 3)

has an incentive to engage in opportunistic behaviors to maximize his or her own self-interest rather than that of the latter. Additionally, information asymmetry, that is, when information is not distributed evenly between two parties (Zajac and Westphal 1994), creates opportunities for agency problems by enabling the agent to behave opportunistically.[25] Thus, and simply put, *misaligned incentives* and *information asymmetry* between the agent and principal are the two root premises for causing agency problems in a principal–agent relationship, and *either can be omitted*.

Two specific agency problems, namely *shirking* and *adverse selection*, are specifically described in the agency theory literature (Fong and Tosi Jr 2007). In an employee-employer relationship, the first agency problem, *shirking* (or moral hazard), occurs when employees devote insufficient effort to performing their tasks or act opportunistically. Employees' shirking can be *malicious*, such as committing theft by stealing money from other employees' wallets or purses in the office, or *nonmalicious*, such as loafing behaviors to potentially avoid difficult or tedious tasks in the workplace (Chen and Sandino 2012; Flammer and Luo 2017; Krueger 1991). Another agency problem is *adverse selection*, which refers to employers' inability to verify information provided by the agent. For example, employees may misrepresent their abilities and skills at the time of hiring, thereby causing adverse selection problems (Eisenhardt 1989).

Generally, agency research suggests that agency problems can be mitigated by

[25] Principal–agency framework has been applied by researchers at various levels, such as owner–manager, employer–employee, buyer–supplier, and lawyer–client (Eisenhardt 1989; Harris and Raviv 1978). Tracing back to Holmstrom (1979), business scholars have extensively used agency theory to conceptualize the relationship between employees (i.e., agents) and employers (i.e., principals) (Eisenhardt 1989; Ross 1973).

reducing *either* misaligned incentive *or* information asymmetry, and the research suggests two countermeasures to solve agency problems (Fong and Tosi Jr 2007; Tosi et al. 1997). First, employers may align incentives to reinforce goal congruence with employees (Laffont and Martimort 2009). For example, incentive pay has been found to motivate employees to consistently act in the interest of firms (Sung et al. 2017). Second, employers may use *monitoring* by, for example, checking the input performance of employees to reduce the information asymmetry between them or implementing policies to monitor employees' opportunistic actions.

Overall, the principal–agent framework indicates that the *coexistence* of misaligned incentives and information asymmetry enables agency problems, namely, *shirking* and *adverse selection*. In addition, *incentives* and *monitoring* represent countermeasures to solve these problems. Figure 3.1 delineates the principal–agent framework. Within such a framework, below I will refocus attention on the security context, and discuss why data breaches, disregarding the ones attributed to insiders or outsiders with malicious or nonmalicious intentions, are extensively caused by agency problems.

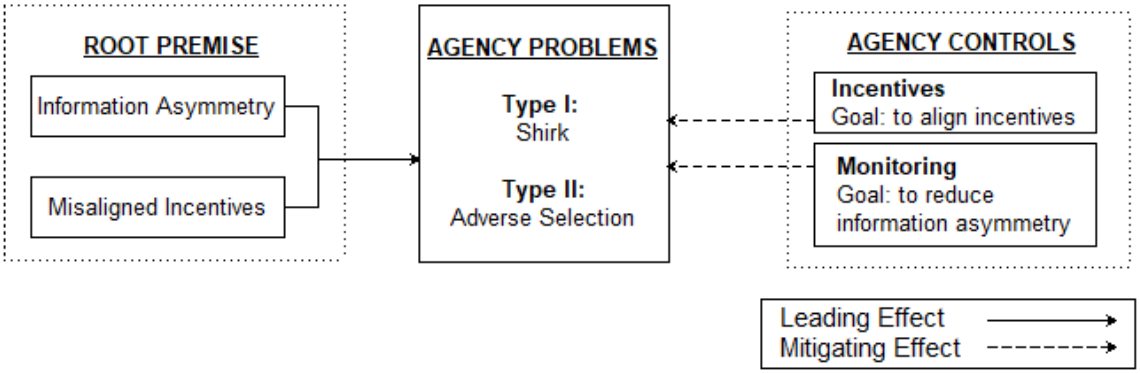

Figure 3.1. Principal–Agent Framework

3.3.2. Agency Problems and Security Threats

To set the stage for a principal–agent investigation of employee-related CSR and data breaches, this subsection discusses how either type of agency problem (i.e., shirking or adverse selection) leads to security threats.

3.3.2.1.Shirking Is Information Insecure

Employees' shirking (or moral hazard) occurs when they fail to exert sufficient effort or act opportunistically. As earlier mentioned, employees' shirking can be either malicious or nonmalicious (Chen and Sandino 2012; Krueger 1991). On the one hand, nonmalicious shirking can lead to considerable security threats. For example, employees may look for ways to work around security policies that they feel hinder their ability to carry out work but thereby create data leakage risks (D'Arcy et al. 2014; D'Arcy et al. 2009; Sarkar et al. 2020). For convenience, employees may choose to deploy only one firewall, even though security policies dictate the use of multiple layers of firewalls (Post and Kagan 2007), inadvertently aiding cybercriminals' ability to gain access to an organization's systems. In addition, employees sending sensitive customer files, storing data in an unencrypted cloud, setting extremely weak passwords, and sharing job-related passwords with others, are all nonmalicious shirking and result in firms encountering additional security threats (D'Arcy et al. 2009; Siponen and Vance 2010). In general, such nonmalicious and "innocuous" misbehaviors are commonly located in the "grey areas" of enterprise security controls. However, each

act may be devastating and break down an entire IT system, even in organizations with ideal IT technological controls (Herath and Rao 2009a).

On the other hand, malicious shirking can also lead to security threats. If nonmalicious shirking are caused by employees misunderstanding the consequences of their disengaged acts, then malicious misbehaviors are the opposite: although these employees are clearly aware that their actions are detrimental to their organizations, they maliciously compromise organizations' information in some forms, such as fraud, theft, and sabotage to serve their own self-interest (Posey et al. 2011; Straub Jr and Nance 1990; Willison and Warkentin 2013; Willison et al. 2018). In essence, any form of malicious security misbehaviors by employees can be defined as malicious shirking (Chen and Sandino 2012; Krueger 1991).

3.3.2.2.Adverse Selection Is Information Insecure

The agency problem of adverse selection occurs when employees misrepresent their skills and abilities to employers (Fong and Tosi Jr 2007). Adverse selection can pose security threats because, for example, it increases the likelihood for firms to hire and select the insiders with a low or inappropriate level of responsibility, loyalty, and security knowledge. Given staff members who lack skills or hold values that are incompatible with the firm may become the "weakest link" and "biggest enemy" in an organization's security equation (Bulgurcu et al. 2010; Colwill 2009; Jensen et al. 2017; Jensen et al. 2020), adverse selection problem can lead to increased security vulnerabilities.

Taken together, I have argued that agency problem in either the manner of shirking or adverse selection leads considerable security threats. Consistent with the agency view that agency controls can solve agency problems (Eisenhardt 1989; Ross 1973), I next discuss that employee-related CSR can play as agency controls to mitigate agency problems and generate security benefits.

3.3.3. Security Benefits of Employee-Related CSR

I build on my security contextualized principal–agent framework and propose three security-beneficial levers of employee-related CSR: (1) *alignment incentives*: aligning employee and firm goals; (2) *informal monitoring*: providing Security Peer Monitoring and Aftercare; and (3) *differentiation*: attracting candidates and retaining employees.

3.3.3.1.Alignment Incentives: Aligning Employee and Firm Goals

Employee-related CSR activities help align organizational and individual incentives and the activities have been extensively accepted as a powerful governance tool to enhance employees' identifications (e.g., Farooq et al. 2017; Flammer and Kacperczyk 2019; Flammer and Luo 2017). For example, workers may draw clues from firms' employee-related CSR activities (e.g., direct queries to CEO) that firms and executives are fair-minded. Certain employee-related CSR (e.g., share incentive plan) can also provide employees with opportunity to buy company shares, thereby directly fostering employee–company incentive congruence. Furthermore, employees can raise their perceptions of the current job and recognize their appreciated

organizational qualities by participating in firms' employee-related CSR programs (e.g., work–life balance, health programs, training and development) (Flammer and Luo 2017). All these approaches can foster employees' company identifications and company-aligned goals, thereby orienting employees' future behaviors toward reinforcing such an identification.

If the incentives and goals between employees and organizations are congruent, then security threats could be significantly reduced. That is because, employees with congruent incentives with their organizations are suggested to hold various positive ideologies at work, such as high levels of compliance, engagement, attentiveness, and responsibility (Farooq et al. 2017; Flammer and Luo 2017; Fong and Tosi Jr 2007; Sung et al. 2017), and these positive ideologies act as a potential remedy to enterprise security risks. For example, high compliance motivation may drive employees to carefully follow firms' security policies, rules, and regulations despite their complexity (Bulgurcu et al. 2010). High responsibility may, for example, deter workers from downloading music and videos on work laptops, thereby avoiding placing firms' systems and networks at risk of malware and virus infections (Posey et al. 2015). In addition, insiders with high engagement are likely to be patient in the face of cumbersome and tedious security-related operations and be willing to patch security flaws and harden the system for resiliency against attacks (Cram et al. 2019).

Overall, pulling the "incentive alignment" lever enables employee-related CSR to reap security benefits and reduce security threats. In particular, such a security beneficial manner of CSR echoes the agency theoretical concept, which states that

employees' shirking can be solved by using alignment incentives.

3.3.3.2.Informal Monitoring: Security Peer Monitoring and Aftercare

Employee-related CSRs can provide an informal environment for employers and employees to interconnect with each other. Compared with other working environments, CSR environments (e.g., open door to managers) tend to be fairer and more caring (Flammer and Luo 2017), thereby enabling employers and employees to collaborate and communicate with each other to reduce information asymmetry. Moreover, employee-related CSRs (e.g., speak-up and feedback programs) may play as a security "aftercare" to further guide employees on their acceptable and unacceptable security behavior in the workplace.

Informal security monitoring is markedly crucial for firms to achieve effective information security protection. That is because, the majority of security concerns originate from employees' negligent behaviors and negative work attitudes (Herath and Rao 2009b; Vance et al. 2015) rather than from deliberate violations of firms' hard and fast rules, thereby driving the inefficacy of managers' direct application of formal power to enforce them. Thus, formal security control (e.g., security technologies, policies, or regulations) is frequently ineffective (Colwill 2009; Herath and Rao 2009a; Post and Kagan 2007). In addition, actively detecting or monitoring employee activities that could pose a security threat may lead to a clash between human and security factors (D'Arcy et al. 2014; Post and Kagan 2007). For example, workers may become disgruntled if they feel they are under constant scrutiny (George 1996; Liang

et al. 2019). In this regard, simply applying formal monitoring as a means of eliciting compliance with security policies may be unwise for firms, making informal security monitoring highly relevant to eliciting compliance with security policies.

In addition, although formal security monitoring or training can prepare the ground for employees to change their security behaviors, true security effectiveness should entail security "aftercare" to completely "install" the security knowledge into employees' mind with being clearly acknowledge of when, where, how, and why to use such knowledge (Colwill 2009). Colwill (2009) highlights that security aftercare is particularly proper to be implemented through some informal aspects of activities for employees (e.g., employee-related CSRs) to build the understanding of the security-related expertise in detail.

In summary, employee-related CSR can also yield security benefits by pulling the "informal monitoring" lever to provide employees informal security monitoring and aftercare. Such a beneficial security mechanism of CSR resonates with agency theory that employees' shirking can be prevented by monitoring.

3.3.3.3.Differentiation: Attracting Candidates and Retaining Employees

Employee-related CSR can serve as a means of increasing organizations' differentiation, thereby serving to attract engaged candidates and retain employees who share firm values.

In terms of attracting candidates, employee-related CSR initiatives (e.g., support and leisure facilities, flexible working, childcare vouchers, and health insurance) can

send “positive” signals to job seekers about corporate culture, perceptions, orientations, and sound enterprise reputation (Albinger and Freeman 2000; Greening and Turban 2000). Engaged and high-quality employees tend to seek a workplace that they would identify with (Farooq et al. 2017), and thus they tend to be attracted to CSR firms that are commonly associated with fair conditions and trustworthy work environments, thereby enabling the CSR firms to deepen their engaged candidate pool (Greening and Turban 2000; Klimkiewicz and Oltra 2017).

It is beneficial to firms’ information security by attracting more engaged candidates. That is because, firms hiring strangers and giving them legitimate access to sensitive information is inherently unsecure, in particular if the new employees are unengaged and irresponsible (Posey et al. 2015; Posey et al. 2013). Therefore, employee-related CSR’s differentiation function as attracting a large candidate pool helps reduce the possibility of hiring unengaged or irresponsible employees and generates security benefits.

Employee-related CSR activities also have the power to reduce workers’ propensity to leave because these activities can optimize the work environment and enhance employee job satisfaction (Bode et al. 2015). I then discuss the security benefits of employee-related CSR’s differentiation function to retain employees from several aspects. First, existing employees should be more security efficient and make less security-related mistakes, given it takes time for new hires to become fully familiar with organizations’ security routines. Second, employees’ turnover poses considerable security threats. For example, anecdotal evidence has extensively documented that

employees departed with keeping sensitive data and consequently compromise firms' security. Third, organizational loyalty, which is often forged by bonds and affinity, takes time to build because of the extensive adoption of work-from-home arrangements; however, absent loyalty, employees may presents security threats to firms by, for example, being more likely to engage collusion with crime groups, sharing sensitive information, or even taking acts of revenge after leaving an organization (Crossler et al. 2013; Willison et al. 2018). Hence, employee-related CSR's ability to reduce employee turnover can help to retain the relatively loyal employees and thus benefit firms' information security.

To summarize, the third manner for employee-related CSR to achieve security benefits and reduce security threats is through displaying a "differentiation" function that helps to attract and retain employees. Such a security beneficial manner of CSR is particularly consistent with the agency view that alignment incentives can play as solutions to adverse selection and shirking problems.

3.4.HYPOTHESIS

My discussion of employee-related CSR and principal–agent theory provides the building blocks for my hypotheses that connect CSR to data breach risk and examine the boundary conditions of this relationship.

3.4.1. Main Effect

Employee-related CSR can assist organizations in reinforcing security defenses

and reducing security threats by pulling three levers: *alignment incentives*, *informal monitoring*, and *differentiation*. I summarize the three security-beneficial levers and their respective security benefits in Table 3.1. Each lever exerts a direct influence on employees' (or candidates') ideologies and behaviors and engenders security benefits. Integration of the three levers leads to decreased security threats that accompany the enactment of employee-related CSR. Thus, I formulate the following hypothesis:

HYPOTHESIS 3-1 (H3-1). *Employee-related CSR is negatively associated with data breach risk.*

Table 3.1. Security-Beneficial Levers of Employee-related CSR

Security-Beneficial Levers	**Direct Impact on Employees**	**Engendered Security Benefits**	**Security Benefits from an Agency Perspective**
Alignment incentives	Stimulating employees' positive ideologies (e.g., high attentiveness, engagement, responsibility) at work	• Employees tend to strictly follow firms' security policies and enhance attentiveness on security procedures. • Employees tend to have heightened awareness of the need to protect firms' information security.	Agency control in the form of *incentives* facilitates the mitigation of the agency problem of *shirking*.
Informal monitoring	Promoting employee–employer interactions to reduce information asymmetry, and providing employees with security aftercare	• Security-related information asymmetry between employers and employees is reduced. • Employees can achieve the security-related assistant in a timely manner.	Agency control in the form of *monitoring* facilitates the mitigation of the agency problems of *shirking*.
Differentiation	Reinforcing employees' and candidates' beliefs that firms are distinctive and attractive	• There is an increase in the number of engaged and high-quality candidates. • Loyal and high-quality employees with high identification are retained. • Security threats caused by employee turnovers are reduced.	Agency control in the form of *incentives* facilitates the mitigation of the agency problem of *shirking* and *adverse selection*.

3.4.2. Moderating Effects

To gain a deeper understanding of the CSR–security relationship from the agency

perspective, I probe three contextual conditions under which the relationship may or may not hold, specifically, (1) firms have deteriorating economic performances (negative performance), (2) firms are located in turbulent industries (environmental dynamism), and (3) firms' products are highly similar to their competitors (total product similarity), given literature suggests that efficacy of monitoring and incentives may vary with firm economic, industry, or market contexts (Hull and Rothenberg 2008; Li and Simerly 1998; Sung et al. 2017).

3.4.2.1.Moderating Effects of Negative Performance

I define negative performance as a situation, in which firms' performance is below the aspiration level, which is evaluated on the basis of the focal firm's prior performance (Jordan and Audia 2012; Lim and McCann 2014). Employees' emotional state, motivations, and satisfaction can be diminished by firm performance moving into the loss domain because firms in weak financial positions may be perceived as (or actually be) relatively incapable of directly granting tangible rewards (e.g., compensation) to their employees as incentives (Spreitzer 1995). Moreover, employees tend to reap an insufficient sense of achievement and satisfaction from their work in organizations suffering from negative performance (Judge et al. 2001; Luthans 1998; Schwab and Cummings 1970). Therefore, employees in such situations tend to act with low conscientiousness and effort.

Fong and Tosi (2007) empirically determined that agency controls (whether in the form of incentives or monitoring) can be highly effective to improve behavior for the

workers with low conscientiousness and effort, since shirking acts of less conscientious employees have been frequently in place prior to the application of incentives or monitoring, a large possibility and room exist for these employees to improve their behavior and alter their psychological responses.

Overall, the preceding arguments indicate that, for firms suffering from negative performance, given their employees tend to have relatively low conscientiousness and efforts (Spreitzer 1995), *agency controls are highly effective in such firms* (Fong and Tosi 2007). Following this logic, given the influence of employee-related CSR on data breach risk *sources from the agency control mechanism of employee-related CSR,* it is reasonable to expect that such a security effectiveness of employee-related CSR is amplified if firms are suffering from negative performance. Thus, I formulate the following hypothesis:

HYPOTHESIS 3-2 (H3-2). *Negative performance strengthens the relationship between employee-related CSR and data breach risk.*

3.4.2.2.Moderating Effects of Environmental Dynamism

Environmental dynamism refers to the volatility, unpredictability, and instability prevalent in firms' external environments (Dess and Beard 1984; Keats and Hitt 1988). Jansen et al. (2006, p. 1664) describe dynamic environments as being characterized by "changes in technologies, variations in customer preferences, and fluctuations in product demand or supply of materials."

When a high level of environmental dynamism is present, a high degree of

instability engenders significant and frequent changes in organizations' technology- or information-related routines (Baskerville et al. 2018; Bstieler 2005). Li and Simerly (1998) suggest that, in such environments, given that managers face highly uncertain situations and are distant from the full process of operations, it will be relatively difficult for them to comprehensively consider the related changes and rapidly executing implementations accordingly. Similarly, in the context of information security, managers tend to find enhanced incapability to effectively monitor employees' security motivations and behavior to fully assess the efficacy of their security supervisions, or to adequately evaluate the security procedures that employees adopted. Therefore, formal security monitoring of employees and their security behavior are extremely difficult and ineffective under conditions of substantial environmental dynamism.

Literature has agreed that informal control is highly relevant in driving the projects, where formal solutions are dispersed (Chua et al. 2012; Kirsch 2004; Kirsch et al. 2010; Kohli and Kettinger 2004). Consequently, in conditions of environmental dynamism, employee-related CSR's function of *informal control* for aligning employee–company incentives and stimulating peer monitoring is further reinforced. Therefore, I expect environmental dynamism to strengthen the security benefits of employee-related CSR.

Such an expectation echoes the findings of numerous organizational studies. For example, Li and Simerly (1998) determined that strategies for aligning incentives are highly effective under conditions of considerable environmental dynamism.

Identifying a similar pattern, Sung et al. (2017) empirically found that the effectiveness of incentives to increase employee commitment is strengthened when organizations have a dynamic environment. Moreover, Aragón-Correa and Sharma (2003) determined that environmental dynamism tends to strengthen the competitive advantage conferred by CSR. Thus, I formulate the following hypothesis:

HYPOTHESIS 3-3 (H3-3). *Environmental dynamism strengthens the relationship between employee-related CSR and data breach risk.*

3.4.2.3.Moderating Effects of Product Similarity

Product similarity refers to general product similarities between firms and their competitors. If a firm's products are highly similar to those of competitors, then the organizations' employees may face markedly low mobility barriers because the requisite task-related skills and knowledge tend to be transferable between organizations and their rivals (Griffeth et al. 2000). In such cases, employees readily engage in job-hopping and are highly adaptable to new working environments (Jackofsky and Peters 1983; Laker 1991). The bare mobility barriers and low costs associated with leaving tend to reduce employees' anxiety about making mistakes or being fired, and thus, such employees may show reduced effort and engagement (Flammer and Luo 2017). Fong and Tosi (2007) found that incentive alignment improves the effort and task performance of low-effort employees more than that of highly engaged and responsible employees. This evidence suggests that employee-related CSR's security benefits can be further reinforced via the *alignment incentive*

lever.

Furthermore, Hull and Rothenberg (2008) determined that the efficacy of organizations' efforts to differentiate themselves through CSR is high if the levels of differentiation from competitors are low. Similarly, I could thus reasonably expect that the added differentiation provided by employee-related CSR is highly effective in the context of poorly differentiated competitors. That is, if an organization's products are minimally different from those of competitors, then employee-related CSR activities may have a more significant differentiation effect, thereby amplifying the security benefits of CSR achieved via the *differentiation* lever. Thus, I formulate the following hypothesis:

HYPOTHESIS 3-4 (H3-4). *High product similarity strengthens the relationship between employee-related CSR and data breach risk.*

3.5.DATA AND VARIABLES

3.5.1. Data Description

This section describes the empirical method used in this study. The sample begins in 2005 and ends in 2013, because the former is the year ITRC and PRC started their data collection. My sample period ends in 2013 since data structures of KLD dataset have changed significantly during the year of 2013 (Flammer and Luo 2017; Qian et al. 2019; Tong et al. 2020). The sample used in the current study was primarily obtained by merging the following public sources: PRC (data breach data), ITRC (data breach data), Kinder, Lydenberg, and Domini (KLD) database (CSR data), TNIC

database (product similarity data), and COMPUSTAT (accounting data).

I collected data breach data from PRC[26] and ITRC[27]. I note that prior empirical information security research (e.g., D'arcy et al. 2020; Higgs et al. 2016; Kamiya et al. 2020) that specifically focuses on me publicly traded firms, commonly adopts a single data breach source of PRC. However, the data breach report in PRC is limited. Consequently, to offer a more robust representation of data breaches, I integrated data breach information from the PRC and ITRC to provide a comprehensive test of the relationships among data breach, firm context, and operational efficiency. I totally identify 5,319 (4,874) reported data breaches from 2006 to 2014 in PRC (ITRC).

Specifically, if a data breach occurred in a US-listed firm and was reported in either PRC or ITRC from 2006 to 2014,[28] the breach was counted in my sample. To this end, I manually match the firm names in my data breach data with the firm names in COMPUSTAT to achieve the information on ticker symbol.[29] If the names reported in PRC or ITRC were similar to but could not entirely matched with the ones in COMPUSTAT, I searched the firms' websites and other sources to further ensure a proper matching. Such an approach enables me to include 940 data breaches involving 518 different firms in my sample.

I collected employee-related CSR data from the KLD database,[30] which reports

[26] Established in 1992, PRC (https://privacyrights.org/) functions as a nonprofit organization for consumer privacy rights.

[27] ITRC (http://www.idtheftcenter.org/) is a nonprofit organization that has publicly provided data breach reports since 2005. The data breaches reported in ITRC are based on confirmed breaches reported by various media sources and notifications from government agencies.

[28] My breach sample is one-year lag and starts in 2006.

[29] When data breaches occurred in the unlisted subsidiaries of listed firms, I considered such breaches as having occurred in their listed parent firms.

[30] KLD database has been extensively used in prior research to construct measurements for CSR (Barnett and Salomon 2012; Chen et al. 2009; Margolis and Walsh 2003; McWilliams and Siegel 2000; Servaes and Tamayo

annual ratings of firms' CSR performance (referred to as *CSR rating* hereafter) since 1991. The CSR ratings identified and provided by the KLD database involve a series of dimensions, such as environment, employee, community, governance, and product. Each CSR rating item was developed as a binary indicator representing whether a firm fulfills a certain criterion in the corresponding dimension. Given that the current study focuses on employee-related CSR, I particularly concentrated on the *employee dimension of* the KLD data.[31] Such a measure is consistent with my definition of employee-related CSR. I collected all the CSR rating items *in the employee dimension* from the KLD database from 2005 to 2013.

Additionally, I collected all total product similarity data between 2005 and 2013 from the Hoberg–Phillips TNIC data based on prior studies (e.g., Hoberg and Phillips 2016; Kim et al. 2016) that used this data set to collect total product similarity data. Finally, I collected all accounting data from Compustat between 2000 and 2013, using these data to measure environmental dynamism, negative performance, and part of my controls.[32]

I merged all the collected data with ticker symbols and years. After excluding the observations with missing accounting information and firms located outside the US, the final sample consists of 19,519 firm-year observations, including the 613 data breaches. Table 3.2 summarizes my sample selection process.

2013).

[31] The employee dimension of the KLD data maintains a record on firms' CSR regarding union relations concerns, health and safety, labor rights in supply chain, child labor, and labor–management relations.

[32] I controlled IT capability by collecting data from the IW 500 database.

Table 3.2. Sample selection process

Sample selection step	
Number of data breaches from 2006 to 2014 reported by PRC or ITRC	10,193
Less: Number of data breaches that cannot be merge with COMPUSTAT	(*9,253*)
Number of data breaches occurred in a US-listed firm.	940
Less: Number of data breaches which are without necessary data from KLD and TNIC	(*327*)
Number of data breaches with necessary data from all other datasets.	613
Final Sample: number of the firm-year observations	19,519

3.5.2. Variable Description

3.5.2.1.Dependent Variable: Data Breach Risk

I calculated my dependent variable, namely, data breach risk (*BREACH*), as the accumulated number of data breaches in the subsequent fiscal year.[33]

3.5.2.2.Independent Variable: Employee-Related CSR

Consistent with CSR constructions used in prior literature (e.g., Koh et al. 2014; Wang and Choi 2013), I measured employee-related CSR (*EMPLOYEE_CSR*) by calculating the difference between the *strength score* (i.e., total CSR ratings in the strength component) and *concern score* (i.e., total CSR ratings in the concern component). This approach specifically involves two potential problems. First, the rating items were not entirely consistent across years. I followed Chen and Ho (2019) to solve this problem by simply considering the CSR rating items consistently through my sample period (i.e., 2005 to 2013).[34] Second, I focused on the comparability between strength and concern scores. I raised this problem because the total number

[33] As one robustness check, I used an alternative measure of data breach risk (*BREACH_DUMMY*), which represents an indicator variable that equals 1 if a firm reported a breach in the subsequent fiscal year and 0 otherwise.

[34] Among the 15 (9) rating items included in the strength (concern) component, 10 (6) items that are consistent over the years were considered in measuring CSR in the main analysis. I also constructed an alternative CSR measurement in my robustness check by considering all (consistent and inconsistent) rating items. I repeated my main analyses by using the alternative CSR measure (see Table 6). Table B in Appendix B lists the detailed information on the rating items used in this study.

of CSR rating items in the strength and concern components are unequal.[35] I followed prior studies (e.g., Tong et al. 2020) in adopting a *standardization* approach to solve this problem.[36]

3.5.2.3.Moderator: Negative Performance

I measure negative performance of firms by *strictly* following prior studies (e.g., Greve 2003; Parker et al. 2017). That is, I calculated the historical aspiration performance as the mean of firms' return on asset (ROA) in the past two years, and the social aspiration performance as the contemporaneous median profitability of all entities within each four-digit SIC industry. I calculated the historical (social) negative performance of the focal firm as the difference between its actual and historical (social) aspiration performance. Lastly, I measured negative performance (*NEG_PER*) as the average absolute value of historical and social negative performances.

3.5.2.4.Moderator: Environmental Dynamism

I *strictly* followed well-cited studies (e.g., Dess and Beard 1984; Keats and Hitt 1988) to compute environmental dynamism (*DYNAMISM*) by regressing industry sales in a five-year period and standardizing the resulting standard error of the regression coefficient by the average industry sale for each three-digit SIC code. The high values of *DYNAMISM* indicate increased industry volatility and environmental dynamism.

3.5.2.5.Moderator: Product Similarity

Consistent with prior work (e.g., Kim et al. 2016; Li and Zhan 2018), I measured

[35] In the employee dimension of the KLD database, the strength (concern) component contains 15 (9) rating items.

[36] That is, I obtained the difference between the strength (concern) score and the sample mean and divided the outcome by the sample standard deviation. I then used this standardized CSR measurement in the main analysis. Thereafter, to ensure robustness, one of my robustness checks repeated the main analysis by replacing the scandalized CSR measure with the unstandardized one (see Table 7).

product similarity using the *TNIC3TSIMM* variable in the TNIC data set provided by Hoberg and Phillips (2010; 2016). Each firm-year's *TNIC3TSIMM* value is the total sum of product similarities between firms and competitors within their industry.[37]

3.5.2.6.Control Variables

I controlled for firm characteristics that may affect data breach risk. First, given that large firms are at greater risk of being involved in data breaches, I controlled for firm size (*SIZE*) by using the natural logarithm of the value of total assets (in $millions) in a fiscal year. Second, firms' capital can determine whether these organizations have sufficient resources or capital to invest in information security if necessary. Hence, I controlled for firm leverage (*LEVERAGE*), which is the natural logarithm of division between initial total liabilities and initial total assets (Aivazian et al. 2005). Third, given that innovative firms are relatively attractive to external hackers, I included R&D expense (*R&D*) as another control, which is calculated as the log of the R&D expenses (in $millions). Fourth, given that advertisements may enhance the possibility of firms becoming the targets of hackers, I also included advertising intensity (*ADVERTISING*) as an additional control, which is calculated as a firm's advertising expense scaled by its total assets. Fifth, given that an increased IT capability enables a firm to reinforce its security defense capability, I controlled for IT capability (*IT_CAPA*) and I followed prior studies (e.g., Bharadwaj 2000; Chari et al. 2008) to operationalize *IT_CAPA*.[38] Sixth, given that some information breaches were the

[37] Online appendix (http://hobergphillips.tuck.dartmouth.edu/idata/Readme_tnic3HHIData.txt) provides a detailed description of the TNIC data set and the variable of *TNIC3TSIMM*.

[38] *IT_CAPA* is an indicator variable that is equal to 1 if a firm was ranked on Information Week (IW) 500 for the focal year and 0 otherwise

result of operational leanness, I controlled for and measured operational slack (*OP_SLACK*) by using the natural logarithm of the industry-adjusted ratio of annual sales to tangible assets. Seventh, I controlled for firms' total number of previous breaches (*BREACH_PRE*). This control is very important because it can generally index the endogenous factors of firms' security vulnerabilities. Finally, society-facing CSR (*SOCIETY_CSR*) is found the increase data breach risk (D'Arcy et al. 2020), I hence control the variable. I followed D'Arcy et al. (2020) and operationalize this variable by summing the strength variables that are specific to the community and environment dimensions of KLD.

I also included variables to control for the firm- and year-fixed effects. Firm-fixed effects account for unobserved heterogeneity, thereby reducing the concerns associated with time-invariant omitted firm characteristics that correlate with firms' data breach risk. Year-fixed effects control for any systematic differences across these years that could influence firms' security risks. Detailed definitions and data sources of all variables used in this study are summarized in Table A (Panel B) of Appendix A. Table 3.3 presents the descriptive statistics for my main regression variables.

Table 3.3. Descriptive Statistics and Correlations

Variables	**Mean**	***S.D.***	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
(1) *BREACH*	0.031	0.205	1											
(2) *EMPLOYEE_CSR*	-0.168	1.406	**-0.043**	1										
(3) *NEG_PER*	-0.051	0.498	**0.012**	-0.006	1									
(4) *DYNAMISM*	0.128	0.097	**-0.042**	**-0.061**	0.009	1								
(5) *TNIC3TSIMM*	7.403	14.019	**0.016**	**0.057**	**-0.031**	**-0.152**	1							
(6) *SIZE*	7.403	1.684	**0.219**	**-0.049**	**0.100**	-0.010	**0.222**	1						
(7) *LEVERAGE*	0.193	0.214	**0.022**	**-0.049**	**-0.023**	**0.089**	**-0.150**	**0.193**	1					
(8) *R&D*	0.032	0.071	**-0.028**	**0.112**	**-0.184**	**-0.151**	**-0.029**	**-0.288**	**-0.153**	1				
(9) *ADVERTISING*	0.013	0.04	0.006	**-0.020**	**0.014**	**0.034**	**-0.107**	**-0.111**	-0.006	**-0.031**	1			
(10) *IT_CAPA*	0.039	0.194	**0.103**	**-0.027**	**0.016**	**-0.045**	**-0.025**	**0.218**	**0.014**	**-0.017**	-0.007	1		
(11) *OP_SLACK*	-0.165	0.621	-0.009	0.0110	**-0.229**	**-0.013**	**0.034**	**-0.063**	**-0.027**	**0.070**	**0.091**	0.001	1	
(12) *BREACH_PRE*	0.075	0.263	**0.269**	**0.015**	**0.019**	**-0.062**	**0.033**	**0.342**	**0.062**	**-0.040**	**0.029**	**0.179**	**0.015**	1
(13) *SOCIETY_CSR*	0.176	0.879	**0.081**	**0.169**	**0.018**	**-0.100**	**-0.041**	**0.244**	0.008	**0.052**	**0.043**	**0.126**	0.009	**0.192**

3.6.RESEARCH DESIGN AND EMPIRICAL RESULTS

3.6.1. Baseline Results

Table 3.4 gives the regression analysis results on the basis of a sample of 19,519 firm-year observations. I conducted my analyses by using a Poisson regression with cluster robust standard errors because of the following reasons. First, my dependent variable (*BREACH*) is a count variable, and I collected the data in multiple years. To model count variable in a panel setting, fixed effects Poisson regression is highly appropriate. That is because, unlike negative binomial regression, Poisson fixed effects model is unlikely to suffer "incidental parameters problem" (Greene, 2012). Wooldridge (2010: 763) also argues that the fixed effects Poisson estimator "has very strong robustness properties for estimating the parameters in the conditional mean." Second, Cameron and Trivedi (2010: 627) argue that "the Poisson panel estimators rely on weaker distributional assumptions—essentially, correct specification of the mean—and it may be more robust to use the Poisson panel estimators with cluster-robust standard errors." Thus, I adopted cluster robust standard errors in my regression.

In particular, my panel regression model is as follows:

$$\begin{aligned} BREACH_{ij} = {} & \beta_0 + \beta_1 EMPLOYEE\_CSR_{ij} + \theta_1 IEMPLOYEE\_CSR_{ij} \times NEG\_PER_{ij} \\ & + \theta_2 EMPLOYEE\_CSR_{ij} \times DYNAMISM_{ij} + \theta_3 EMPLOYEE\_CSR_{ij} \times TNIC3TSIMM_{ij} \\ & + \kappa_1 NEG\_PER_{ij} + \kappa_2 DYNAMISM_{ij} + \kappa_3 SIMILARITY_{ij} + \sum_{r=1}^{8} \alpha_r CONTROL_{ij} + \upsilon_i + \omega_j + \varepsilon_{ij}, \end{aligned} \quad (1)$$

where β_1 is the coefficient of the independent variable; θ_n, $n \in [1, 2, 3]$ capture the moderating effects of the moderators; υ_i and ω_j represent the firm- and year-fixed effects; and ε_{ij} is the error term.

Model 1 introduces the control variables only. As expected, larger firm (*SIZE*), firms with more attention (*ADVERTISING*), firms with more surplus resource (*OP_SLACK*) are associated with higher data breach risks.

Model 2 introduces the independent variable (*EMPLOYEE_CSR*) and includes the moderators as additional controls. The coefficient of the *EMPLOYEE_CSR* variable is negative and significant ($\beta = -0.084$, $p < 0.05$), indicating that high-level employee-related CSR decreases tend to reduce firms' data breach risk. In particular, given a one-standard-deviation (1.406) increase in firms' employee-related CSR, the *logarithm count* of firms' data breaches is expected to decrease by approximately $0.084 \times 1.406 = 0.118$.[39]

Model 3 introduces the interaction term (*EMPLOYEE_CSR* × *NEG_PER*). The coefficient of the interaction term is significant and negative ($\beta = -2.329$, $p < 0.1$), suggesting that the negative relationship between employee-related CSR and data breach risk is strong in firms with negative performance.[40] Thus, H3-2 is supported. Model 4 introduces the interaction term (*EMPLOYEE_CSR* × *DYNAMISM*). The coefficient of the interaction term is significantly negative ($\beta = -0.538$, $p < 0.05$). This result suggests that the CSR–security relationship is strong when external environments are highly dynamic.[41] Thus, H3-3 is supported. Model 6 introduces the interaction term (*EMPLOYEE_CSR* × *TNIC3TSIMM*). The coefficient of the interaction term is significant and negative ($\beta = -0.007$, $p < 0.01$), indicating that the effect of employee-related CSR on data breach risk is strong when firms' products are

[39] The incidence rate ratio (IRR; estimated rate ratio for a one-unit increase in employee-related CSR) is $e^{-0.084} = 0.919$, suggesting that for a one-unit increase in firms' employee-related CSR, the data breach risk is reduced by 8.1% (1-0.919=0.081).

[40] The decreasing effectiveness of firms' employee-related CSR on their breach number will be further decreased by approximately 1.160 (2.329×0.498) with a one-standard-deviation (0.498) increase in firms' negative performance.

[41] Employee-related CSR is expected to further reduce breach number by approximately 0.052 (0.538×0.097) with a one-standard-deviation (0.097) increase in environmental dynamism.

highly similar to their rivals.[42] Thus, H3-4 is supported. Finally, Model 6 includes all the moderators and shows entirely consistent moderating effects.

To mitigate the concern that the introduction of firm fixed-effects into the regression considerably reduced the sample size by dropping the observations where firms had not experienced a data breach during my sample period, I replaced firm-fixed effects with industry-fixed effects to control for unobserved time and industry trends. The related results are presented in Models 7 and 8, supporting all my hypotheses.

Table 3.4. Regression Analysis Results

	Fixed-effect Poisson (*BREACH*)						Poisson (*BREACH*)	
Variables	**Model1**	**Model2**	**Model3**	**Model4**	**Model5**	**Model6**	**Model7**	**Model8**
EMPLOYEE_CSR		**-0.084****	-0.106***	-0.033	-0.034	0.011	**-0.054****	0.008
		[0.035]	[0.036]	[0.043]	[0.035]	[0.041]	**[0.024]**	[0.034]
EMPLOYEE_CSR			**-2.329***			**-2.296***		**-1.691****
×NEG_PER			**[1.196]**			**[1.218]**		**[0.672]**
EMPLOYEE_CSR				**-0.538****		**-0.676*****		**-0.515***
×DYNAMISM				**[0.228]**		**[0.223]**		**[0.300]**
EMPLOYEE_CSR					**-0.007*****	**-0.008*****		**-0.005****
×TNIC3TSIMM					**[0.002]**	**[0.002]**		**[0.002]**
NEG_PER		0.055	-0.174	0.061	0.113	-0.113	0.857	1.463*
		[0.463]	[0.414]	[0.471]	[0.568]	[0.503]	[0.921]	[0.779]
DYNAMISM		4.018**	4.074**	3.269	4.125**	3.299	-0.041	-0.411
		[1.964]	[1.985]	[2.044]	[1.889]	[2.010]	[0.652]	[0.722]
TNIC3TSIMM		-0.003	-0.004	-0.003	-0.001	-0.002	-0.019***	-0.019***
		[0.014]	[0.014]	[0.014]	[0.013]	[0.013]	[0.005]	[0.005]
SIZE	0.580***	0.478**	0.530***	0.483**	0.508***	0.562***	0.656***	0.662***
	[0.204]	[0.199]	[0.192]	[0.199]	[0.193]	[0.187]	[0.041]	[0.041]
LEVERAGE	0.919	1.046	0.862	1.046	0.820	0.643	0.419*	0.409*
	[0.626]	[0.658]	[0.619]	[0.643]	[0.643]	[0.596]	[0.231]	[0.231]
R&D	3.233	2.470	3.194	2.441	2.695	3.320	2.879***	2.926***
	[2.310]	[2.409]	[2.559]	[2.395]	[2.353]	[2.451]	[0.670]	[0.695]
ADVERTISING	10.377**	10.365**	9.922*	10.383**	10.529**	10.149**	3.776***	3.857***
	[5.214]	[5.141]	[5.114]	[5.156]	[5.156]	[5.149]	[1.249]	[1.254]
IT_CAPA	-0.014	-0.037	-0.044	-0.036	-0.119	-0.129	0.017	-0.024
	[0.143]	[0.142]	[0.143]	[0.143]	[0.146]	[0.147]	[0.135]	[0.136]
OP_SLACK	-0.315*	-0.334**	-0.317**	-0.332**	-0.323**	-0.305**	-0.064	-0.063
	[0.164]	[0.158]	[0.160]	[0.157]	[0.154]	[0.154]	[0.088]	[0.088]
BREACH_PRE	-2.077***	-2.105***	-2.137***	-2.117***	-2.154***	-2.200***	0.709***	0.693***
	[0.243]	[0.235]	[0.236]	[0.235]	[0.236]	[0.235]	[0.166]	[0.167]
SOCIETY_CSR	-0.047*	-0.043	-0.039	-0.043	-0.040	-0.037	-0.001	0.001
	[0.026]	[0.027]	[0.027]	[0.026]	[0.026]	[0.026]	[0.017]	[0.017]
Firm Dummies	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Industry Dummies	No	No	No	No	No	No	Yes	Yes
Year Dummies	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Number of observations	2,593	2,593	2,593	2,593	2,593	2,593	19,519	19,519

Notes. The sample consists of 19,519 firm-years for 3,075 unique firms from 2005 to 2013. The dependent variable is *BREACH* and is measured in year *t*+1. All variables are defined in Table A (Panel B) of Appendix A in online appendix. Models 1−6 use fixed-effect Poisson regression analysis, and include firm and year fixed effects in the

[42] Given a one-standard-deviation (14.091) increase in product similarity, the reduction in data breach number that is driven by employee-related CSR will further decrease by approximately 0.099 (0.007 × 14.091).

regression (*the observations where firms had not experienced a data breach during my sample period were dropped in the regression*). Models 7 and 8 use Poisson regression and include industry-fixed effects in the regressions. Robust standard errors are in parentheses. The symbols ∗∗∗, ∗∗, and ∗ denote significance at the 1%, 5%, and 10% levels, respectively.

3.6.2. Robustness Checks

3.6.2.1.Alternative Measure of the Independent Variable

In the main analysis, I measured the independent variable (*EMPLOYEE_CSR*) as the difference between the standardized sum of the strength and concern ratings, where standardization is used to mitigate the incomparability between the strength and concern scores (Tong et al. 2020). To ensure robustness, I alternatively measured employee-related CSR (*EM_CSR_UNSTD*) without using standardization. Table 3.5 presents the description of the variable *EM_CSR_UNSTD*.

Table 3.5. An Alternative Measures of Employee-Related CSR

	Fixed-effect Poisson (*BREACH*)				
	(1)	(2)	(3)	(4)	(5)
EM_CSR_UNSTD	**-0.108****	-0.140***	-0.076	-0.032	-0.019
	[0.053]	[0.052]	[0.078]	[0.055]	[0.075]
EM_CSR_UNSTD×NEG_PER		**-3.720*****			**-3.562*****
		[1.180]			**[1.183]**
EM_CSR_UNSTD×DYNAMISM			**-0.318**		**-0.468**
			[0.595]		**[0.569]**
EM_CSR_UNSTD×TNIC3TSIMM				**-0.008*****	**-0.008*****
				[0.003]	**[0.003]**
Moderators	Included	Included	Included	Included	Included
Controls	Included	Included	Included	Included	Included
Firm Dummies	Yes	Yes	Yes	Yes	Yes
Year Dummies	Yes	Yes	Yes	Yes	Yes
Number of observations	3,212	3,212	3,212	3,212	3,212

Notes. *I* repeated the Models 2−6 in the main analysis by alternatively measuring employee-related CSR (*EM_CSR_ALLITEM*). All variables are defined in Table A (Panel B) of Appendix A in online appendix. Firm and year fixed effects are included in the regression. Robust standard errors are in parentheses. The symbols ∗∗∗, ∗∗, and ∗ denote significance at the 1%, 5%, and 10% levels, respectively.

3.6.2.2.Alternative Measure of the Dependent Variable

I alternatively measured data breach risk (*BREACH_DUMMY*) as an indicator variable that equals 1 if firms reported a breach in the subsequent fiscal year and 0 otherwise. I repeated my main analyses by replacing *BREACH* with

BREACH_DUMMY. I followed prior data breach risk literature (D'Arcy et al. 2020; Haislip et al. 2021) and adopted a fixed-effect ordinary least squares (OLS) regression. Results are show in Table 3.6, which are highly consistent with the ones in the main analyses.

Table 3.6. An Alternative Measures of Data Breach Risk

	Fixed-effect OLS (*BREACH_DUMMY*)				
	(1)	(2)	(3)	(4)	(5)
EMPLOYEE_CSR	**-0.003****	-0.003**	0.000	0.002	-0.006***
	[0.001]	[0.001]	[0.002]	[0.001]	[0.001]
EMPLOYEE_CSR×NEG_PER		**-0.019**			**-0.021**
		[0.013]			**[0.013]**
EMPLOYEE_CSR×DYNAMISM			**-0.024***		**-0.036*****
			[0.013]		**[0.013]**
EMPLOYEE_CSR×TNIC3TSIMM				**-0.001*****	**-0.001*****
				[0.000]	**[0.000]**
Moderators	Included	Included	Included	Included	Included
Controls	Included	Included	Included	Included	Included
Firm Dummies	Yes	Yes	Yes	Yes	Yes
Year Dummies	Yes	Yes	Yes	Yes	Yes
Number of observations	19,519	19,519	19,519	19,519	19,519
adj. R^2	0.029	0.029	0.029	0.032	0.033

Notes. ***I*** repeated the Models 2−6 in the main analysis by changing my model into fixed-effect OLS regression. All the independent variables are measured in year t. All variables are defined in Table A (Panel B) of Appendix A in online appendix. Firm and year fixed effects are included in the regression. Robust standard errors are in parentheses. The symbols ∗∗∗, ∗∗, and ∗ denote significance at the 1%, 5%, and 10% levels, respectively.

3.6.2.3.*Endogeneity and Heckman Correlation*

I cannot neglect the potential that there are inherent differences between employee-related CSR firms that covered by KLD database and others. Failing to account for such an endogeneity concern in CSR may lead to biased results. For instance, the employee-related CSR firms covered by KLD might possess sufficient resources or in idle markets.

To mitigate such a concern, I adopted a Heckman selection two-stage analysis (Heckman 1977). I *strictly* followed Wiengarten et al. (2019) in conducting the test. That is, Heckman (1977) two-stage analysis entails using at least one predictor related to firms' relative performance that is exogenous to the focal firm. I followed

Wiengarten et al. (2019) and adopted industry munificence and concentration are two ideal choices given that they can capture firms' external economic conditions and external competitiveness, respectively. In addition, I followed Wiengarten et al. (2019) and included certain basic corporate economic indexes (i.e., ROA, firm size, leverage, and age) as additional predictors. The aforementioned predictors enabled me to generate inverse Mills ratio (*IMR*) by using a probit model. I repeated the main analyses by adding *IMR* as an additional control and achieved consistent results (see Table 3.7).

Table 3.7. Heckman Correlation

	Fixed-effect Poisson (*BREACH*)				
	(1)	(2)	(3)	(4)	(5)
EMPLOYEE_CSR	**-0.081****	-0.102***	-0.028	-0.034	0.013
	[0.035]	[0.036]	[0.043]	[0.035]	[0.041]
EMPLOYEE_CSR×NEG_PER		**-2.266****			**-2.247***
		[1.137]			**[1.174]**
EMPLOYEE_CSR×DYNAMISM			**-0.559****		**-0.684*****
			[0.228]		**[0.223]**
EMPLOYEE_CSR×TNIC3TSIMM				**-0.007*****	**-0.007*****
				[0.002]	**[0.002]**
IMR	-2.701	-2.548	-2.794	-2.088	-2.013
	[2.067]	[2.002]	[2.057]	[2.016]	[1.947]
Moderators	Included	Included	Included	Included	Included
Controls	Included	Included	Included	Included	Included
Firm Dummies	Yes	Yes	Yes	Yes	Yes
Year Dummies	Yes	Yes	Yes	Yes	Yes
Number of observations	2,593	2,593	2,593	2,593	2,593

Notes. *I* repeated the Models 2−6 in my main analysis by adding *IMR* as an additional control. All variables are defined in Table A (Panel B) of Appendix A in online appendix. Firm and year fixed effects are included in the regression. Robust standard errors are in parentheses. The symbols ∗∗∗, ∗∗, and ∗ denote significance at the 1%, 5%, and 10% levels, respectively

3.6.2.4.Endogeneity and Two-stage Residual Inclusion (2SRI) Approach

I then checked for endogeneity problems. I recognize that employee-related CSR and security risks might be endogenous. For example, certain unobserved time-variant factors might drive both firms' employee-related CSR and occurrences of data breach. To mitigate the endogenous concern, I adopted a 2SRI approach (Terza et al. 2008), which has been increasingly used by business research to avoid endogeneity bias

(Gamache et al. 2020; Li et al. 2018; Maksimov et al. 2019; Turner and Rindova 2018). The first stage of the test (instrument variable approach) requires the instrument to correlate with employee-related CSR and not be a direct cause of data breach. I adopted two strong instruments in the step. First, unemployment insurance (UI) benefits, as a policy initiated by the local government, has been used by Flammer (2015) as a natural shock to stimulate firms' employee-related CSR.[43] Meanwhile, such a policy is exogenous to firm's data breach incidences. Thus, UI benefit (*UI_BENEFIT*) is a highly ideal instrumental variable. Second, the previous year' employee CSR (*PRE_EM_CSR*) is also a good instrument because it can affect the focal firm's employee-related CSR level via a coherent strategic orientation in the firm, but it would not be a direct cause of (exogenous to) the focal firm's data breach in the next year.

With the two instrument variables, I performed regressions using a two-stage residual inclusion (2SRI) approach (the results are shown in the Model 1 of Table 3.8). In the second stage of the 2SRI test, I adopted the residual from the first stage (i.e., *RESIDUAL*) as an additional control in my model and achieved the results (see Model 2 to 6 in Table 3.8) which are highly consistent with the ones in the main analysis, thereby mitigating endogeneity problems.

Table 3.8. 2SRI Approach

	Fixed OLS (*BREACH*)	Fixed-effect Poisson (*BREACH*)				
	(1)	(2)	(3)	(4)	(5)	(6)
EMPLOYEE_CSR		**-0.123***	**-0.134***	-0.077	-0.070	-0.018
		[0.074]	**[0.076]**	[0.075]	[0.072]	[0.074]
EMPLOYEE_CSR×NEG_PER			-0.979			-0.916
			[0.745]			[0.837]
EMPLOYEE_CSR×DYNAMISM				**-0.501****		-

[43] Flammer (2015) suggests that firm tend to investment more resource in employed-related CSR to mitigate the negative effect of UI benefits.

				[0.225]		**0.644*** [0.220]**
EMPLOYEE_CSR×TNIC3TSIMM					**- 0.007*** [0.002]**	**- 0.007*** [0.002]**
UI_BENEFIT	**0.051 *** [0.011]**					
PRE_EM_CSR	**0.459*** [0.012]**					
RESIDUAL		0.047 [0.075]	0.050 [0.075]	0.049 [0.076]	0.042 [0.075]	0.046 [0.075]
Moderators	Included	Included	Included	Included	Included	Included
Controls	Included	Included	Included	Included	Included	Included
Firm Dummies	Yes	Yes	Yes	Yes	Yes	Yes
Year Dummies	Yes	Yes	Yes	Yes	Yes	Yes
Number of observations		2,593	2,593	2,593	2,593	2,593

Notes. Col. 1 reports the results in the first step of 2SRI approach. I followed Agrawal and Matsa (2013) and Cols. 2−6 report the results in the second step of 2SRI. In the second step of 2SRI, I repeated the Models 2−6 in the main analysis by adding *RESIDUAL* as an additional control. All variables are defined in Table A (Panel B) of Appendix A in online appendix. Firm and year fixed effects are included in the regression. Robust standard errors are in parentheses. The symbols ∗∗∗, ∗∗, and ∗ denote significance at the 1%, 5%, and 10%.

3.7.DISCUSSION AND IMPLICATIONS

3.7.1. General Discussion

The current study presents the following research questions:

(1) How does firms' employee-related CSR influence their data breach risks?

(2) How does negative performance, environmental dynamism, or product similarity individually moderate the association between employee-related CSR and data breach risks?

I exerted theoretical and empirical effort to answer my research questions. For the theoretical aspect, I synthesized the extensive agency theory literature and applied it in the CSR and security contexts. I used the principal–agent framework as basis to propose that employee-related CSR could reduce the security threats of firms via alignment incentives, informal monitoring, and differentiation. These security beneficial levers of employee-related CSR are analogous to clan control, which regulate employees' security behaviors via fostering peer interactions, promulgating

shared values and norms, and aligning the goals of members in terms of information security.

For the empirical aspect, I used secondary data in a longitudinal setting as the basis to conduct a rigorous examination of the CSR–security nexus and moderating effects. Accordingly, I achieved empirical results that are entirely consistent with my predictions. That is, I found that employee-related CSR can effectively reduce firms' likelihood of data breaches. Such an influence is particularly strong when organizations suffer from deteriorating economic performance, face turbulent environments, or encounter high product similarity with their competitors.

My findings yielded substantial theoretical and practical implications, which are discussed as follows.

3.7.2. Theoretical Implications

The present study has several contributions to the academic literature. First, my study may advance the behavioral information security research, which has extensively investigated the influence of employees' behaviors on information security. However, given that an overwhelming majority of the related studies have been conducted in an individual level, whether their theories and findings are available in an organizational level have yet to be sufficiently supported. Therefore, I may push the behavioral information security research forward by applying and testing its theories in an organizational level.

Second, the present study may extend the limited scope of the research on

organizational determinants of data breaches. Despite the long-term call for security research from the organizational perspective (Ernest Chang and Ho 2006; Vermeulen and Von Solms 2002), only a few attempts have been made to investigate how organizational factors influence firms' data breach likelihood (D'Arcy et al. 2020). Beyond this effort, the limited research in this realm has generally constricted their foci within the technical domain, and few of them have uncovered how human-related strategies can influence data breach risks. Therefore, the current study expands this line of research by proposing employee-related CSR as a novel organizational determinant of data breaches.

Third, the current study may contribute to the CSR research by providing relatively direct empirical discussion in terms of employee reactions. CSR researchers are developing increased interest on the relationship between CSR and employee behaviors (e.g., Flammer and Kacperczyk 2019; Flammer and Luo 2017; Gubler et al. 2018). However, observing employee behaviors empirically is typically difficult because organizations' internal systems are often prohibited from measuring and tracking their sustainability influence. Thus, direct empirical evidence on this topic (i.e., CSR and employee behaviors) is considerably limited. This study focuses on the security context and contributes to the literature by presenting a relatively direct empirical investigation on the relationship between CSR and employee behaviors.

3.7.3. Practical Implications

Several meaningful practical implications can be drawn from this study. First,

despite the long-term use of security technologies for the majority of organizations, practitioners have considerably acknowledged that technological tools alone are markedly insufficient. These organizations have also realized the frequent inefficacy of formal security practices in monitoring the security-related procedures and operations of their employees. Such practical limitations of technologies and formal monitoring are also academically supported by various empirical evidence. For example, the findings of prior studies have suggested that security technologies (Angst et al. 2017; Sen and Borle 2015) or formal monitoring (e.g., punishment) (Herath and Rao 2009a; Pahnila et al. 2007) are relatively ineffective in reducing enterprise security threats. However, the strategies that are truly effective to defend against total data breaches have been barely supported by empirical evidence. Consequently, managers are practically constrained in their ability to apply empirical academic knowledge to sufficiently protect sensitive enterprise information. Against such a backdrop, my findings can explicitly remind managers that they can reinforce corporate security controls through a "do good by doing good" manner, particularly by increasing their investments on employee-related CSR.

Second, an evident and significant increase in employees' involvement in CSR activities is observed. Accordingly, this trend suggests that enterprise CSR effort is substantially integrated into the cultural fabric of an increasing number of organizations. Given the high emphasis on CSR, my findings facilitate the advancement of managers' understanding of the benefits of their CSR effort. That is, investing on employee-related CSR programs generates economic benefits and also

facilitates the reduction of firms' information security concerns.

Third, the current results can remind managers that the role of employee-related CSR in reducing data breach risk can be strengthened if organizations operate in a loss position, dynamic setting, or market with similar products. Managers may achieve enhanced security benefits from their CSR effort if these contexts are incorporated into their employee-related CSR decisions.

3.7.4. Limitations and Future Research

Similar to other empirical studies, my results are also subject to limitations, thereby possibly providing avenues for future research. First, my arguments refer to the concept of clan control and suggest that employee-related CSR's security functions are analogous to clan control. However, information security should leverage *other forms of control* that do not rely on trust or values, such as zero trust modes and access controls. Hence, future research may investigate whether an optimal point or trade-off exists between informal (e.g., social) and formal (e.g., technical) control systems. Second, the scope of the current study only extended to the occurrences of data breaches. Future studies may consider possible extensions to analyze whether CSR programs may help mitigate the negative impact of data breaches. Third, although the present research has brought the factors of environmental dynamic, negative performance, and product similarity in the security context, I only focused on the moderating roles of these factors. Therefore, future studies may consider investigating the direct influence of these factors on data breach risks. Lastly, I failed to control the

variable of security investment in my model because of data limitations. Hence, researchers may consider the corresponding improvement as a direction for future research.

Chapter 4. Firm Diversity, Data Breach Risk, and the Moderating Roles of Managerial Ability

4.1. INTRODUCTION

"*It's essential that organizations look at diversity as a key metric for [information security] success.*"[44] –Nicola Whiting, chief strategy officer at Titania

Given the numerous cases of high-profile data breaches, few firms need convincing that achieving business goals requires information security. Information security failures, or data breaches, can expose organizations to such risks as high financial penalties, brand damage, and lawsuits (Cavusoglu et al. 2004; Gwebu et al. 2018; Janakiraman et al. 2018; Kannan et al. 2007). However, even when the need for information security is fully recognized and adequately funded, or perhaps even over-funded, organizations continue to be plagued by an increasing number of serious security failures. Studies on information security have suggested that a possible source of this paradox stems from firms' inadequate attempts to detect vulnerabilities and control risks that *lie beyond IT and IS* (Alexander et al. 2013; Axelrod et al. 2009; Brotby 2009; Colwill 2009; Cram et al. 2019; Crossler et al. 2013; Hedström et al. 2011; Hsu et al. 2012; Hu et al. 2007; Moody et al. 2018).

The manner by which firms' data breaches is organizationally determined is a popular topic that has become the focus of recent research. Although security research has recently investigated how firms' data breach risk (i.e., likelihood to experience a

[44] https://uktechnews.co.uk/2019/10/25/information-security-industry-has-to-become-more-diverse-warns-chartered-institute-of-information-security/

data breach) is influenced by some organizational factors, such as IT security investment (Angst et al. 2017; Kwon and Johnson 2014; Sen and Borle 2015), IT governance (Higgs et al. 2016; Kwon et al. 2012; Liu et al. 2020), IS application (Wang et al. 2015), and meaningful-use attestation (Kwon and Johnson 2018), I note that research has largely limited its focus to organizational policies and actions that taken within the scope of IT and IS domains.

Against such a backdrop, to understand how firm factors impact data breach risk, I believe it is important to examine how firm non-technical policies, yet influence knowledge diversity, can influence information security. I believe so, because an increasing number of security experts and managers recently highlight the concept that *knowledge specialization does not benefit information security controls or security-related decision-making.*[45] For example, related to the experience that diversity can practically benefit information security controls, Ann Johnson, corporate VP of Microsoft's Cybersecurity Solutions Group, provided the following comment: "*I must remember that cybersecurity is people; the cyber defenders, the people who create the technology, and the people the technology protects. That is why at the core of it all, my security teams need to be as diverse as the problems I are trying to solve – because diversity is how I get the best security*."[46] Against the backdrop, to connect knowledge diversity to data breach risk, I examine *firm diversity*[47] (*diversified*

[45] Related news can be found in the following links: https://datafloq.com/read/diversity-cybersecurity-diverse-security-teams/7257, https://www.information-age.com/how-diversity-can-cyber-123477494/, https://betanews.com/2019/10/24/information-security-lack-diversity/, and https://www.teissrecruitment.com/lack-of-diversity-in-the-it-security-industry-worsening-the-skills-gap/, etc.

[46] https://cybersecurityventures.com/cybersecurity-is-people-cybersecurity-is-diversity/

[47] I adopt the term of "firm diversity" rather than "firm diversification" given the later term represents strategy (e.g., merger and acquisition) which expands firm operational scope and entails firm changes in a variety of aspects. However, "firm change" is not my focus, and my focus is firm structures that enable firms the diversified operations

operations in multiple industries) (Grant et al. 1988; Tallman and Li 1996; Varadarajan 1986), which enables firms to diversify their knowledge collection (Markides and Williamson 1994), influences their information security performance. Such an investigation is critical because it could offer firms insight into how to design firmwide non-technic and structural policies that comprehensively enhance information security. Accordingly, I propose my first research question: (1) *How does firm diversity influence their data breach risks*?

I draw from organizational diverse learning and security literatures to answer the question. I first take cues from security literature and discuss that information security protection is a highly complex, non-routine, and uncertain challenge (Alexander et al. 2013; Axelrod et al. 2009; Brotby 2009; Colwill 2009; D'Arcy et al. 2014). Such knowledge inspires me to investigate the diversity–security relationship from a *diverse learning* perspective, which suggests that a diverse learning mode are highly effective and needed in solving complex, non-routine, and uncertain problems (Hambrick et al. 1996; Jehn et al. 1999; Matusik and Fitza 2012). Moreover, given knowledge relatedness and an effective knowledge transfer are important premises for enabling diverse learning (Beckman and Haunschild 2002; Hambrick et al. 1996; Schilling et al. 2003), I then discuss why such premise are valid in my context. That is, current firms' networks are highly interconnected. The weakest point of one unit may also become the largest security vulnerability of another, making security a bigger organizational issue and requiring the collaboration among different firm units to direct

in multiple industries. Thus, the term of "firm diversity" is more appropriate in such a context.

and control information security. As a result, current firms' security-related decision-making, which ranges from security policy development to security threat identification and responses, is generally uniform and coordinated (Calder and Watkins 2012; Kayworth and Whitten 2010).

Then, I infuse the foregoing background into my theorizing. Drawing from organizational diverse learning literature, which suggests that a diverse learning mode can benefit organizations' learning process in various ways, such as accelerating learning curves (Schilling et al. 2003), stimulating deliberate thinking (Beckman and Haunschild 2002; Jehn et al. 1999), and facilitating complex problem solving (Matusik and Fitza 2012; Van Der Vegt and Bunderson 2005), I expect that firms' multi-industry operations tend to improve their abilities in protecting information security in ways that reduce data breach risks. Moreover, I examine such a diversity–security relationship further by focusing on different types of diversity (i.e., related versus unrelated diversity), given related variations are suggested to yield further learning benefits (Schilling et al. 2003).

After establishing the relationship between firm diversity and data breach risk, whether this effectiveness is contingent upon other factors is also important. I particularly focus on the moderator of *managerial ability*. That is because, in my theory, firms' diverse security learning across industries essentially enables an improved security protection and a reduced data breach risk, and the chairperson to monitor such a cross-industry security learning is commonly a board member (Kayworth and Whitten 2010). Calder and Watkins (2012) suggested that the most

significant characteristic for security chairpersons is their managerial abilities, such as interpersonal and project management skills, rather than their IT competency. Thus, I may expect that cross-unit security interrelationships can be highly effective under the guidance of capable top managers, thereby moderating the firm diversity–security relationship.

To summarize, the objective of this study is to analyze the relationships among (total, related versus unrelated) diversity, managerial ability as the moderator, and data breach risk. The research questions are empirically tested using longitudinal secondary data of US-listed firms over an 11-year period (2006–2016). The empirical results in nearly all my tests are highly consistent with my hypotheses and suggest that data breach risk is reduced as the level of firm diversity increases, particularly in the context of related diversity. Meanwhile, such a benefit of firm diversity to reduce data breach risk is strengthened when managerial ability is high, particularly in related diversified firms.

This study contributes to the literature in the following aspects. First, the current study may advance the prior information security research. The prior security works (e.g., Alexander et al. 2013; Axelrod et al. 2009; Brotby 2009) have theoretically emphasized the importance of investigating information security issues beyond the traditional IT domain. However, I note that the now-burgeoning scholarly debate as to the organizational determinants of data breach risk has generally centered on the perspectives of IT and IS (see the literature review in Subsection 2.1). This debate remains markedly limited because the literature has yet to investigate the security

effectiveness of firm structure. Such a lack of attention is alarming because the seamless Internet-connectivity entails information security to be controlled collaboratively among all business units in a firm (Kayworth and Whitten 2010). To the best of my knowledge, this research is the first to empirically examine discourse on information security from a non-technical and structural perspective, bridging the aforementioned research gaps. This study also contributes to the security literature by introducing organizational diverse learning theory to analyze how firms can comprehensively protect information security.

Second, I may contribute to the firm diversity literature by broadening the extant understanding of the rationale for diversity. Such an exploration expands the traditional debate on the effectiveness of firm diversity into the novel range of information security, and initially quantifies the security effectiveness of firm diversity. My results are also consistent with previous firm diversity literature in terms that related diversity is superior to unrelated diversity (e.g., Grant et al. 1988).

Third, my boundary condition analysis helps complement the potential "missing link" in applying organizational learning theory and firm diversity to security research. I determined that the security benefits of firms' multi-industry operations vary with firms' managers' ability. Thus, my investigation on the moderating influence advances the organizational learning and firm diversity literatures by showing that firms' managerial ability intervenes in the association between their diversified operations and information security outcome.

4.2.LITERATURE REVIEW

4.2.1. Data Breach

Data breach refers to the malicious or accidental leakage of confidential or private information to unauthorized parties (Cheng et al. 2017b; Sen and Borle 2015). Although they have a common outcome, data breaches may occur for different reasons. That is, information may be leaked by insiders or outsiders, with either malicious or inadvertent intent (Kwon and Johnson 2018). However, given the widespread reports of a few high-profile hackings and malware insertion incidents, the public tends to believe that other data breaches are due to similar external malicious attacks. However, this is a misperception, as less than half of data breaches are intentionally caused by outsiders through hacking or malware (Hauer 2015), while the majority are due to negligence, human error, and other non-malicious behaviors (Cram et al. 2019; Crossler et al. 2013).

Security scholars in the past few decades have been continuously developing appropriate data breach prevention measures. Traditionally, substantial technological measures against security threats have been proposed, such as sensitive data scanning (Shu et al. 2015), machine learning (Hart et al. 2011), collection intersection (Liu et al. 2015), and watermarking (Papadimitriou and Garcia-Molina 2011). Nevertheless, the solutions offered by these isolated improvements to technical tools are considerably limited because successful security controls should include improved techniques, enhanced security awareness, and proper enforcement of security policies (Colwill 2009). An over-reliance on technology without considering other factors can have

disastrous consequences for information security (D'Arcy et al. 2014; D'Arcy and Teh 2019).

Therefore, security scholars have increasingly called for further research on data breach solutions from the organizational and managerial perspectives. Several recent studies have responded and proposed a few organizational factors that can influence firms' data breach risks. First, some studies in the research strand focus on the *IT security investment*. Sen and Borle (2015) drew on the opportunity theory of crime, institutional anomie theory, and institutional theory to identify factors that increase or decrease the contextual risk of data breach. They revealed that investment in IT security is likely to increase the data breach risk within both state and industry sectors. Kwon and Johnson (2014) empirically demonstrated a direct negative association between firms' proactive IT security investments and the failure rate of information security, and they also found that such an association can be mitigated by external pressure. Angst et al. (2017) also focused on how IT security investments can influence data breach risk and determined that institutional factors create conditions under which IT security investments can effectively prevent data breaches.

IT governance is another proposed organizational determinant of data breach risk. Kwon et al. (2012) showed that an IT executive's involvement in top management is negatively related to the possibility of data breaches. They also found that differences in the amount of compensation between IT and non-IT executives is negatively associated with the likelihood of data breaches. In addition, Higgs et al. (2016) drew on signaling theory and showed that firms with technology committees are more likely

to report breaches than firms that lack such committees. Liu et al. (2020) found that universities with centralized IT governance experience a reduced number of data breaches. Such an effect is moderated by the heterogeneity of universities, university type, and research intensity isolated efforts.

Furthermore, Kwon and Johnson (2018) focused on the security impact of *meaningful-use attestation* and found that hospitals that attest to having reached Stage 1 meaningful-use standards have fewer external breaches in the short term. Kim and Kwon (2019) found that the *adoptions of electronic health records (EHRs)* increase firms likelihood of experiencing data breaches. In addition, Mcleod and Dolezel (2018) focused on technical facilitates and several organizational factors, and their findings suggest that several technical facilitates (e.g., EHR system, neonatal intensive care unit, lab barcoding, and health information exchange initiative) are highly likely to increase firms' data breach risk.

Overall, the preceding literature review indicates that exploration of the organizational factors that can influence data breach risks has been quite limited in scope and focused purely on IT. I aim to provide several novel insights into the literature from a fresh non-technical perspective of *firm diversity*. I are motivated to do so because, in recent years, an increasing number of security experts and managers have highlighted the concepts that "the best way to improve information security is to learn on the job" and "diversify benefits corporate information security controls."[48] An integration of the concepts suggests knowledge diversity help benefit information

[48] A related news can be found in https://www.scmagazineuk.com/organisations-failing-diversify-infosec-teams-will-fail-meet-skills-requirements/article/1663347.

security controls. Given firms' multi-industry operations help diversify their knowledge collection, I can reasonably expect firm diversity to exert influence on their quality of security control. Such an expectation suggests further opportunities to expand the scope of the organizational determinants of data breach risk research to firm diversity.

4.2.2. Firm Diversity

Firm diversity represents the coordination of a portfolio of activities and operations *across multiple industries* (Collis and Montgomery 1997; Grant et al. 1988; Nayyar 1992; Tallman and Li 1996; Varadarajan 1986). The advantages of firms' multi-industry operations fundamentally stem from the relatedness among businesses in diverse environments. More specifically, relatedness enables different resources to be shared and transferred among businesses to realize reciprocity (Ravichandran et al. 2009). Researchers have long emphasized the importance of relatedness and confirmed that it can determine diversification, including when and where to diversity and in which mode to enter (Neffke and Henning 2013; Sakhartov 2017). In addition, previous research has analyzed the role of relatedness by distinguishing the different relatedness types, such as manufacturing (St. John and Harrison 1999), knowledge (Miller 2006; Tanriverdi and Venkatraman 2005), skill (Neffke and Henning 2013), product (Luo 2002), and IT (Tanriverdi 2005) relatedness.

Numerous studies have explained the motives and rationales for firm multi-industry operations from the perspective of operating synergy. Related to the motives

of operating synergies, some potential sources of value for multi-industry operations may stem from economies of scale and scope, where acquirers can consolidate operations with those in the targeted businesses to cut costs (Hoberg and Phillips 2010; Rabier 2017; Rumelt 1974), new product offering (Hitt et al. 1996), or competition reduction (Chatterjee 1986). Alternative motives of diversification can be related to financial synergies, where firm diversified operations may generate values through some manners such as, smoothing cash flow (Amit and Livnat 1988; Rabier 2017), reducing cost of capital (Hughes et al. 2007), saving taxes (Leland 2007), and lowering the bankruptcy probabilities (Lewellen 1971).

In particular, stemming from Rumelt (1974), the strategy literature commonly distinguishes between related and unrelated diversity (Grant et al. 1988; Hall Jr and St. John 1994). Related diversity involves firm operations in businesses in a portfolio of industries that are related to one another, whereas unrelated diversity involves the operations in businesses in industries unrelated to one another (Chari et al. 2008). There is a broad consensus among these studies that related diversity is superior to unrelated diversity in terms of economic performance (Amit and Livnat 1988; Bettis 1981; Chatterjee and Wernerfelt 1988; Martin and Sayrak 2003; Palepu 1985; Palich et al. 2000).

Collectively, the literature has suggested that firm diversity helps firms reap economic benefits (e.g., economies of scope) via the manner of synergy. However, I emphasize that nearly all of the extant studies have measured and interpreted the rationale for firms' multi-industry operations from an economic perspective. While the

impact of firm diversified operations has yet to be examined in an information security context, where anecdotal evidence exists that, as earlier-mentioned, diversity might benefit firms' information security controls.

4.3.THEORETICAL BACKGROUND

4.3.1. Nature of Information Security Protection

Although organizations commonly include information security as one of their crucial issues, their information is substantially less secure than it could be. Why is this so? One viable explanation for this phenomenon is that information security is highly uncertain and complex to handle (Alexander et al. 2013; Axelrod et al. 2009; Brotby 2009), and organizations are commonly unaware of the appropriate remedies. This section discusses the nature of information security protection in a detailed manner.

Information security protection is highly *complex*. The reason is that information security has numerous and intricate sources of danger, including but not limited to fire, espionage, data theft, breakdown, malicious attacks, flood, computer fraud, accidental damage, power failure, hacking, lightning, telecommunication failure, explosion, internal operation error, and vermin (Alexander et al. 2013; Axelrod et al. 2009). Such a complex nature is further confounded by the fact that some leakage sources are considerably minimal and isolated, making them difficult to perceive. Therefore, firms may easily overlook that their privacy information is already in danger and fail to promptly address new security gaps as they emerge.

Information security protection is substantially *non-routine*. The reason is that security measures, particularly those used in defending against insider threats, are scarcely in place for use. In general, outside attacks (e.g., hacking and malware) are relatively easy to detect and defend against using technological measures (e.g., antivirus software, intrusion detection systems, and firewalls) (Colwill 2009). However, these measures are unsuitable for controlling employees who need privileged access to information to perform their jobs (Herath and Rao 2009a; Post and Kagan 2007), and thus, firms commonly lack awareness of the measures to effectively defend against insider threats. Lee et al. (2017, p. 16) described the situation as follows: "No matter how much technological advancements have been made, the current solutions for addressing insider threats are still limited."

Information security protection is also markedly *uncertain*. Although the implementation of certain countermeasures (i.e., policies and technical controls) may help firms defend against a part of data breaches, the effectiveness in reducing firms' total security threats, including the insider and external ones, is substantially uncertain. For example, the security countermeasure of IT security investment, which is considered as effective in defending against external threats, has been found to increase firms' total data breach risk (Sen and Borle 2015), particularly in the short-run (Angst et al. 2017). The behavioral security literature (D'Arcy et al. 2014; D'Arcy and Teh 2019; Pienta et al. 2018) has suggested a plausible explanation for this paradox. That is, security ITs tend to post considerable security technostress on employees, thereby increasing firms' insider threats. Pointing to a similar trend, the adoption of additional

security rules may lead to a clash of security controls and human factors (Colwill 2009) and bring employees considerable inconvenience at work (Post and Kagan 2007). This situation is also likely to cause numerous security threats.

4.3.2. Diverse Security Learning as A Solution

Given the highly *complex*, *non-routine*, and *uncertain* nature of security protection, I propose the following question based on the preceding background: How do firms move forward to effectively protect their information security and reduce data breach risk? I answer this question from an organizational learning-based perspective.

Organizational learning theory represents a classical theory in organizational behavioral studies (Fiol and Lyles 1985; Levitt and March 1988). The tenet of this theory is that firms have to acquire knowledge to guide behaviors and improve operational outcomes (Fiol and Lyles 1985; Levitt and March 1988). In a similar vein and in theory, firms could improve their information security performance through acquiring security knowledge. An important learning-based topic is discussing how diverse knowledge acquisition influences organizational learning. A strand of the literature has emphasized the role of variation or diversity for *individual learning*, and the related studies have reached a consensus on the learning benefits of diverse knowledge within organizations (Matusik and Fitza 2012).[49] On the other hand, the

[49] Simon (1985) contended that learning from a diverse knowledge base elicits advanced learning and problem-solving abilities. A series of studies (Denrell and March 2001; March 1991) highlighted that organizations' intelligence and knowledge creation will be the beneficiary of learning from heterogeneous experience. Schilling et al. (2003) focused on task variation and proposed that organizations' learning rates can be increased by "learning by doing something else." The empirical results in Schilling et al. (2003) were consistent with this postulation and showed a higher learning rate under related variation than under specialization. Matusik and Fitza (2012) found that diverse knowledge is particularly powerful in solving uncertain or complex problems owing to the capability of accessing broad information.

literature also focuses on *group learning* and highlights the beneficial learning effects of knowledge diversity in an alliance (Beckman and Haunschild 2002; Hambrick et al. 1996; Jiang et al. 2010; Weigelt and Sarkar 2009).[50] Beyond these aspects, I note that the literature has reached an additional consensus that, diversity is markedly needed and particularly important in coping with *complex* (Jehn et al. 1999; Liu and Ravichandran 2015; Matusik and Fitza 2012), *uncertain* (Fang et al. 2010; Matusik and Fitza 2012), or *non-routine* (Hambrick et al. 1996) problems. Such a finding is highly notable in my context, given that information security protection has a similar nature as I discussed earlier.

Collectively, the organizational diverse learning literature has suggested that the learning benefits of diverse knowledge acquisition, particularly for solving complex, uncertain, or non-routine problems. Although I later integrate such a perspective into my theorizing on the diversity–security relationship, *a problem remains for this undertaking*. That is, the benefits of diverse learning are based on the premise that the varied knowledge for learning is *related* and can be *effectively shared* among entities (Beckman and Haunschild 2002; Hambrick et al. 1996; Schilling et al. 2003). However, *the validity of such a premise cannot be taken for granted in my context*. To justify the validity of the aforementioned premise in my context (i.e., security protection in a diversified firm), the following contents discuss (1) why security knowledge is cross-

[50] Hambrick et al. (1996) supported the positive role of diversification on team learning and found that high top management team diversity is associated with high propensity and large magnitude for actions and responses. Beckman and Haunschild (2002) found that the diverse experiences of firms' inter-organizational network partners is associated with a decreased pay for acquisitions and increased acquisition performance. Weigelt and Sarkar (2009) showed that a certain degree of technical experiential diversity tends to facilitate firms to overcome technological hurdles and positively influence their client innovation adoptions. Jiang et al. (2010) found that high alliance functional diversity leads to a balanced portfolio of exploration and exploitation activities and enhanced firm performance.

industry related in a diversified firm, and (2) what are the channels used for enabling cross-industry security knowledge sharing in a diversified firm.

4.3.2.1.Cross-industry security relatedness in a diversified firm

The cross-industry security knowledge relatedness fundamentally underpins a diverse security learning. I clarify the concept that security knowledge relatedness is widespread among industries of diversified firms in the following aspects.

First, IT infrastructure and related practices exhibit a high degree of applicability across nearly all industries. Tanriverdi (2006) particularly highlighted that a firm often has to set common rules, standards, and policies to ensure the application of a common IT infrastructure across its business units, thereby indicating a high degree of security knowledge relatedness across its business units given IT operations involve intensive security knowledge.

Second, knowledge of security threats and security-related routines is generally transferable across business units. This concept is partially supported by the operations of Information Technology Information Sharing and Analysis Centre (IT-ISAC)[51], which is a government-created security sharing consortium and provides a virtual space for members to share IT security knowledge of potential vulnerabilities and successful controls. In addition, National Infrastructure Advisory Council (NIAC, 2008)[52] highlighted the crucial role of information sharing and partnership in protecting organizations' internal information security, and recommended that the government establish a mechanism to communicate intelligence and understanding on

[51] https://www.it-isac.org
[52] https://www.dhs.gov/publication/niac-insider-threat-final-report

internal security threats. Academically, a big body of literature has also confirmed the extensive availability of security knowledge sharing and generally found that sharing security knowledge leads to an increased level of enterprise security (Gal-Or and Ghose 2005; Gordon et al. 2003; Landwehr 2004; Safa and Von Solms 2016; Tamjidyamcholo et al. 2014).

Lastly, firms' security management structure determines high security knowledge relatedness among different industries. That is, with the extensive adoptions of ISO 27000 family of standards, virtually all security functions and decision-makings have been generally centralized under such a security management structure (Calder and Watkins 2012; Kayworth and Whitten 2010; Peltier 2013). For example, firms have to uniformly identify significant threats and security-related changes and make a unified response thereafter to each relevant group and unit. They also develop enterprise-wide security policies and standards by combining all the collected security information into the same framework. Evidently, such a centralized security management structure leads to a high relatedness of security knowledge among the different industries of firms.

4.3.2.2.Channels for cross-industry security knowledge sharing in a diversified firm

A cross-industry diverse security learning entails another premise that there are channels used for enabling security knowledge share across industries in a diversified firm. Such a premise is practically valid. The construction of a security management structure that is consistent with the expectation of ISO 27000 series also involves setting up certain coordinating forums to facilitate security knowledge communication

and coordination among different parts in organizations (Calder and Watkins 2012; Kayworth and Whitten 2010; Peltier 2013). In particular, a key pattern of a coordinating forum is the steering committee. This forum commonly gathers firms' managers and representatives from different business units and groups, thereby enabling firms to receive multiple perspectives on each security issue. Firms are available to apply the lessons learned throughout the enterprise to effectively make joint decisions and respond to situations, thereby increasing firms' cost efficiency in security controls. In addition, the steering committee can also facilitate the dissemination of security-related "best practices" throughout an organization.

Another extensively adopted coordinating forum is information security liaisons (Kayworth and Whitten 2010). The liaisons act as an intermediary between the respective unit and information security services. In addition, they can act as advisors and consultants on firms' security-related matters and play a role to ensure that security best practices are included in all enterprise architectures.

A variety of additional interrelating channels, such as team days, intranet, email, and face to face working, are also practically available (Calder and Watkins 2012). The implementation of these platforms further enables firms to realize the expectation that "all employees of the organization and, were relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function" (ISO 27001 A. 7.2.2).

4.4.HYPOTHESES

The preceding review of the theoretical foundations has provided the following building blocks to further conceptualize hypotheses.

- Information security protection is replete with complexities, non-routine problems, and complexities.
- An organizational learning perspective suggests that firms could improve their security protection through acquiring security knowledge.
- Security knowledge are cross-industry related and can be effectively shared and integrated among different industries in a firm.

My further analysis of the diversity–security relationship, as I discuss next, is based on the preceding foundations.

4.4.1. Security Effectiveness of Firm Diversity

I first propose the hypothesis on the relationship between firm diversity and information security performance. I use the organizational diverse learning and security literatures as bases to propose that firm diversity may advance firms' security learning in three aspects: (1) extending security learning breadth, (2) increasing security learning depth, and (3) invigorating security learning mode.

First, firms' multi-industry operations can advance security learning by extending the breadth of security knowledge acquisition (Markides and Williamson 1994; Thornhill and White 2007). This advantage stems from the case that firms' operations in distinct industries enables firms to apply security routines into diverse contexts. In this situation, firms can simply access enriched security-related experience, feedback,

and information stock. They can also search for potential security threats in a broadened scope (Liu and Ravichandran 2015; Zollo and Winter 2002). Thus, via an effective cross-unit interrelationship in the manners as described in Subsection 3.3, the entire organization tends to have an enhanced possibility to obtain plausible security solutions and a comprehensive threat-detection system.

For example, if a diversified firm has a medical or financial business, the sensitive nature of customer information in the business makes securing information security considerably paramount. Thus, the employees in the business unit are likely to encounter intensive security concerns and strict requirement in security operations, thereby facilitating the achievement of useful behavioral security knowledge in a variety of aspects (e.g., potential threats, operational vulnerabilities, training, and policies). Consequently, such behavioral security knowledge can be transferred from its medical or financial business into other units and help improve the latter ones' quality of information security controls.

Second, multi-industry operation advances security learning in the manner of increasing security learning depth and invigorate the mode of security learning (Denrell and March 2001; March 1991; Matusik and Fitza 2012; Simon 1985). Given that diversified firms can apply the same routine in different environments, they are able to form a relative comprehensive knowledge structure in terms of each security routine to benefit security-related problem-solving and decision-making (Schilling et al. 2003).

Reconsidering the aforementioned example, when a diversified firm applies

behavioral security knowledge that achieved from its medical business into its other industries, the changes of operational environments bring related knowledge variations and further possible associations. Thus, the diversified firm can be inspired and exploit deep intelligences at the security knowledge by combining the extended associations.

Third, firm multi-industry operations can invigorate the mode of security learning. Organizational learning studies have held the viewpoint that "differences tend to capture my attention" (Beckman and Haunschild 2002, p. 94). That is, when encountering different experiences, firms are highly motivated to resolve such a difference and stir further thinking around their specific security issue at hand (Crocker et al. 1984).

In summary, the operations in diversified industries enables organizations to achieve an advanced security learning ability via extending security learning breadth, increasing security learning depth, and invigorating security learning mode. In such an environment, firms can develop a comprehensive awareness of the potential threats and vulnerabilities, search security countermeasures in a boarded scope, and incorporate diversified feedbacks for implementing security policies and IT controls which are highly economic-balanced and match with insiders' expectations, thereby eventually enhancing firms' quality of security protection and reduce their security risks.

HYPOTHESIS 4-1 (H4-1): *Firm diversity is negatively associated with data breach risk.*

To build a finer-grained understanding of the diversity–security relationship, I

further compare the security effectiveness of different types of diversity (i.e., related versus unrelated diversity). I propose that the security effectiveness of multi-industry operations is more evident under related than unrelated diversity, and presents the following theoretical justifications.

First, a considerably broader scope of learning is available under related than unrelated diversity. As earlier discussed, knowledge relatedness is suggested to be the premise to enable a diverse learning. If businesses in diversified firms are highly related, then a high degree of relatedness exists among IT assets, information-related operations and activities, marketing data, and external environments (Markides and Williamson 1994; Miller 2006), thereby increasing the relatedness of their security threats and controls. Thus, a broad range of security knowledge can be directly transferred among related businesses to advance the acquisition of security knowledge.

Second, compared with unrelated variation, related variation can better guide learners in developing abstract principles (Graydon and Griffin 1996; Schmidt 1975) and enhancing the understanding of the learning context (Maskarinec and Thompson 1976). Schilling et al. (2003) empirically determined that related diversification can better enhance organizations' learning rates and problem-solving capabilities than unrelated diversification. Therefore, a reasonable expectation is that firms can achieve a deeper security learning depth when operating businesses in related than in unrelated industries.

Third, a more vigorous learning mode can be realized under related than unrelated diversity because businesses operated in related industries have more extensive

interrelationships than unrelated businesses (Alonso-Borrego and Forcadell 2010; Datta et al. 1991). The result is the promotion of social networks and a culture in which security-related routines and experiences can be shared frequently and effectively among business units.

Evidently, related diversity allows a *greater learning scope*, *deeper learning depth,* and *more vigorous learning mode* than unrelated diversity. Thus, security knowledge is more available and its acquisition is more effective in the former than in the latter context. Accordingly, data breach risk is considerably reduced under related diversity.

HYPOTHESIS 4-2 (H4-2): *The effectiveness of firm diversity to reduce data breach risk is greater under related than unrelated diversity.*

4.4.2. Moderating Roles of Managerial Ability

Given the effectiveness of firm diversity in reducing data breach risks, my further question involves whether any variable may act as a boundary condition. I focus on the moderator of *managerial ability* because firms' cross-unit security interrelationships should be commonly chaired by a board member, and the most important competency for such a role is managerial ability (Calder and Watkins 2012). I propose the following reasons to expect a strengthening effect of managerial ability on the security effectiveness of firm diversity.

First, capable top managers are suggested to possess excellent analytical and decision-making abilities. Thus, they are likely to accept and invest in the cost-

effective security standards of the ISO 27000 series (Calder and Watkins 2012; Peltier 2013). In particular, one of the most important concepts recommended by the ISO 27000 series is enterprise-wide security interrelationship (e.g., coordination and communication) (Calder and Watkins 2012; Kayworth and Whitten 2010; Peltier 2013). Therefore, I expect that capable executives tend to increase the *availability* of cross-unit security interrelationship, thereby further advancing security learning and controls.

Second, firms often nominate a senior executive on the board as chairperson to coordinate all security-related activities within the organizations (Calder and Watkins 2012; Kayworth and Whitten 2010; Peltier 2013). Calder and Watkins (2012) proposed that the primarily crucial criterion to select such chairpersons is not how knowledgeable they are on IT issues but whether they have good managerial abilities (e.g., interpersonal and coordinating abilities and experience in implementing change projects). That is, managerial competencies are the most important competences for security chairpersons to effectively carry out their coordination and management responsibilities under a centralized security governance structure. Therefore, I may expect that cross-unit security interrelationships can be highly *effective* under the guidance of capable top managers.

In summary, the *availability* and *effectiveness* of a cross-unit security interrelationship, which benefits diversified firms' security decision-makings and reduces security risk, tend to be high if the firms' managers are highly capable, thereby strengthening the security benefits of multi-industry operations.

HYPOTHESIS 4-3 (H4-3): *Managerial ability strengthens the negative relationship between firm diversity and data breach risk.*

Figures 4.1 illustrates my conceptual model.

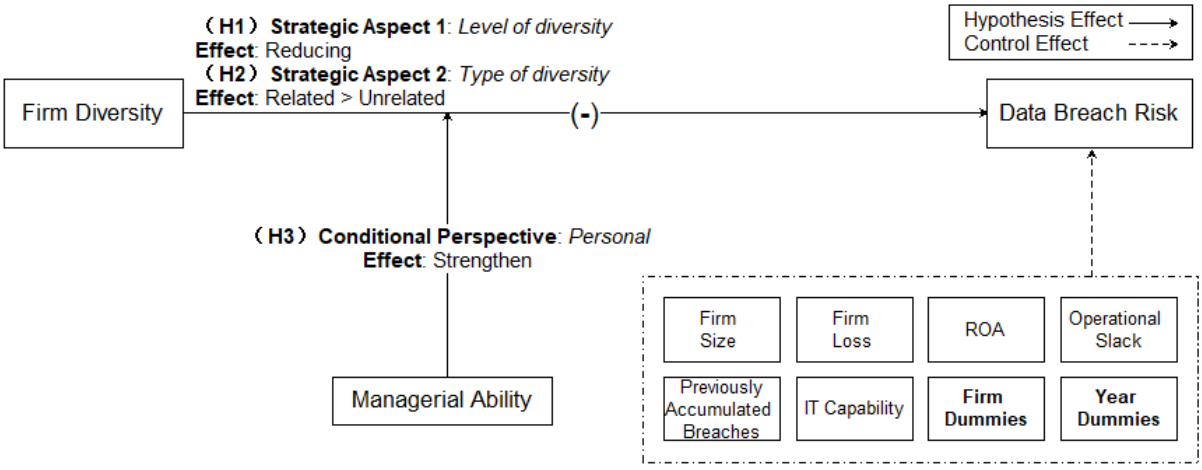

Figure 4.1. Research Conceptual Model

4.5.DATA AND VARIABLES

4.5.1. Data Descriptions

This section describes the empirical methodology used. To test the research model, I compiled a variety of data primarily from four public sources, namely, the Privacy Rights Clearinghouse (PRC; data breach data), Identity Theft Resource Center (ITRC; data breach data), COMPUSTAT (accounting data), and Peter Demerjian data (managerial ability data).

First, I collected data breach data from PRC and ITRC. In the current study, I used both PRC and ITRC as the data breach sources to ensure a comprehensive data collection. If one data breach occurred in a US-listed firm and was reported in either PRC or ITRC from 2006 to 2017, it is counted as one breach in my sample. Such an

approach eventually yields 1,327 data breaches involving 649 different firms. Second, I collected all accounting data (95,673 firm-years) from COMPUSTAT between 2006 and 2016. These data were used to measure firm diversity and a part of my control variables. Third, I collected all managerial ability data (56,273 firm-years) between 2006 and 2016 from the Peter Demerjian data.

4.5.2. Variable Descriptions

4.5.2.1.Dependent Variable

I calculated the dependent variable of data breach risk (*BREACH*) as an indicator variable that equals 1 if a firm has a reported breach in the current or next fiscal year, and 0 otherwise.

4.5.2.2.Independent Variable

The independent variable in this study is firm diversity. I followed Chari et al. (2008) and Dewan et al. (1998) in computing the variable of firm diversity as an entropy measure using data obtained from COMPUSTAT. This measure is appropriate for the current study because "it allows the distinction between related and unrelated diversity, which other measures do not permit" (Dewan et al. 1998, p. 225). Overall, this entropy measure assesses three levels of diversity, namely, total diversity (*TD*), related diversity (*RD*), and unrelated diversity (*UD*).

4.5.2.3.Moderator (Managerial Ability)

I measured the moderator variable of managerial ability (*MA*) using the measure operationalized by Demerjian et al. (2012) and subsequently applied by Koester et al.

(2016) and Custódio et al. (2017). To measure *MA*, Demerjian et al. (2012) considered a multitude vector of inputs, which includes the cost of goods sold and inventory; selling, general, and administrative (SG&A) expenses; net plant, property, and equipment (PP&E); operating leases; research and development (R&D) expenditures; goodwill; and other fixed or intangible assets. Demerjian and the colleagues then employed a data envelopment analysis (DEA) method and compared the revenues generated by each firm conditional on all these inputs relative to the firm's competitors. Demerjian et al. (2012) argued that *MA* is a comprehensive and ideal managerial ability measure, and this viewpoint has been extensively affirmed in the academic literature (e.g., Bonsall IV et al. 2016; Custódio et al. 2017; Demerjian et al. 2013; Koester et al. 2016).

4.5.2.4.Control Variables

I included a comprehensive list of control variables. *First*, given that large firms have many opportunities to be involved in data breaches, the first control variable is firm size (*SIZE*), which is measured as the natural logarithm of the value of the total assets in a fiscal year. *Second*, firms' financial performance can determine whether these organizations have sufficient resources or capital to invest in information security if needed. Hence, I controlled for return on assets (*ROA*), which equals the net income before extraordinary items and discontinued operations divided by the total assets and multiplied by 100. *Third*, resource slacks play considerable roles in reducing firms' uncertainty; any leanness at resources can be a source of role overload and thus increase accidents (McLain 1995; Wiengarten et al. 2017). Thus, I controlled for

operational slack (*OP_SLACK*), which is measured following Azadegan et al. (2013) as a natural logarithm of industry adjusted ratio of annual sales to tangible assets. *Fourth,* I controlled for firms' total number of previous breaches (*BREACH_PRE*). This control is very important because it can generally index the endogenous factors of firms' security vulnerabilities. *Fifth,* given that an increased IT capability enables a firm to reinforce its security defense capability, I controlled for IT capability (*IT_CAPA*) and measured the variable as an indicator variable that is equal to 1 if a firm is ranked on IW500 for the focal year, and 0 otherwise. *Sixth*, firms' market environments tend to influence their vulnerabilities (Sen and Borle 2015) to security attacks and insiders' loyalty (Adeoye and Hope 2020). Thus, I controlled for external market competition (*COMPETITION*).[53]

I also included variables to control for *firm*- and *year-fixed effects*. Firm-fixed effects further account for unobserved heterogeneity, thereby reducing the concerns associated with time-invariant omitted firm characteristics that are correlated with firms' data breach risks. Year-fixed effects control for any systematic differences across these years that could influence firms' security risk.

After measure constructions, all the collected data with the constructed variables were combined with ticker symbols and years. After excluding the observations with missing accounting information and firms located outside the US, the final sample consists of 55,715 firm-year observations associated with 8,711 unique firms from

[53] I followed Kim et al. (2016) and Li and Zhan (2018) and measured this variable with the product market competition variable in TNIC dataset (http://hobergphillips.tuck.dartmouth.edu/) provided by Hoberg and Phillips (2010, 2016).

2006 to 2016. Table A (Panel C) of Appendix A presents the variable descriptions, in which *i* and *j* are index firm and year, respectively. Table 4.1 reports the descriptive statistics and correlations of all variables in this study.

Table 4.1. Descriptive Statistics and Correlations

	Variable	Mean	*S.D.*	Min	Max	1	2	3
1	*BREACH*	0.018	0.132	0.000	1.000	1.000		
2	*TD*	0.191	0.345	0.000	2.459	0.046	1.000	
3	*RD*	0.067	0.190	0.000	1.580	0.031	0.642	1.000
4	*UD*	0.124	0.267	0.000	1.953	0.038	0.836	0.116
5	*MA*	0.004	0.142	−0.303	0.681	0.046	−0.041	−0.025
6	*SIZE*	5.824	2.705	−6.215	14.254	0.162	0.320	0.254
7	*ROA*	−0.979	110.913	−25884.810	525.815	0.001	0.005	0.003
8	*OP_SLACK*	−0.023	1.416	−9.339	11.217	0.019	0.039	0.028
9	*BREACH_PRE*	0.062	0.374	0.000	9.000	0.551	0.068	0.045
10	*IT_CAPA*	0.016	0.127	0.000	1.000	0.111	0.076	0.066
11	*COMPETITION*	4.570	7.700	0.953	75.610	−0.010	−0.131	−0.073

	Variable	4	5	6	7	8	9	10
4	*UD*	1.000						
5	*MA*	−0.035	1.000					
6	*SIZE*	0.233	0.043	1.000				
7	*ROA*	0.004	−0.001	0.025	1.000			
8	*OP_SLACK*	0.031	−0.176	0.134	0.006	1.000		
9	*BREACH_PRE*	0.056	0.061	0.209	0.002	0.025	1.000	
10	*IT_CAPA*	0.050	0.049	0.151	0.001	0.009	0.161	1.000
11	*COMPETITION*	−0.115	0.118	−0.049	−0.104	0.036	−0.013	−0.029

4.6.RESULTS

4.6.1. Baseline Analysis

I conducted my analyses using the *fixed-effect logit models* because my dependent variable (*BREACH*) is binary. Table 4.2 presents the baseline analysis results and shows four models.

Model 1 (Table 4.2) tests the main effect of *TD*. The coefficient of the *TD* variable is negative and significant ($\beta = -0.798$, $p < 0.05$), thereby indicating that a high-level total firm diversity tends to decrease firms' data breach risks. Given a one-standard-

deviation (0.345) increase in firms' total level of diversity, firms' likelihood of data breach in the focal and subsequent years is expected to decrease by approximately 0.275 (0.798 × 0.345). Hence, H4-1, which states that firm diversity will be negatively associated with data breach risk, is supported.

Model 2 (Table 4.2) tests the main effects of *RD* and *UD*. *RD* has a significantly negative effect ($\beta = -2.056$, $p < 0.01$) on *BREACH*, thereby indicating that a one-standard-deviation (0.191) in related diversity decreases firms' likelihood of data breach by approximately 0.393 (2.056 × 0.191). By contrast, *UD* has no significant effect on *BREACH*. Beyond these two results, a t-test on the difference between the coefficients for the two terms (Wooldridge 2003, p. 139−142) shows that the difference is significant ($p < 0.01$). Therefore, H2, which states that the security effectiveness of firm diversity is more evident in the context of related than unrelated diversity, is supported.

Models 3 and 4 (Table 4.3) test the moderating effect of managerial ability. In Models 3 and 4, the coefficient of *TD*× *MA* is significantly and negative ($\beta = -0.841$, $p < 0.1$). In addition, the coefficient of *RD*× *MA* is significantly negative ($\beta = -5.632$, $p < 0.05$). In particular, the decreasing effectiveness of firms' level of diversity on their data breach risk will be further decreased by approximately 0.800 (5.632 × 0.142) with a one-standard-deviation (0.142) increase in managerial ability under related diversity. Meanwhile, Model 4 does not support the moderating role of managerial ability under unrelated diversity because the coefficient of *UD*× *MA* is insignificant. Therefore, H4-3, which states that managerial ability strengthen the security effect of

firm diversity is supported.

Table 4.2. Baseline Analysis

	Fixed−effect logit model (Dependent variable: *BREACH*)			
	Model 1	Model 2	Model 3	Model 4
TD	**−0.798****		**−0.764****	
	(−2.15)		**(−2.05)**	
RD		**−2.056*****		**−1.716*****
		(−3.22)		**(−2.60)**
UD		**−0.086**		**−0.064**
		(−0.19)		**(−0.14)**
TD× MA			**−0.841***	
			(−1.79)	
RD× MA				**−5.632****
				(−2.28)
UD× MA				**0.813**
				(0.70)
MA	−0.277	−0.327	−0.002	−0.118
	(−0.56)	(−0.67)	(−0.00)	(−0.20)
SIZE	0.482***	0.482***	0.486***	0.476***
	(2.85)	(2.83)	(2.87)	(2.79)
ROA	−0.050	−0.050	−0.074	−0.029
	(−0.09)	(−0.09)	(−0.13)	(−0.05)
OP_SLACK	−0.039	−0.041	−0.028	−0.029
	(−0.19)	(−0.20)	(−0.14)	(−0.14)
BREACH_PRE	0.606***	0.606***	0.603***	0.597***
	(7.39)	(7.38)	(7.36)	(7.27)
IT_CAPA	−0.404*	−0.382	−0.395	−0.343
	(−1.65)	(−1.55)	(−1.61)	(−1.38)
COMPETITION	−0.085**	−0.082*	−0.083*	−0.078*
	(−1.96)	(−1.89)	(−1.92)	(−1.81)
Firm Fixed	Yes	Yes	Yes	Yes
Year Fixed	Yes	Yes	Yes	Yes
N	2,178	2,178	2,178	2,178
pseudo R^2	0.122	0.126	0.123	0.130

Notes. The sample consists of 2,187 firm-years from 2006 to 2016. All variables are defined in Table A (Panel C) of Appendix A in online appendix. Models 1−4 use fixed-effect Logit regression analysis, and include firm and year fixed effects in the regression (*the observations where firms had not experienced a data breach during my sample period were dropped in the regression*). The symbols ∗∗∗, ∗∗, and ∗ denote significance at the 1%, 5%, and 10% levels, respectively.

4.6.2. Robustness Tests

4.6.2.1.Two-Stage Residual Inclusion (2SRI) Approach

Other specifications are used to ensure robustness. First, I attempt to ameliorate *endogeneity concerns*. I recognize that firm diversity and security risks might be endogenous. For example, certain unobserved time-variant factors might drive both firm diversity and occurrences of data breach. To mitigate the endogenous concern, I

adopted a 2SRI approach (Terza et al. 2008), which has been increasingly used by business research to avoid endogeneity bias (Gamache et al. 2020; Li et al. 2018; Maksimov et al. 2019; Turner and Rindova 2018). In the first stage of the test, I respectively calculated the average total / related / unrelated level of diversity of peer firms (i.e., firms operating in the same industry) and respectively used each value as an instrument to test the effect of data breach risk.[54] In the second stage, I adopted the residual from the first stage (i.e., *RESIDUAL_TD*, *RESIDUAL_RD*, *and RESIDUAL_UD*) as additional controls in my model and achieved the results (see Table 4.3) which are highly consistent with the ones in the baseline analysis, thereby mitigating endogeneity problems.

Table 4.3. 2SRI Model

	Fixed−effect ordinary least squares model[55] (Dependent variable: *BREACH*)			
	(1)	(2)	(3)	(4)
TD	**−0.023****		**−0.024****	
	(−2.09)		**(−2.18)**	
RD		**−0.039***		**−0.043****
		(−1.86)		**(−2.09)**
UD		**−0.015**		**−0.013**
		(−1.15)		**(−1.05)**
TD× MA			**−0.082*****	
			(−3.34)	
RD× MA				**−0.280*****
				(−5.70)
UD× MA				**0.007**
				(0.23)
MA	Included	Included	Included	Included
RESIDUAL_TD	Included		Included	
RESIDUAL_RD		Included		Included
RESIDUAL_UD		Included		Included
Controls	Included	Included	Included	Included
Firm Fixed	Yes	Yes	Yes	Yes
Year Fixed	Yes	Yes	Yes	Yes
N	29,195	29,195	29,195	29,195

Notes. The sample consists of 2,004 firm-years from 2006 to 2016. All variables are defined in Table A (Panel C) of Appendix A in online appendix. In Cols. 1−4, I use fixed-effect OLS regression analysis, and include firm and year fixed effects in the regression (*the observations where firms had not experienced a data breach during my sample period were dropped in the regression*). The symbols ∗∗∗, ∗∗, and ∗ denote significance at the 1%, 5%, and 10% levels, respectively.

[54] The averaged diversification degree from peer firms is a good instrument since it can influence the focal firm's diversification via mimetic isomorphism (DiMaggio and Powell 1983; Maksimov et al. 2019) but will not influence the firm's security risk.

[55] I followed Maksimov et al. (2019) and used a OLS regression in the 2SRI approach.

4.6.2.2.An Alternative Measure of the dependent Variable

Second, I used an alternative measure in terms of the dependent variable. That is, I replaced *BREACH* with *BREACH_NUM*, which represents the accumulated number of data breaches within the current or next fiscal years. I used *fixed-effect* Poisson regression because *BREACH_NUM* is a count variable. Such an approach yields consistent results (see Table 4.4).

Table 4.4. Alternative Measure of Data Breach Risk

	Fixed−effect Poisson model (Dependent variable: *BREACH_NUM*)			
	(1)	(2)	(3)	(4)
TD	**−0.554***		**−0.535***	
	(−1.95)		**(−1.86)**	
RD		**−1.610*****		**−1.315*****
		(−3.32)		**(−2.66)**
UD		**−0.057**		**−0.040**
		(−0.17)		**(−0.12)**
TD× MA			**−0.277**	
			(−0.43)	
RD× MA				**−3.482****
				(−2.15)
UD× MA				**0.842**
				(1.02)
MA	Included	Included	Included	Included
Controls	Included	Included	Included	Included
Firm Fixed	Yes	Yes	Yes	Yes
Year Fixed	Yes	Yes	Yes	Yes
N	2,004	2,004	2,004	2,004

Notes. The sample consists of 2,004 firm-years from 2006 to 2016. All variables are defined in Table A (Panel C) of Appendix A in online appendix. In Cols. 1−4, I use fixed-effect Poisson regression analysis, and include firm and year fixed effects in the regression. The symbols ∗∗∗, ∗∗, and ∗ denote significance at the 1%, 5%, and 10% levels, respectively.

4.6.2.3.An Alternative Model

Another concern is raised given that the introduction of firm fixed-effects into the regression has considerably reduced the sample size. In my sample, the number of observations (*BREACH* = 1) is substantially limited in comparison with the total number of observations. Thus, the dependent variable (i.e., *BREACH*) remains equal

to 0 in all the focused years (i.e., 2006–2016) for the overwhelming majority of the observations. Evidently, these observations would be excluded in analysis when including firm fixed-effects in the model, thereby generally reducing the comprehensiveness of my sample. To mitigate such a concern, I tested my hypotheses using a logit model by controlling for the industry fixed-effects and year fixed-effects over the entire sample period. The results (see Table 4.5) remained consistent, thereby mitigating the proposed concern.

Table 4.5. Logit Model

	Logit model (Dependent variable: *BREACH*)			
	(1)	(2)	(3)	(4)
TD	**−0.419*****		**−0.410*****	
	(−2.79)		**(−2.73)**	
RD		**−0.840*****		**−0.790*****
		(−3.12)		**(−2.99)**
UD		**−0.176**		**−0.192**
		(−0.92)		**(−1.00)**
TD× MA			**−0.757**	
			(−0.94)	
RD× MA				**−5.019*****
				(−2.84)
UD× MA				**1.170**
				(1.14)
MA	Included	Included	Included	Included
Controls	Included	Included	Included	Included
Industry Fixed	Yes	Yes	Yes	Yes
Year Fixed	Yes	Yes	Yes	Yes
N	27,148	27,148	27,148	27,148
pseudo R^2	0.448	0.449	0.449	0.451

Notes. The sample consists of 27,148 firm-years from 2006 to 2016. All variables are defined in Table A (Panel C) of Appendix A in online appendix. In Cols. 1−4, I use Logit regression analysis, and include industry and year fixed effects in the regression. The symbols ∗∗∗, ∗∗, and ∗ denote significance at the 1%, 5%, and 10% levels, respectively.

4.6.2.4.Subsample Analysis

To further ensure robustness, I conducted a subsample analysis by filtering my sample. I shortened my sample into the one from 2009 to 2016. The sample used in this test consists of 38,642 firm-years from 2009 to 2016. I used two models, namely, fixed-effect logit and logit models, for analysis. The results of using either model (see

Table 4.6) remained nearly consistent.

Table 4.6. Subsample Analysis

	Fixed−effect logit model (Dependent variable: *BREACH*)				Logit model (Dependent variable: *BREACH*)			
	(1)	(2)	(3)	(4)	(5)	(7)	(7)	(8)
TD	**−0.597**		**−0.476**		**−0.453****		**−0.432****	
	(−1.20)		**(−0.94)**		**(−2.44)**		**(−2.33)**	
RD		**−1.846****		**−1.461**		**−0.900*****		**−0.866****
		(−2.02)		**(−1.59)**		**(−2.58)**		**(−2.51)**
UD		**−0.043**		**0.046**		**−0.219**		**−0.206**
		(−0.07)		**(0.08)**		**(−0.94)**		**(−0.88)**
TD× MA			**−2.607***				**−1.345**	
			(−1.84)				**(−1.28)**	
RD× MA				**−6.598****				**−5.070****
				(−2.03)				**(−1.99)**
UD× MA				**−1.237**				**−0.193**
				(−0.76)				**(−0.16)**
MA	Included	Included	Included	Included	Included	Included	Included	Included
Controls	Included	Included	Included	Included	Included	Included	Included	Included
Firm fixed	Yes	Yes	Yes	Yes				
Industry fixed					Yes	Yes	Yes	Yes
Year fixed	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
N	1,372	1,372	1,372	1,372	17,983	17,983	17,983	17,983

t statistics in parentheses (*p < 0.1, **p < 0.05, ***p < 0.01)

4.6.2.5.Dynamic Analysis

My theory suggests that diverse security learning is the plausible mechanism that enables firms' operating diversity to reduce data breach risks. However, given security learning might take time to show the effect, I further would like to analyze whether the diversity-security relationship will take time to be realized and whether such a relationship will be long-term. Accordingly, I conduct a dynamic analysis by using the longitudinal data.

First, I analyze whether the impact of total diversity on data breach risk is long-term, and the related results are shown in Panel A (Table 4.7). In Columns 1-5 of Panel A, the dependent variable is *BREACH* and is measured in year *t*+1, *t*+2, *t*+3, *t*+4, and *t*+5, respectively. The results show that the influence of diversity on data breach risk will not take time to be realized and is relatively long-term. Furthermore, I focus on

related and unrelated diversity and see whether they are long-term. The related results are shown in Panel B (Table 7). In Columns 1-5 of Panel B, the dependent variable is *BREACH* and is measured in year *t*+1, *t*+2, *t*+3, *t*+4, and *t*+5, respectively. Accordingly, the results show that the influence of related diversity on data breach risk do not take time to be realized and is relatively long-term. I also find that unrelated diversity will not exert any influence on data breach risk, whether in terms in the short- or long- run.

Table 4.7. Dynamic Analysis

Panel A. Dynamic analysis on the security effectiveness of *TD*					
	Fixed−effect logit model				
	(1)	(2)	(3)	(4)	(5)
	$BREACH_{t+1}$	$BREACH_{t+2}$	$BREACH_{t+3}$	$BREACH_{t+4}$	$BREACH_{t+5}$
TD	-0.969**	-0.980**	-1.044**	-0.723	-0.088
	(-2.41)	(-2.16)	(-2.01)	(-1.17)	(-0.11)
MA	Included	Included	Included	Included	Included
Controls	Included	Included	Included	Included	Included
Firm fixed	Yes	Yes	Yes	Yes	Yes
Year fixed	Yes	Yes	Yes	Yes	Yes
N	1888	1548	1260	1022	709
Panel B. Dynamic analysis on the security effectiveness of *RD* and *UD*					
	Fixed−effect logit model				
	(1)	(2)	(3)	(4)	(5)
	$BREACH_{t+1}$	$BREACH_{t+2}$	$BREACH_{t+3}$	$BREACH_{t+4}$	$BREACH_{t+5}$
RD	-3.214***	-2.792***	-1.268	-0.377	1.886
	(-4.23)	(-3.32)	(-1.45)	(-0.36)	(1.39)
UD	0.226	-0.046	-0.920	-0.907	-1.384
	(0.44)	(-0.08)	(-1.42)	(-1.18)	(-1.29)
MA	Included	Included	Included	Included	Included
Controls	Included	Included	Included	Included	Included
Firm fixed	Yes	Yes	Yes	Yes	Yes
Year fixed	Yes	Yes	Yes	Yes	Yes
N	1888	1548	1260	1022	709

4.7.DISCUSSIONS AND IMPLICATIONS

4.7.1. General Discussions

Various bodies of practical and empirical evidence have suggested that enterprise

information security is a technical and non-technical issue that requires exploration beyond the IT domain. Nonetheless, this issue has been generally disregarded in the empirical security research literature. The case that information security is oftentimes centrally managed in current firms also highlights the significance to investigate the security impact of firm structure. Consequently, the current study explored the diversity–security relationship from a non-technical and structural perspective. I used a sample of US firms from 2006 to 2016 and obtained empirical results that are completely consistent with my predictions. That is, I found that firms' level of diversity is negatively associated with their data breach risk, and that the association is more evident under related than unrelated diversity. In addition, I found that managerial ability can strengthen the negative relationship between firm diversity and data breach risk, particularly for related diversified firms.

4.7.2. Theoretical Implications

This study makes several theoretical contributions. First, the current study may advance prior information security research. Despite the repeated call for information security research from the organizational and managerial perspectives, empirical effort in this area has been extremely limited. The current study may fill in the research gap by focusing on a novel security determinant (i.e., firm diversity) and initially validating the association between firm diversity and data breach risk. My justifications and findings also empirically support the viewpoints in several security studies (e.g., Gal-Or and Ghose 2005; Safa and Von Solms 2016; Tamjidyamcholo et al. 2014), which

accentuated the importance of security knowledge sharing to handle corporate information security.

Second, the extant organizational diverse learning literature has extensively discussed the effect of knowledge diversity and variation on organizational learning. I may advance this research strand by finding a consistent result in a novel context of information security protection. The present study particularly resonates with numerous prior diverse learning studies. For example, my findings are consistent with the findings of Schilling et al. (2003), which indicate that *variation increases learners' learning rate and skills, particularly under related variation*. Schilling et al. (2003) also explained that variation at the organizational level is decided by such factors as firms' product lines and geographic scope. In addition, given that current firms have extensively delegated all the security control and management to a chairperson, my findings are consistent with that of Csaszar and Eggers (2013). That is, delegation is the most effective organizational decision-making structure in the presence of diversity of expertise. Furthermore, the present study echoes the diverse learning research (e.g., Fang et al. 2010; Goerzen and Beamish 2005; Hambrick et al. 1996), which has highlighted the significance of diversity when firms face particularly complex, uncertain, or non-routine problems.

Third, I may contribute to the firm diversity literature. This strand of literature has been relatively extensive, although minimal attention has been given to the effectiveness of firm diversity beyond the economic scope. I also note that the diversity literature has typically equated the rationale for firms' multi-industry operations with

economic benefits, and I advance such a traditional view by proposing information security benefits as another rationale for multi-industry operations. In particular, my findings are consistent with those of previous diversity studies, which have indicated the economic or operational benefits of cross−unit knowledge or asset sharing (e.g., Bettis and Hall 1982; Markides and Williamson 1994; Robins and Wiersema 1995).

Fourth, given the limited empirical evidence on the role of top executives in influencing data breaches, the current study may empirically clarify the relevant wisdom by investigating the individual moderating roles of managerial ability. I note that the prior security research (e.g., Higgs et al. 2016; Kwon et al. 2012) has mainly focused on top managers' ***IT*** competency and its association with data breach risk. Differently, given the suggestion of the ISO 27000 series that *managerial ability* plays the more significant role than *IT* competency for leaders in information security protection, my finding in terms of managerial ability may better resonate with the concept proposed in the ISO 27000 series.

4.7.3. Practical Implications

Several meaningful practical implications can be drawn from this study. First, managers have realized that excellence alone is insufficient to maintain corporate success in today's increasingly competitive environment. My findings help to advance managers' understanding of the benefits of multi-industry operations. That is, apart from generating economic benefits (e.g., economies of scope), operating businesses in diversified industries, particularly in related ones, facilitates the reduction of firms'

data breach risk. My findings may also accentuate the importance of enterprise-wide security sharing coordination which have been highly recommended by the ISO 27000 series and security literature. Further, my findings serve as a reminder for diversified firms that they should take the advantage of their diversified security knowledge collection and feedback to further reinforce their security protection.

Second, deciding whether to target related or unrelated businesses is strategically significant but challenging for managers. My results indicate that when organizations plan to extend their businesses by entering new industries, entering the related industries is highly likely to benefit organizations' information security controls, since such an undertaking help better improve information security protection than entering unrelated ones.

Third, the current results can serve as a reminder that high-ability managers can strengthen the role of diversity to reduce data breach risk under the operations in multiple related industries. Accordingly, the security significance of capable managers in the firm diversity context is highlighted, while I found that such a role of capable managers is obscure in unrelated diversified firms.

4.7.4. Limitations and Future Research

The present study has a few research limitations that may provide avenues for future research. First, although this study has brought the factors of managerial ability in the security context, I only focused on the individual moderating role of the factor. Therefore, future studies may consider examining the direct effect of managerial

ability on data breach risks. Second, the scope of the current study only extended to the occurrences of data breaches. Future studies may consider the possible extensions to analyze how diversity matters to the learning that follows data breaches.

Chapter 5. General Conclusions and Future Research

Information is one of the most significant non-tangible assets of firms. At present, firms operating without any access to information is virtually impossible. However, compromised information may exert a domino effect and trigger firms' eventual failures. Therefore, practically no firms could afford to disregard their information security issues.

To address firms' security failures, security scholars have extensively highlighted the concept that information security protection is no longer a technology issue, and have increasingly called for security research from the organizational and managerial perspectives. Accordingly, recent isolated effort has been exerted to investigate how organizational factors will influence firms' data breach risks. The related investigations are important because they can benefit firms to improve their security protection at the firm level. Despite this implication, I note that research in this realm is considerably limited, thereby necessitating further effort to extend this research strand. Accordingly, the three studies in this thesis investigate how firms' data breach risks will be influenced by firms' IT innovativeness (Study 1), employee-related CSR (Study 2), and firm diversity (Study 3). I briefly summarize my motivations and findings as follows.

First, the digital domain provides firms with considerable convenience and benefits, and at present, firms' operations are highly dependent on IT performance. However, such a reliance tends to expose their marked weaknesses in terms of information security. Against this backdrop, Study 1 draws upon organizational

learning theory and investigates the influence of firms' IT innovativeness on data breach risks. My findings show that IT innovativeness is associated with a high data breach risk; such an association is weakened if firms' long-term incentives are high and strengthened if firms' external environments are complex. I pioneeringly provide empirical evidence to remind firms to caution the significant security concerns of their IT innovations. I also highlight the crucial role of leaders' long-term orientation in mitigating such concerns and the further severity of such concerns in a complex environment.

Second, in Study 2, I use principal–agent theory to frame my investigation of the relationships among CSR, firm contexts, and data breach risk. My findings show that employee-related CSR reduces firms' data breach risk, particularly if such firms are operating in a loss position, dynamic industry, or markets with similar products. I note that one of the hallmarks of information security research is the general focus on security-related or technical-centered countermeasures to defend against data breach incidents. My findings advance such conventional academic wisdom by determining that non-security and human-centered positive policies, such as employee-related CSR policies, are also effective in protecting firms' information security and thus merit the attention of information security researchers.

Third, security research suggests that firm-structural related factors will influence firm information security (Calder and Watkins 2012; Kayworth and Whitten 2010; Peltier 2013). Therefore, I am motivated to investigate whether or not firms' operations in diversified industries tend to benefit their security problem solving and improve

their information security performance. Accordingly, Study 3 draws upon organizational learning theory and investigates the relationships among firms' operating diversity (i.e., total, related, and unrelated), managerial ability as the moderator, and data breach risk. My empirical results support my expectations that firms' diversity tends to reduce the likelihood of breaches, specifically under the operations in related industries. I also found that capable managers tend to strengthen this influence.

Table 5.1 presents a summary of my findings.

Although the three studies were conducted separately, they are closely related with and complement each other. First, all studies investigated firms' determinants of data breach risks at the firm level. Given the limitation of the extant literature on the related topic, the three studies in this thesis can extend the literature on the organizational determinants of data breaches from different perspectives. My findings also provide beneficial avenues in understanding how to enhance firms' information security performance via adopting the appropriate organizational strategies and structures. Second, I adopted organizational learning theory and agency theory in these studies; the adoption of the former theory sources from the complex and uncertain natures of information security; and the adoption of the latter one sources from the human-root nature of information security. The application of both theories in the security context enables them to complement each other, thereby leading to a comprehensive understanding of the mechanisms of information security protection.

This study provides beneficial directions for future research. First, the scope of

my study only extended to the analysis of the occurrences of data breaches. That is, I did not analyze how organizational factors will influence firms' operations after experiencing data breaches. Therefore, future research can consider certain topics, such as how firms' strategies (e.g., IT adoption or CSR) could benefit their recovery processes. Second, although my studies presented environmental uncertainty and managerial ability in my application of organizational learning theory in the security context; and negative performance, environmental dynamism, and product similarity in the application of agency theory to the security research, I only focused on the moderating role of these factors. Therefore, future studies may consider investigating the direct influence of these factors on data breach risks. Third, future studies may consider linking organizational learning and agency theories in the same framework to investigate whether a relationship exists between agency controls and the efficiencies of firms' security learning.

Table 5.1. Summary of Results

Hypothesis	Result
Study 1	
HYPOTHESIS 2-1 (H2-1). IT innovativeness is positively associated with data breach risks.	Supported
HYPOTHESIS 2-3 (H2-2). High long-term incentives weaken the relationship between corporate IT innovativeness and data breach risk	Supported
HYPOTHESIS 2-3 (H2-3). High environmental dynamism strengthens the relationship between corporate IT innovativeness and data breach risks.	Not Supported
HYPOTHESIS 2-4 (H2-4). High environmental complexity strengthens the relationship between corporate IT innovativeness and data breach risks.	Supported
Study 2	
HYPOTHESIS 3-1 (H3-1). Employee-related CSR is positively associated with data breach risks.	Supported
HYPOTHESIS 3-2 (H3-2). Negative performance strengthens the relationship between employee-related CSR and data breach risks.	Supported
HYPOTHESIS 3-3 (H3-3). Environmental dynamism strengthens the relationship between employee-related CSR and data breach risks.	Supported
HYPOTHESIS 3-4 (H3-4). High product similarity strengthens the relationship between employee-related CSR and data breach risks.	Supported
Study 3	
HYPOTHESIS 4-1 (H4-1). Firm diversity degree is negatively associated with data breach risk.	Supported
HYPOTHESIS 4-2 (H4-2). The effectiveness of firm diversity to reduce data breach risk is greater under related than unrelated diversity.	Supported
HYPOTHESIS 4-3 (H4-3). Managerial ability strengthens the negative relationship between firm diversity and data breach risk.	Supported

References

Abrahamson, E. 1996. "Management Fashion," *Academy of management review* (21:1), pp. 254-285.

Adbi, A., Chatterjee, C., Drev, M., and Mishra, A. 2019. "When the Big One Came: A Natural Experiment on Demand Shock and Market Structure in India's Influenza Vaccine Markets," *Production and Operations Management* (28:4), pp. 810-832.

Adeoye, A. O., and Hope, O. 2020. "Organizational Culture, Employee Retention and Employee Loyalty: Empirical Evidence from Nigeria," *Academic Journal of Economic Studies* (6:3), pp. 139-145.

Aivazian, V. A., Ge, Y., and Qiu, J. 2005. "The Impact of Leverage on Firm Investment: Canadian Evidence," *Journal of corporate finance* (11:1-2), pp. 277-291.

Albinger, H. S., and Freeman, S. J. 2000. "Corporate Social Performance and Attractiveness as an Employer to Different Job Seeking Populations," *Journal of Business Ethics* (28:3), pp. 243-253.

Alexander, D., Finch, A., and Sutton, D. 2013. "Information Security Management Principles," BCS.

Alonso-Borrego, C., and Forcadell, F. J. 2010. "Related Diversification and R&D Intensity Dynamics," *Research Policy* (39:4), pp. 537-548.

Amit, R. 1986. "Cost Leadership Strategy and Experience Curves," *Strategic Management Journal* (7:3), pp. 281-292.

Amit, R., and Livnat, J. 1988. "Diversification Strategies, Business Cycles and Economic Performance," *Strategic Management Journal* (9:2), pp. 99-110.

Angst, C. M., Block, E. S., D'Arcy, J., and Kelley, K. 2017. "When Do It Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches," *MIS Quarterly* (41:3), pp. 893-916.

Aragón-Correa, J. A., and Sharma, S. 2003. "A Contingent Resource-Based View of Proactive Corporate Environmental Strategy," *Academy of management review* (28:1), pp. 71-88.

Argote, L., and Miron-Spektor, E. 2011. "Organizational Learning: From Experience to Knowledge," *Organization science* (22:5), pp. 1123-1137.

Attewell, P. 1992. "Technology Diffusion and Organizational Learning: The Case of Business Computing," *Organization science* (3:1), pp. 1-19.

Axelrod, C. W., Bayuk, J. L., and Schutzer, D. 2009. *Enterprise Information Security and Privacy*. Artech House.

Azadegan, A., Patel, P. C., and Parida, V. 2013. "Operational Slack and Venture Survival," *Production and Operations Management* (22:1), pp. 1-18.

Bala, H. 2013. "The Effects of It-Enabled Supply Chain Process Change on Job and Process Outcomes: A Longitudinal Investigation," *Journal of Operations Management* (31:6), pp. 450-473.

Baldwin, D. J., Buckley, J. P., and Slaugh, D. R. 2017. "Insuring against Privacy Claims Following a Data Breach," *Penn St. L. Rev.* (122), p. 683.

Bapna, R., Gupta, A., Ray, G., and Singh, S. 2016. "Research Note—It Outsourcing and the Impact of Advisors on Clients and Vendors," *Information Systems Research* (27:3), pp. 636-647.

Barber, L. 2004. *Csr for Employees: Proof Of'employer Engagement'*. Institute for Employment Studies.

Barnett, M. L., and Salomon, R. M. 2012. "Does It Pay to Be Really Good? Addressing the Shape of the Relationship between Social and Financial Performance," *Strategic Management Journal* (33:11), pp. 1304-1320.

Baskerville, R., Rowe, F., and Wolff, F.-C. 2018. "Integration of Information Systems and Cybersecurity Countermeasures: An Exposure to Risk Perspective," *ACM SIGMIS Database: the DATABASE for Advances in Information Systems* (49:1), pp. 33-52.

Beckman, C. M., and Haunschild, P. R. 2002. "Network Learning: The Effects of Partners' Heterogeneity of Experience on Corporate Acquisitions," *Administrative science quarterly* (47:1), pp. 92-124.

Bell, G. G. 2005. "Clusters, Networks, and Firm Innovativeness," *Strategic management journal* (26:3), pp. 287-295.

Benaroch, M., Chernobai, A., and Goldstein, J. 2012. "An Internal Control Perspective on the Market Value Consequences of It Operational Risk Events," *International Journal of Accounting Information Systems* (13:4), pp. 357-381.

Bennett, C. 1969. "Diffusion within Dynamic Populations," *Human Organization* (28:3), pp. 243-247.

Bettis, R. A. 1981. "Performance Differences in Related and Unrelated Diversified Firms," *Strategic Management Journal* (2:4), pp. 379-393.

Bettis, R. A., and Hall, W. K. 1982. "Diversification Strategy, Accounting Determined Risk, and Accounting Determined Return," *Academy of Management journal* (25:2), pp. 254-264.

Bharadwaj, A. S. 2000. "A Resource-Based Perspective on Information Technology Capability and Firm

Performance: An Empirical Investigation," *MIS quarterly*), pp. 169-196.
Bode, C., Singh, J., and Rogan, M. 2015. "Corporate Social Initiatives and Employee Retention," *Organization Science* (26:6), pp. 1702-1720.
Bonsall IV, S. B., Holzman, E. R., and Miller, B. P. 2016. "Managerial Ability and Credit Risk Assessment," *Management Science* (63:5), pp. 1425-1449.
Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., and Polak, P. 2015. "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors," *MIS Quarterly (MISQ)* (39:4), pp. 837-864.
Bourgeois III, L. J. 1980. "Strategy and Environment: A Conceptual Integration," *Academy of management review* (5:1), pp. 25-39.
Boyd, B. K. 1995. "Ceo Duality and Firm Performance: A Contingency Model," *Strategic Management Journal* (16:4), pp. 301-312.
Brotby, K. 2009. *Information Security Governance: A Practical Development and Implementation Approach*. John Wiley & Sons.
Bstieler, L. 2005. "The Moderating Effect of Environmental Uncertainty on New Product Development and Time Efficiency," *Journal of Product Innovation Management* (22:3), pp. 267-284.
Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS quarterly* (34:3), pp. 523-548.
Calder, A., and Watkins, S. 2012. *It Governance: An International Guide to Data Security and Iso27001/Iso27002*. Kogan Page Publishers.
Carley, K. 1992. "Organizational Learning and Personnel Turnover," *Organization science* (3:1), pp. 20-46.
Carpenter, M. A., and Sanders, W. G. 2004. "The Effects of Top Management Team Pay and Firm Internationalization on Mnc Performance," *Journal of Management* (30:4), pp. 509-528.
Carpenter, R. E., and Guariglia, A. 2008. "Cash Flow, Investment, and Investment Opportunities: New Tests Using Uk Panel Data," *Journal of Banking & Finance* (32:9), pp. 1894-1906.
Cavusoglu, H., Mishra, B., and Raghunathan, S. 2004. "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers," *International Journal of Electronic Commerce* (9:1), pp. 70-104.
Chae, H.-C., Koh, C. E., and Prybutok, V. R. 2014. "Information Technology Capability and Firm Performance: Contradictory Findings and Their Possible Causes," *Mis Quarterly* (38:1), pp. 305-326.
Chari, M. D., Devaraj, S., and David, P. 2008. "Research Note—the Impact of Information Technology Investments and Diversification Strategies on Firm Performance," *Management Science* (54:1), pp. 224-234.
Chatterjee, S. 1986. "Types of Synergy and Economic Value: The Impact of Acquisitions on Merging and Rival Firms," *Strategic management journal* (7:2), pp. 119-139.
Chatterjee, S., and Wernerfelt, B. 1988. "Related or Unrelated Diversification: A Resource Based Approach," *Academy of Management Proceedings*: Academy of Management, pp. 7-11.
Chen, C. M., and Ho, H. 2019. "Who Pays You to Be Green? How Customers' Environmental Practices Affect the Sales Benefits of Suppliers' Environmental Practices," *Journal of Operations Management* (65:4), pp. 333-352.
Chen, C. X., and Sandino, T. 2012. "Can Wages Buy Honesty? The Relationship between Relative Wages and Employee Theft," *Journal of Accounting Research* (50:4), pp. 967-1000.
Chen, P.-Y., Kataria, G., and Krishnan, R. 2011. "Correlated Failures, Diversification, and Information Security Risk Management," *MIS quarterly*), pp. 397-422.
Chen, Y., Ganesan, S., and Liu, Y. 2009. "Does a Firm's Product-Recall Strategy Affect Its Financial Value? An Examination of Strategic Alternatives During Product-Harm Crises," *Journal of Marketing* (73:6), pp. 214-226.
Cheng, L., Liu, F., and Yao, D. 2017a. "Enterprise Data Breach: Causes, Challenges, Prevention, and Future Directions," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* (7:5), p. e1211.
Cheng, L., Liu, F., and Yao, D. D. 2017b. "Enterprise Data Breach: Causes, Challenges, Prevention, and Future Directions," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* (7:5).
Chua, C. E. H., Lim, W.-K., Soh, C., and Sia, S. K. 2012. "Enacting Clan Control in Complex It Projects: A Social Capital Perspective," *Mis Quarterly*), pp. 577-600.
Chun, H., Kim, J.-W., and Lee, J. 2015. "How Does Information Technology Improve Aggregate Productivity? A New Channel of Productivity Dispersion and Reallocation," *Research Policy*

(44:5), pp. 999-1016.
Chwelos, P., Ramirez, R., Kraemer, K. L., and Melville, N. P. 2010. "Research Note—Does Technological Progress Alter the Nature of Information Technology as a Production Input? New Evidence and New Results," *Information Systems Research* (21:2), pp. 392-408.
Collis, D., and Montgomery, C. 1997. *Corporate Strategy: Resources and the Scope of the Firm*. McGraw-Hill/Irwin.
Colwill, C. 2009. "Human Factors in Information Security: The Insider Threat–Who Can You Trust These Days?," *Information Security Technical Report* (14:4), pp. 186-196.
Cram, W. A., D'arcy, J., and Proudfoot, J. G. 2019. "Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance," *MIS Quarterly* (43:2), pp. 525-554.
Cram, W. A., Proudfoot, J. G., and D'arcy, J. 2017. "Organizational Information Security Policies: A Review and Research Framework," *European Journal of Information Systems* (26:6), pp. 605-641.
Crocker, J., Fiske, S. T., and Taylor, S. E. 1984. "Schematic Bases of Belief Change," in *Attitudinal Judgment*. Springer, pp. 197-226.
Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future Directions for Behavioral Information Security Research," *computers & security* (32), pp. 90-101.
Crouch, C. 2006. "Modelling the Firm in Its Market and Organizational Environment: Methodologies for Studying Corporate Social Responsibility," *Organization studies* (27:10), pp. 1533-1551.
Csaszar, F. A., and Eggers, J. 2013. "Organizational Decision Making: An Information Aggregation View," *Management Science* (59:10), pp. 2257-2277.
Currim, I. S., Lim, J., and Kim, J. W. 2012. "You Get What You Pay For: The Effect of Top Executives' Compensation on Advertising and R&D Spending Decisions and Stock Market Return," *Journal of Marketing* (76:5), pp. 33-48.
Custódio, C., Ferreira, M. A., and Matos, P. 2017. "Do General Managerial Skills Spur Innovation?," *Management Science*).
D'Arcy, J., Adjerid, I., Angst, C. M., and Glavas, A. 2020. "Too Good to Be True: Firm Social Performance and the Risk of Data Breach," *D'Arcy, J., Aderid, I., Angst, CM, and Glavas, A. Forthcoming." Too Good to Be True: Firm Social Performance and the Risk of Data Breach," Information Systems Research*), pp. 1-45.
D'arcy, J., and Herath, T. 2011. "A Review and Analysis of Deterrence Theory in the Is Security Literature: Making Sense of the Disparate Findings," *European Journal of Information Systems* (20:6), pp. 643-658.
D'Arcy, J., Herath, T., and Shoss, M. K. 2014. "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective," *Journal of management information systems* (31:2), pp. 285-318.
D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information systems research* (20:1), pp. 79-98.
D'Arcy, J., and Teh, P.-L. 2019. "Predicting Employee Information Security Policy Compliance on a Daily Basis: The Interplay of Security-Related Stress, Emotions, and Neutralization," *Information & Management* (56:7), p. 103151.
Daft, R. L., and Macintosh, N. B. 1981. "A Tentative Exploration into the Amount and Equivocality of Information Processing in Organizational Work Units," *Administrative science quarterly*), pp. 207-224.
Damanpour, F. 1991. "Organizational Innovation: A Meta-Analysis of Effects of Determinants and Moderators," *Academy of management journal* (34:3), pp. 555-590.
Damaraju, N. L., and Makhija, A. K. 2018. "The Role of Social Proximity in Professional Ceo Appointments: Evidence from Caste/Religion-Based Hiring of Ceos in India," *Strategic Management Journal* (39:7), pp. 2051-2074.
Datta, D. K., Rajagopalan, N., and Rasheed, A. M. 1991. "Diversification and Performance: Critical Review and Future Directions," *Journal of Management Studies* (28:5), pp. 529-558.
Demerjian, P., Lev, B., and McVay, S. 2012. "Quantifying Managerial Ability: A New Measure and Validity Tests," *Management science* (58:7), pp. 1229-1248.
Demerjian, P. R., Lev, B., Lewis, M. F., and McVay, S. E. 2013. "Managerial Ability and Earnings Quality," *The accounting review* (88:2), pp. 463-498.
Denrell, J., and March, J. G. 2001. "Adaptation as Information Restriction: The Hot Stove Effect," *Organization Science* (12:5), pp. 523-538.

Dess, G. G., and Beard, D. W. 1984. "Dimensions of Organizational Task Environments," *Administrative science quarterly*), pp. 52-73.
Dewan, S., Michael, S. C., and Min, C.-K. 1998. "Firm Characteristics and Investments in Information Technology: Scale and Scope Effects," *Information Systems Research* (9:3), pp. 219-232.
DiMaggio, P. J., and Powell, W. W. 1983. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields," *American sociological review*), pp. 147-160.
Donaldson, L. 2001. *The Contingency Theory of Organizations*. Sage.
Downey, H. K., Hellriegel, D., and Slocum Jr, J. W. 1975. "Environmental Uncertainty: The Construct and Its Application," *Administrative science quarterly*), pp. 613-629.
Drazin, R., and Van de Ven, A. H. 1985. "Alternative Forms of Fit in Contingency Theory," *Administrative science quarterly*), pp. 514-539.
Duncan, R. B. 1972. "Characteristics of Organizational Environments and Perceived Environmental Uncertainty," *Administrative science quarterly*), pp. 313-327.
Eisenhardt, K. M. 1989. "Agency Theory: An Assessment and Review," *Academy of management review* (14:1), pp. 57-74.
Ernest Chang, S., and Ho, C. B. 2006. "Organizational Factors to the Effectiveness of Implementing Information Security Management," *Industrial Management & Data Systems* (106:3), pp. 345-361.
Esposito, C., Castiglione, A., Martini, B., and Choo, K.-K. R. 2016. "Cloud Manufacturing: Security, Privacy, and Forensic Concerns," *IEEE Cloud Computing* (3:4), pp. 16-22.
Fama, E. F. 1980. "Agency Problems and the Theory of the Firm," *Journal of political economy* (88:2), pp. 288-307.
Fang, C., Lee, J., and Schilling, M. 2010. "Balancing Exploration and Exploitation through Structural Design: Advantage of the Semi-Isolated Subgroup Structure in Organizational Learning," *Organization Science* (21), pp. 625-642.
Farooq, O., Rupp, D. E., and Farooq, M. 2017. "The Multiple Pathways through Which Internal and External Corporate Social Responsibility Influence Organizational Identification and Multifoci Outcomes: The Moderating Role of Cultural and Social Orientations," *Academy of Management Journal* (60:3), pp. 954-985.
Ferrell, A., Liang, H., and Renneboog, L. 2016. "Socially Responsible Firms," *Journal of financial economics* (122:3), pp. 585-606.
Fichman, R. G. 2001. "The Role of Aggregation in the Measurement of It-Related Organizational Innovation," *MIS quarterly*), pp. 427-455.
Fichman, R. G. 2004. "Real Options and It Platform Adoption: Implications for Theory and Practice," *Information systems research* (15:2), pp. 132-154.
Fichman, R. G., and Kemerer, C. F. 1997. "The Assimilation of Software Process Innovations: An Organizational Learning Perspective," *Management science* (43:10), pp. 1345-1363.
Fiol, C. M., and Lyles, M. A. 1985. "Organizational Learning," *Academy of management review* (10:4), pp. 803-813.
Flammer, C. 2015. "Does Corporate Social Responsibility Lead to Superior Financial Performance? A Regression Discontinuity Approach," *Management Science* (61:11), pp. 2549-2568.
Flammer, C., and Bansal, P. 2017. "Does a Long-Term Orientation Create Value? Evidence from a Regression Discontinuity," *Strategic Management Journal* (38:9), pp. 1827-1847.
Flammer, C., and Kacperczyk, A. 2016. "The Impact of Stakeholder Orientation on Innovation: Evidence from a Natural Experiment," *Management Science* (62:7), pp. 1982-2001.
Flammer, C., and Kacperczyk, A. 2019. "Corporate Social Responsibility as a Defense against Knowledge Spillovers: Evidence from the Inevitable Disclosure Doctrine," *Strategic Management Journal* (40:8), pp. 1243-1267.
Flammer, C., and Luo, J. 2017. "Corporate Social Responsibility as an Employee Governance Tool: Evidence from a Quasi-Experiment," *Strategic Management Journal* (38:2), pp. 163-183.
Fleming, L. 2001. "Recombinant Uncertainty in Technological Search," *Management science* (47:1), pp. 117-132.
Fong, E. A., and Tosi Jr, H. L. 2007. "Effort, Performance, and Conscientiousness: An Agency Theory Perspective," *Journal of Management* (33:2), pp. 161-179.
Gal-Or, E., and Ghose, A. 2005. "The Economic Incentives for Sharing Security Information," *Information Systems Research* (16:2), pp. 186-208.
Gamache, D. L., Neville, F., Bundy, J., and Short, C. E. 2020. "Serving Differently: Ceo Regulatory Focus and Firm Stakeholder Strategy," *Strategic Management Journal* (41:7), pp. 1305-1335.
Garel, A., and Petit-Romec, A. 2020. "Engaging Employees for the Long Run: Long-Term Investors and Employee-Related Csr," *Journal of Business Ethics*), pp. 1-29.

George, J. F. 1996. "Computer-Based Monitoring: Common Perceptions and Empirical Results," *Mis Quarterly*), pp. 459-480.
Gnyawali, D. R., and Stewart, A. C. 2003. "A Contingency Perspective on Organizational Learning: Integrating Environmental Context, Organizational Learning Processes, and Types of Learning," *Management Learning* (34:1), pp. 63-89.
Goerzen, A., and Beamish, P. W. 2005. "The Effect of Alliance Network Diversity on Multinational Enterprise Performance," *Strategic management journal* (26:4), pp. 333-354.
Gond, J. P., El Akremi, A., Swaen, V., and Babu, N. 2017. "The Psychological Microfoundations of Corporate Social Responsibility: A Person-Centric Systematic Review," *Journal of Organizational Behavior* (38:2), pp. 225-246.
Gordon, L. A., Loeb, M. P., and Lucyshyn, W. 2003. "Sharing Information on Computer Systems Security: An Economic Analysis," *Journal of Accounting and Public Policy* (22:6), pp. 461-485.
Grant, R. M., Jammine, A. P., and Thomas, H. 1988. "Diversity, Diversification, and Profitability among British Manufacturing Companies, 1972–1984," *Academy of management Journal* (31:4), pp. 771-801.
Graydon, J., and Griffin, M. 1996. "Specificity and Variability of Practice with Young Children," *Perceptual and motor skills* (83:1), pp. 83-88.
Greening, D. W., and Turban, D. B. 2000. "Corporate Social Performance as a Competitive Advantage in Attracting a Quality Workforce," *Business & society* (39:3), pp. 254-280.
Greenwood, B. N., and Gopal, A. 2017. "Ending the Mending Wall: Herding, Media Coverage, and Co-Location in It Entrepreneurship," *MIS Quarterly: Management Information Systems* (41:3).
Greve, H. R. 2003. *Organizational Learning from Performance Feedback: A Behavioral Perspective on Innovation and Change*. Cambridge University Press.
Griffeth, R. W., Hom, P. W., and Gaertner, S. 2000. "A Meta-Analysis of Antecedents and Correlates of Employee Turnover: Update, Moderator Tests, and Research Implications for the Next Millennium," *Journal of management* (26:3), pp. 463-488.
Gruschka, N., and Jensen, M. 2010. "Attack Surfaces: A Taxonomy for Attacks on Cloud Services," *2010 IEEE 3rd international conference on cloud computing*: IEEE, pp. 276-279.
Gubler, T., Larkin, I., and Pierce, L. 2018. "Doing Well by Making Well: The Impact of Corporate Wellness Programs on Employee Productivity," *Management Science* (64:11), pp. 4967-4987.
Guillén, M. F., and Capron, L. 2016. "State Capacity, Minority Shareholder Protections, and Stock Market Development," *Administrative Science Quarterly* (61:1), pp. 125-160.
Guo, K. H. 2013. "Security-Related Behavior in Using Information Systems in the Workplace: A Review and Synthesis," *Computers & Security* (32), pp. 242-251.
Gurbaxani, V., and Whang, S. 1991. "The Impact of Information Systems on Organizations and Markets," *Communications of the ACM* (34:1), pp. 59-73.
Gwebu, K. L., Wang, J., and Wang, L. 2018. "The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management," *Journal of Management Information Systems* (35:2), pp. 683-714.
Haislip, J., Lim, J.-H., and Pinsker, R. 2021. "The Impact of Executives' It Expertise on Reported Data Security Breaches," *Information Systems Research*).
Hall Jr, E. H., and St. John, C. H. 1994. "A Methodological Note on Diversity Measurement," *Strategic Management Journal* (15:2), pp. 153-168.
Hambrick, D. C., Cho, T. S., and Chen, M.-J. 1996. "The Influence of Top Management Team Heterogeneity on Firms' Competitive Moves," *Administrative science quarterly*), pp. 659-684.
Hanelt, A., Bohnsack, R., Marz, D., and Antunes Marante, C. 2020. "A Systematic Review of the Literature on Digital Transformation: Insights and Implications for Strategy and Organizational Change," *Journal of Management Studies*).
Harris, M., and Raviv, A. 1978. "Some Results on Incentive Contracts with Applications to Education and Employment, Health Insurance, and Law Enforcement," *The American economic review* (68:1), pp. 20-30.
Hart, M., Manadhata, P., and Johnson, R. 2011. "Text Classification for Data Loss Prevention," *International Symposium on Privacy Enhancing Technologies Symposium*: Springer, pp. 18-37.
Hauer, B. 2015. "Data and Information Leakage Prevention within the Scope of Information Security," *IEEE Access* (3), pp. 2554-2565.
Hausman, J. A. 1978. "Specification Tests in Econometrics," *Econometrica: Journal of the econometric society*), pp. 1251-1271.
Heckman, J. J. 1977. "Sample Selection Bias as a Specification Error (with an Application to the

Estimation of Labor Supply Functions)," 0898-2937, National Bureau of Economic Research.
Hedström, K., Kolkowska, E., Karlsson, F., and Allen, J. P. 2011. "Value Conflicts for Information Security Management," *The Journal of Strategic Information Systems* (20:4), pp. 373-384.
Herath, T., and Rao, H. R. 2009a. "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems* (47:2), pp. 154-165.
Herath, T., and Rao, H. R. 2009b. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 106-125.
Higgs, J. L., Pinsker, R. E., Smith, T. J., and Young, G. R. 2016. "The Relationship between Board-Level Technology Committees and Reported Security Breaches," *Journal of Information Systems* (30:3), pp. 79-98.
Hilary, G., Segal, B., and Zhang, M. H. 2016. "Cyber-Risk Disclosure: Who Cares?," *Georgetown McDonough School of Business Research Paper*:2852519).
Hite, G. L., and Long, M. S. 1982. "Taxes and Executive Stock Options," *Journal of Accounting and Economics* (4:1), pp. 3-14.
Hitt, M. A., Hoskisson, R. E., Johnson, R. A., and Moesel, D. D. 1996. "The Market for Corporate Control and Firm Innovation," *Academy of management journal* (39:5), pp. 1084-1119.
Ho-Jin, P., and Cho, J.-S. 2016. "The Influence of Information Security Technostress on the Job Satisfaction of Employees," *Journal of Business and Retail Management Research* (11:1).
Hoberg, G., and Phillips, G. 2010. "Product Market Synergies and Competition in Mergers and Acquisitions: A Text-Based Analysis," *The Review of Financial Studies* (23:10), pp. 3773-3811.
Hoberg, G., and Phillips, G. 2016. "Text-Based Network Industries and Endogenous Product Differentiation," *Journal of Political Economy* (124:5), pp. 1423-1465.
Hölmstrom, B. 1979. "Moral Hazard and Observability," *The Bell journal of economics*), pp. 74-91.
Hou, K., and Robinson, D. T. 2006. "Industry Concentration and Average Stock Returns," *The Journal of Finance* (61:4), pp. 1927-1956.
Hsu, C., Lee, J.-N., and Straub, D. W. 2012. "Institutional Influences on Information Systems Security Innovations," *Information systems research* (23:3-part-2), pp. 918-939.
Hu, Q., Hart, P., and Cooke, D. 2007. "The Role of External and Internal Influences on Information Systems Security–a Neo-Institutional Perspective," *The Journal of Strategic Information Systems* (16:2), pp. 153-172.
Hua, J., and Bapna, S. 2013. "Who Can I Trust?: The Economic Impact of Insider Threats," *Journal of Global Information Technology Management* (16:4), pp. 47-67.
Huber, G. P. 1991. "Organizational Learning: The Contributing Processes and the Literatures," *Organization science* (2:1), pp. 88-115.
Hughes, J. S., Liu, J., and Liu, J. 2007. "Information Asymmetry, Diversification, and Cost of Capital," *The accounting review* (82:3), pp. 705-729.
Hull, C. E., and Rothenberg, S. 2008. "Firm Performance: The Interactions of Corporate Social Performance with Innovation and Industry Differentiation," *Strategic management journal* (29:7), pp. 781-789.
Hurley, R. F., and Hult, G. T. M. 1998. "Innovation, Market Orientation, and Organizational Learning: An Integration and Empirical Examination," *Journal of marketing* (62:3), pp. 42-54.
Hwang, I., and Cha, O. 2018. "Examining Technostress Creators and Role Stress as Potential Threats to Employees' Information Security Compliance," *Computers in Human Behavior* (81), pp. 282-293.
Jackofsky, E. F., and Peters, L. H. 1983. "The Hypothesized Effects of Ability in the Turnover Process," *Academy of Management Review* (8:1), pp. 46-49.
Jacobs, B. W., Swink, M., and Linderman, K. 2015. "Performance Effects of Early and Late Six Sigma Adoptions," *Journal of Operations Management* (36), pp. 244-257.
Janakiraman, R., Lim, J. H., and Rishika, R. 2018. "The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer," *Journal of Marketing* (82:2), pp. 85-105.
Jansen, J. J., Van Den Bosch, F. A., and Volberda, H. W. 2006. "Exploratory Innovation, Exploitative Innovation, and Performance: Effects of Organizational Antecedents and Environmental Moderators," *Management science* (52:11), pp. 1661-1674.
Jansen, J. J., Vera, D., and Crossan, M. 2009. "Strategic Leadership for Exploration and Exploitation: The Moderating Role of Environmental Dynamism," *The Leadership Quarterly* (20:1), pp. 5-18.
Jehn, K. A., Northcraft, G. B., and Neale, M. A. 1999. "Why Differences Make a Difference: A Field

Study of Diversity, Conflict and Performance in Workgroups," *Administrative science quarterly* (44:4), pp. 741-763.
Jensen, M. L., Dinger, M., Wright, R. T., and Thatcher, J. B. 2017. "Training to Mitigate Phishing Attacks Using Mindfulness Techniques," *Journal of Management Information Systems* (34:2), pp. 597-626.
Jensen, M. L., Wright, R., Durcikova, A., and Karumbaiah, S. 2020. "Building the Human Firewall: Combating Phishing through Collective Action of Individuals Using Leaderboards," *Available at SSRN 3622322*).
Jiang, R. J., Tao, Q. T., and Santoro, M. D. 2010. "Alliance Portfolio Diversity and Firm Performance," *Strategic management journal* (31:10), pp. 1136-1144.
Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS quarterly*), pp. 549-566.
Jordan, A. H., and Audia, P. G. 2012. "Self-Enhancement and Learning from Performance Feedback," *Academy of Management Review* (37:2), pp. 211-231.
Judge, T. A., Thoresen, C. J., Bono, J. E., and Patton, G. K. 2001. "The Job Satisfaction–Job Performance Relationship: A Qualitative and Quantitative Review," *Psychological bulletin* (127:3), p. 376.
Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., and Stulz, R. M. 2020. "Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms," *Journal of Financial Economics*).
Kannan, K., Rees, J., and Sridhar, S. 2007. "Market Reactions to Information Security Breach Announcements: An Empirical Analysis," *International Journal of Electronic Commerce* (12:1), pp. 69-91.
Karahanna, E., Chen, A., Liu, Q. B., and Serrano, C. 2019. "Capitalizing on Health Information Technology to Enable Digital Advantage in U.S. Hospitals," *MIS Quarterly* (43:1), pp. 113-140.
Kayworth, T., and Whitten, D. 2010. "Effective Information Security Requires a Balance of Social and Technology Factors," *MIS Quarterly executive* (9:3), pp. 2012-2052.
Keats, B. W., and Hitt, M. A. 1988. "A Causal Model of Linkages among Environmental Dimensions, Macro Organizational Characteristics, and Performance," *Academy of management journal* (31:3), pp. 570-598.
Khan, F. S., Kim, J. H., Moore, R. L., and Mathiassen, L. 2019. "Data Breach Risks and Resolutions: A Literature Synthesis,").
Kim, K., Gopal, A., and Hoberg, G. 2016. "Does Product Market Competition Drive Cvc Investment? Evidence from the Us It Industry," *Information Systems Research* (27:2), pp. 259-281.
King, J. L., Gurbaxani, V., Kraemer, K. L., McFarlan, F. W., Raman, K., and Yap, C.-S. 1994. "Institutional Factors in Information Technology Innovation," *Information systems research* (5:2), pp. 139-169.
Kirsch, L. J. 2004. "Deploying Common Systems Globally: The Dynamics of Control," *Information systems research* (15:4), pp. 374-395.
Kirsch, L. J., Ko, D.-G., and Haney, M. H. 2010. "Investigating the Antecedents of Team-Based Clan Control: Adding Social Capital as a Predictor," *Organization Science* (21:2), pp. 469-489.
Kleis, L., Chwelos, P., Ramirez, R. V., and Cockburn, I. 2012. "Information Technology and Intangible Output: The Impact of It Investment on Innovation Productivity," *Information Systems Research* (23:1), pp. 42-59.
Klimkiewicz, K., and Oltra, V. 2017. "Does Csr Enhance Employer Attractiveness? The Role of Millennial Job Seekers' Attitudes," *Corporate Social Responsibility and Environmental Management* (24:5), pp. 449-463.
Koellinger, P. 2008. "The Relationship between Technology, Innovation, and Firm Performance—Empirical Evidence from E-Business in Europe," *Research policy* (37:8), pp. 1317-1328.
Koester, A., Shevlin, T., and Wangerin, D. 2016. "The Role of Managerial Ability in Corporate Tax Avoidance," *Management Science* (63:10), pp. 3285-3310.
Koh, P. S., Qian, C., and Wang, H. 2014. "Firm Litigation Risk and the Insurance Value of Corporate Social Performance," *Strategic Management Journal* (35:10), pp. 1464-1482.
Kohli, R., and Kettinger, W. J. 2004. "Informating the Clan: Controlling Physicians' Costs and Outcomes," *Mis Quarterly*), pp. 363-394.
Kolympiris, C., Hoenen, S., and Klein, P. G. 2019. "Learning by Seconding: Evidence from National Science Foundation Rotators," *Organization Science* (30:3), pp. 528-551.
Krueger, A. B. 1991. "Ownership, Agency, and Wages: An Examination of Franchising in the Fast Food Industry," *The Quarterly Journal of Economics* (106:1), pp. 75-101.

Krüger, P. 2015. "Corporate Goodness and Shareholder Wealth," *Journal of financial economics* (115:2), pp. 304-329.
Kwon, J., and Johnson, M. E. 2014. "Proactive Versus Reactive Security Investments in the Healthcare Sector," *Mis Quarterly* (38:2).
Kwon, J., and Johnson, M. E. 2018. "Meaningful Healthcare Security: Does "Meaningful-Use" Attestation Improve Information Security Performance?," *MIS Quarterly* (42:4), pp. 1043-1067.
Kwon, J., Ulmer, J. R., and Wang, T. 2012. "The Association between Top Management Involvement and Compensation and Information Security Breaches," *Journal of Information Systems* (27:1), pp. 219-236.
Laffont, J.-J., and Martimort, D. 2009. *The Theory of Incentives: The Principal-Agent Model*. Princeton university press.
Laker, D. R. 1991. "Job Search, Perceptions of Alternative Employment and Turnover," *Journal of Applied Business Research (JABR)* (7:1), pp. 6-15.
Landwehr, C. E. 2004. "Improving Information Flow in the Information Security Market," in *Economics of Information Security*. Springer, pp. 155-163.
Leland, H. E. 2007. "Financial Synergies and the Optimal Scope of the Firm: Implications for Mergers, Spinoffs, and Structured Finance," *The Journal of Finance* (62:2), pp. 765-807.
Levitt, B., and March, J. G. 1988. "Organizational Learning," *Annual review of sociology* (14:1), pp. 319-338.
Lewellen, W. G. 1971. "A Pure Financial Rationale for the Conglomerate Merger," *The journal of Finance* (26:2), pp. 521-537.
Li, J., Netessine, S., and Koulayev, S. 2018. "Price to Compete… with Many: How to Identify Price Competition in High-Dimensional Space," *Management Science* (64:9), pp. 4118-4136.
Li, M., and Simerly, R. L. 1998. "The Moderating Effect of Environmental Dynamism on the Ownership and Performance Relationship," *Strategic Management Journal* (19:2), pp. 169-179.
Li, S., and Zhan, X. 2018. "Product Market Threats and Stock Crash Risk," *Management Science* (65:9), pp. 4011-4031.
Liang, H., Xue, Y., Pinsonneault, A., and Wu, Y. 2019. "What Users Do Besides Problem-Focused Coping When Facing It Security Threats: An Emotion-Focused Coping Perspective," *MIS Quarterly* (43:2), pp. 373-394.
Lim, E. N., and McCann, B. T. 2014. "Performance Feedback and Firm Risk Taking: The Moderating Effects of Ceo and Outside Director Stock Options," *Organization Science* (25:1), pp. 262-282.
Lin, Y., Shi, W., Prescott, J. E., and Yang, H. 2019. "In the Eye of the Beholder: Top Managers' Long-Term Orientation, Industry Context, and Decision-Making Processes," *Journal of Management* (45:8), pp. 3114-3145.
Lineberry, S. 2007. "The Human Element: The Weakest Link in Information Security," *Journal of Accountancy* (204:5), p. 44.
Liu, C.-W., Huang, P., and Lucas, H. C. 2020. "Centralized It Decision Making and Cybersecurity Breaches: Evidence from Us Higher Education Institutions," *JOURNAL OF MANAGEMENT INFORMATION SYSTEMS* (37:3), pp. 758–787.
Liu, F., Shu, X., Yao, D., and Butt, A. R. 2015. "Privacy-Preserving Scanning of Big Content for Sensitive Data Exposure with Mapreduce," *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*: ACM, pp. 195-206.
Liu, Y., and Ravichandran, T. 2015. "Alliance Experience, It-Enabled Knowledge Integration, and Ex Ante Value Gains," *Organization Science* (26:2), pp. 511-530.
Lu, Y., and Ramamurthy, K. 2010. "Proactive or Reactive It Leaders? A Test of Two Competing Hypotheses of It Innovation and Environment Alignment," *European Journal of Information Systems* (19:5), pp. 601-618.
Luo, Y. 2002. "Product Diversification in International Joint Ventures: Performance Implications in an Emerging Market," *Strategic Management Journal* (23:1), pp. 1-20.
Luthans, F. 1998. "Organisational Behaviour 8th Edition." Boston, MA: Irwin, McGraw-Hill.
Makridis, C., and Dean, B. 2018. "Measuring the Economic Effects of Data Breaches on Firm Outcomes: Challenges and Opportunities," *Journal of Economic and Social Measurement* (43:1-2), pp. 59-83.
Maksimov, V., Wang, S. L., and Yan, S. 2019. "Global Connectedness and Dynamic Green Capabilities in Mnes," *Journal of International Business Studies*), pp. 1-18.
March, J. G. 1991. "Exploration and Exploitation in Organizational Learning," *Organization science* (2:1), pp. 71-87.
Margolis, J. D., and Walsh, J. P. 2003. "Misery Loves Companies: Rethinking Social Initiatives by

Business," *Administrative science quarterly* (48:2), pp. 268-305.
Markides, C. C., and Williamson, P. J. 1994. "Related Diversification, Core Competences and Corporate Performance," *Strategic Management Journal* (15:S2), pp. 149-165.
Martin, J. D., and Sayrak, A. 2003. "Corporate Diversification and Shareholder Value: A Survey of Recent Literature," *Journal of corporate finance* (9:1), pp. 37-57.
Maskarinec, A. S., and Thompson, C. P. 1976. "The within-List Distributed Practice Effect: Tests of the Varied Context and Varied Encoding Hypotheses," *Memory & Cognition* (4:6), pp. 741-746.
Matusik, S. F., and Fitza, M. A. 2012. "Diversification in the Venture Capital Industry: Leveraging Knowledge under Uncertainty," *Strategic Management Journal* (33:4), pp. 407-426.
McLain, D. L. 1995. "Responses to Health and Safety Risk in the Work Environment," *Academy of Management Journal* (38:6), pp. 1726-1743.
McLeod, A., and Dolezel, D. 2018. "Cyber-Analytics: Modeling Factors Associated with Healthcare Data Breaches," *Decision Support Systems* (108), pp. 57-68.
McWilliams, A., and Siegel, D. 2000. "Corporate Social Responsibility and Financial Performance: Correlation or Misspecification?," *Strategic management journal* (21:5), pp. 603-609.
McWilliams, A., and Siegel, D. 2001. "Corporate Social Responsibility: A Theory of the Firm Perspective," *Academy of management review* (26:1), pp. 117-127.
Mendelson, H., and Pillai, R. R. 1998. "Clockspeed and Informational Response: Evidence from the Information Technology Industry," *Information Systems Research* (9:4), pp. 415-433.
Miller, A. R., and Tucker, C. E. 2011. "Can Health Care Information Technology Save Babies?," *Journal of Political Economy* (119:2), pp. 289-324.
Miller, D. J. 2006. "Technological Diversity, Related Diversification, and Firm Performance," *Strategic Management Journal* (27:7), pp. 601-619.
Milliken, F. J. 1987. "Three Types of Perceived Uncertainty About the Environment: State, Effect, and Response Uncertainty," *Academy of Management review* (12:1), pp. 133-143.
Mithas, S., and Rust, R. T. 2016. "How Information Technology Strategy and Investments Influence Firm Performance: Conjecture and Empirical Evidence," *Mis Quarterly* (40:1), pp. 223-245.
Mithas, S., Tafti, A., and Mitchell, W. 2013. "How a Firm's Competitive Environment and Digital Strategic Posture Influence Digital Business Strategy," *MIS quarterly*), pp. 511-536.
Mitra, S., and Ransbotham, S. 2015. "Information Disclosure and the Diffusion of Information Security Attacks," *Information Systems Research* (26:3), pp. 565-584.
Moody, G. D., Siponen, M., and Pahnila, S. 2018. "Toward a Unified Model of Information Security Policy Compliance," *MIS quarterly* (42:1).
Mory, L., Wirtz, B. W., and Göttel, V. 2016. "Factors of Internal Corporate Social Responsibility and the Effect on Organizational Commitment," *The International Journal of Human Resource Management* (27:13), pp. 1393-1425.
Nagar, V., Nanda, D., and Wysocki, P. 2003. "Discretionary Disclosure and Stock-Based Incentives," *Journal of accounting and economics* (34:1-3), pp. 283-309.
Nagle, F. 2019. "Open Source Software and Firm Productivity," *Management Science* (65:3), pp. 1191-1215.
Nayyar, P. R. 1992. "On the Measurement of Corporate Diversification Strategy: Evidence from Large Us Service Firms," *Strategic Management Journal* (13:3), pp. 219-235.
Neffke, F., and Henning, M. 2013. "Skill Relatedness and Firm Diversification," *Strategic Management Journal* (34:3), pp. 297-316.
Ocasio, W. 2011. "Attention to Attention," *Organization science* (22:5), pp. 1286-1296.
Ojha, D., Acharya, C., and Cooper, D. 2018. "Transformational Leadership and Supply Chain Ambidexterity: Mediating Role of Supply Chain Organizational Learning and Moderating Role of Uncertainty," *International Journal of Production Economics* (197), pp. 215-231.
Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' Behavior Towards Is Security Policy Compliance," *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*: IEEE, pp. 156b-156b.
Palepu, K. 1985. "Diversification Strategy, Profit Performance and the Entropy Measure," *Strategic management journal* (6:3), pp. 239-255.
Palich, L. E., Cardinal, L. B., and Miller, C. C. 2000. "Curvilinearity in the Diversification–Performance Linkage: An Examination of over Three Decades of Research," *Strategic management journal* (21:2), pp. 155-174.
Palmer, T. B., and Wiseman, R. M. 1999. "Decoupling Risk Taking from Income Stream Uncertainty: A Holistic Model of Risk," *Strategic Management Journal* (20:11), pp. 1037-1062.
Papadimitriou, P., and Garcia-Molina, H. 2011. "Data Leakage Detection," *IEEE Transactions on knowledge and data engineering* (23:1), pp. 51-63.

Parker, O. N., Krause, R., and Covin, J. G. 2017. "Ready, Set, Slow: How Aspiration-Relative Product Quality Impacts the Rate of New Product Introduction," *Journal of Management* (43:7), pp. 2333-2356.
Peltier, T. R. 2013. *Information Security Fundamentals*. CRC press.
Peng, L., and Röell, A. 2014. "Managerial Incentives and Stock Price Manipulation," *The Journal of Finance* (69:2), pp. 487-526.
Petrenko, O. V., Aime, F., Ridge, J., and Hill, A. 2016. "Corporate Social Responsibility or Ceo Narcissism? Csr Motivations and Organizational Performance," *Strategic Management Journal* (37:2), pp. 262-279.
Pienta, D., Thatcher, J., Sun, H., and George, J. 2018. "Information Systems Betrayal: When Cybersecurity Systems Shift from Agents of Protection to Agents of Harm," *Information Systems* (6), p. 26.
Posey, C., Bennett, B., Roberts, T., and Lowry, P. B. 2011. "When Computer Monitoring Backfires: Invasion of Privacy and Organizational Injustice as Precursors to Computer Abuse," *Journal of Information System Security* (7:1), pp. 24-47.
Posey, C., Roberts, T. L., and Lowry, P. B. 2015. "The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets," *Journal of Management Information Systems* (32:4), pp. 179-214.
Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., and Courtney, J. F. 2013. "Insiders' Protection of Organizational Information Assets: Development of a Systematics-Based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors," *Mis Quarterly*), pp. 1189-1210.
Post, G. V., and Kagan, A. 2007. "Evaluating Information Security Tradeoffs: Restricting Access Can Interfere with User Tasks," *Computers & Security* (26:3), pp. 229-237.
Qian, C., Lu, L. Y., and Yu, Y. 2019. "Financial Analyst Coverage and Corporate Social Performance: Evidence from Natural Experiments," *Strategic Management Journal* (40:13), pp. 2271-2286.
Qian, Y., Fang, Y., and Gonzalez, J. J. 2012. "Managing Information Security Risks During New Technology Adoption," *Computers & security* (31:8), pp. 859-869.
Rabier, M. R. 2017. "Acquisition Motives and the Distribution of Acquisition Performance," *Strategic Management Journal* (38:13), pp. 2666-2681.
Ransbotham, S., Fichman, R. G., Gopal, R., and Gupta, A. 2016. "Special Section Introduction—Ubiquitous It and Digital Vulnerabilities," *Information Systems Research* (27:4), pp. 834-847.
Ratnawat, R., and Jha, P. 2014. "Impact of Job Related Stress on Employee Performance: A Review and Research Agenda," *Journal of Business and Management* (16:11), pp. 1-16.
Ravichandran, T., Liu, Y., Han, S., and Hasan, I. 2009. "Diversification and Firm Performance: Exploring the Moderating Effects of Information Technology Spending," *Journal of Management Information Systems* (25:4), pp. 205-240.
Robins, J., and Wiersema, M. F. 1995. "A Resource-Based Approach to the Multibusiness Firm: Empirical Analysis of Portfolio Interrelationships and Corporate Financial Performance," *Strategic management journal* (16:4), pp. 277-299.
Rogers, E. M. 2003. "Diffusion of Innovations. Free Press," *New York* (551).
Rogers Everett, M. 1995. "Diffusion of Innovations," *New York* (12).
Ross, S. A. 1973. "The Economic Theory of Agency: The Principal's Problem," *The American economic review* (63:2), pp. 134-139.
Rumelt, R. P. 1974. "Strategy, Structure, and Economic Performance,").
Russo, M. V., and Fouts, P. A. 1997. "A Resource-Based Perspective on Corporate Environmental Performance and Profitability," *Academy of management Journal* (40:3), pp. 534-559.
Sabherwal, R., Sabherwal, S., Havakhor, T., and Steelman, Z. 2019. "How Does Strategic Alignment Affect Firm Performance? The Roles of Information Technology Investment and Environmental Uncertainty," *MIS Quarterly* (43:2).
Safa, N. S., and Von Solms, R. 2016. "An Information Security Knowledge Sharing Model in Organizations," *Computers in Human Behavior* (57), pp. 442-451.
Sakhartov, A. V. 2017. "Economies of Scope, Resource Relatedness, and the Dynamics of Corporate Diversification," *Strategic Management Journal* (38:11), pp. 2168-2188.
Saldanha, T. J., Sahaym, A., Mithas, S., Andrade-Rojas, M. G., Kathuria, A., and Lee, H.-H. 2020. "Turning Liabilities of Global Operations into Assets: It-Enabled Social Integration Capacity and Exploratory Innovation," *Information Systems Research*).
Sanders, W. G. 2001. "Behavioral Responses of Ceos to Stock Ownership and Stock Option Pay," *Academy of Management journal* (44:3), pp. 477-492.
Sarkar, S., Vance, A., Ramesh, B., Demestihas, M., and Wu, D. T. 2020. "The Influence of Professional Subculture on Information Security Policy Violations: A Field Study in a Healthcare Context,"

Information Systems Research (31:4), pp. 1240-1259.
Schilling, M. A., Vidal, P., Ployhart, R. E., and Marangoni, A. 2003. "Learning by Doing Something Else: Variation, Relatedness, and the Learning Curve," *Management science* (49:1), pp. 39-56.
Schmidt, R. A. 1975. "A Schema Theory of Discrete Motor Skill Learning," *Psychological review* (82:4), p. 225.
Schneier, B. 2015. *Secrets and Lies: Digital Security in a Networked World*. John Wiley & Sons.
Schwab, D. P., and Cummings, L. L. 1970. "Theories of Performance and Satisfaction: A Review," *Industrial Relations: A journal of economy and society* (9:4), pp. 408-430.
Sen, R., and Borle, S. 2015. "Estimating the Contextual Risk of Data Breach: An Empirical Approach," *Journal of Management Information Systems* (32:2), pp. 314-341.
Seo, J., Gamache, D. L., Devers, C. E., and Carpenter, M. A. 2015. "The Role of Ceo Relative Standing in Acquisition Behavior and Ceo Pay," *Strategic Management Journal* (36:12), pp. 1877-1894.
Servaes, H., and Tamayo, A. 2013. "The Impact of Corporate Social Responsibility on Firm Value: The Role of Customer Awareness," *Management science* (59:5), pp. 1045-1061.
Sheng, H., Nah, F. F.-H., and Siau, K. 2008. "An Experimental Study on Ubiquitous Commerce Adoption: Impact of Personalization and Privacy Concerns," *Journal of the Association for Information Systems* (9:6), p. 15.
Shiu, Y. M., and Yang, S. L. 2017. "Does Engagement in Corporate Social Responsibility Provide Strategic Insurance-Like Effects?," *Strategic Management Journal* (38:2), pp. 455-470.
Shu, X., Yao, D., and Bertino, E. 2015. "Privacy-Preserving Detection of Sensitive Data Exposure," *IEEE transactions on information forensics and security* (10:5), pp. 1092-1103.
Simon, H. A. 1985. "What I Know About the Creative Process," *Frontiers in creative and innovative management* (4), pp. 3-22.
Singh, A., and Malhotra, M. 2015. "Security Concerns at Various Levels of Cloud Computing Paradigm: A Review," *International journal of computer networks and applications* (2:2), pp. 41-45.
Sinkula, J. M. 1994. "Market Information Processing and Organizational Learning," *Journal of marketing* (58:1), pp. 35-45.
Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS quarterly*), pp. 487-502.
Solove, D. J., and Citron, D. K. 2017. "Risk and Anxiety: A Theory of Data-Breach Harms," *Tex. L. Rev.* (96), p. 737.
Soto-Acosta, P. 2020. "Covid-19 Pandemic: Shifting Digital Transformation to a High-Speed Gear," *Information Systems Management* (37:4), pp. 260-266.
Spetz, J., and Maiuro, L. S. 2004. "Measuring Levels of Technology in Hospitals," *The quarterly review of economics and finance* (44:3), pp. 430-447.
Spreitzer, G. M. 1995. "Psychological Empowerment in the Workplace: Dimensions, Measurement, and Validation," *Academy of management Journal* (38:5), pp. 1442-1465.
St. John, C. H., and Harrison, J. S. 1999. "Manufacturing-Based Relatedness, Synergy, and Coordination," *Strategic Management Journal*), pp. 129-145.
Stock, G. N., and Tatikonda, M. V. 2008. "The Joint Influence of Technology Uncertainty and Interorganizational Interaction on External Technology Integration Success," *Journal of operations management* (26:1), pp. 65-80.
Straub Jr, D. W., and Nance, W. D. 1990. "Discovering and Disciplining Computer Abuse in Organizations: A Field Study," *MIS quarterly*), pp. 45-60.
Sullivan, B. N. 2010. "Competition and Beyond: Problems and Attention Allocation in the Organizational Rulemaking Process," *Organization Science* (21:2), pp. 432-450.
Sung, S. Y., Choi, J. N., and Kang, S. C. 2017. "Incentive Pay and Firm Performance: Moderating Roles of Procedural Justice Climate and Environmental Turbulence," *Human resource management* (56:2), pp. 287-305.
Sussman, S. W., and Siegal, W. S. 2003. "Informational Influence in Organizations: An Integrated Approach to Knowledge Adoption," *Information systems research* (14:1), pp. 47-65.
Swanson, E. B., and Ramiller, N. C. 2004. "Innovating Mindfully with Information Technology," *MIS quarterly*), pp. 553-583.
Takabi, H., Joshi, J. B., and Ahn, G.-J. 2010. "Security and Privacy Challenges in Cloud Computing Environments," *IEEE Security & Privacy* (8:6), pp. 24-31.
Tallman, S., and Li, J. 1996. "Effects of International Diversity and Product Diversity on the Performance of Multinational Firms," *Academy of Management journal* (39:1), pp. 179-196.
Tamjidyamcholo, A., Baba, M. S. B., Shuib, N. L. M., and Rohani, V. A. 2014. "Evaluation Model for Knowledge Sharing in Information Security Professional Virtual Community," *Computers & Security* (43), pp. 19-34.

Tanriverdi, H. 2005. "Information Technology Relatedness, Knowledge Management Capability, and Performance of Multibusiness Firms," *MIS quarterly*), pp. 311-334.
Tanriverdi, H. 2006. "Performance Effects of Information Technology Synergies in Multibusiness Firms," *Mis Quarterly*), pp. 57-77.
Tanriverdi, H., and Venkatraman, N. 2005. "Knowledge Relatedness and the Performance of Multibusiness Firms," *Strategic management journal* (26:2), pp. 97-119.
Tatikonda, M. V., and Montoya-Weiss, M. M. 2001. "Integrating Operations and Marketing Perspectives of Product Innovation: The Influence of Organizational Process Factors and Capabilities on Development Performance," *Management science* (47:1), pp. 151-172.
Tatikonda, M. V., and Rosenthal, S. R. 2000. "Technology Novelty, Project Complexity, and Product Development Project Execution Success: A Deeper Look at Task Uncertainty in Product Innovation," *IEEE Transactions on engineering management* (47:1), pp. 74-87.
Terza, J. V., Basu, A., and Rathouz, P. J. 2008. "Two-Stage Residual Inclusion Estimation: Addressing Endogeneity in Health Econometric Modeling," *Journal of health economics* (27:3), pp. 531-543.
Thornhill, S., and White, R. E. 2007. "Strategic Purity: A Multi-Industry Evaluation of Pure Vs. Hybrid Business Strategies," *Strategic Management Journal* (28:5), pp. 553-561.
Tian, F., and Xu, S. X. 2015. "How Do Enterprise Resource Planning Systems Affect Firm Risk? Post-Implementation Impact," *Mis Quarterly* (39:1).
Tong, L., Wang, H., and Xia, J. 2020. "Stakeholder Preservation or Appropriation? The Influence of Target Csr on Market Reactions to Acquisition Announcements," *Academy of Management Journal* (63:5), pp. 1535-1560.
Tosi, H. L., Katz, J. P., and Gomez-Mejia, L. R. 1997. "Disaggregating the Agency Contract: The Effects of Monitoring, Incentive Alignment, and Term in Office on Agent Decision Making," *Academy of Management Journal* (40:3), pp. 584-602.
Trantopoulos, K., von Krogh, G., Wallin, M. W., and Woerter, M. 2017. "External Knowledge and Information Technology: Implications for Process Innovation Performance," *MIS quarterly* (41:1), pp. 287-300.
Turner, S. F., and Rindova, V. P. 2018. "Watching the Clock: Action Timing, Patterning, and Routine Performance," *Academy of Management Journal* (61:4), pp. 1253-1280.
Tushman, M. L., and Anderson, P. 1986. "Technological Discontinuities and Organizational Environments," *Administrative science quarterly*), pp. 439-465.
Tushman, M. L., and Nadler, D. A. 1978. "Information Processing as an Integrating Concept in Organizational Design," *Academy of management review* (3:3), pp. 613-624.
Van Der Vegt, G. S., and Bunderson, J. S. 2005. "Learning and Performance in Multidisciplinary Teams: The Importance of Collective Team Identification," *Academy of management Journal* (48:3), pp. 532-547.
Vance, A., Lowry, P. B., and Eggett, D. 2013. "Using Accountability to Reduce Access Policy Violations in Information Systems," *Journal of Management Information Systems* (29:4), pp. 263-290.
Vance, A., Lowry, P. B., and Eggett, D. L. 2015. "Increasing Accountability through the User Interface Design Artifacts: A New Approach to Addressing the Problem of Access-Policy Violations," *Mis Quarterly* (39:2), pp. 345-366.
Varadarajan, P. R. 1986. "Product Diversity and Firm Performance: An Empirical Investigation," *Journal of Marketing* (50:3), pp. 43-57.
Vera, D., and Crossan, M. 2004. "Strategic Leadership and Organizational Learning," *Academy of management review* (29:2), pp. 222-240.
Vermeulen, C., and Von Solms, R. 2002. "The Information Security Management Toolbox–Taking the Pain out of Security Management," *Information Management & Computer Security* (10:3), pp. 119-125.
Vial, G. 2019. "Understanding Digital Transformation: A Review and a Research Agenda," *The Journal of Strategic Information Systems* (28:2), pp. 118-144.
Waldman, D. A., Ramirez, G. G., House, R. J., and Puranam, P. 2001. "Does Leadership Matter? Ceo Leadership Attributes and Profitability under Conditions of Perceived Environmental Uncertainty," *Academy of management journal* (44:1), pp. 134-143.
Wang, H., and Choi, J. 2013. "A New Look at the Corporate Social–Financial Performance Relationship: The Moderating Roles of Temporal and Interdomain Consistency in Corporate Social Performance," *Journal of Management* (39:2), pp. 416-441.
Wang, J., Gupta, M., and Rao, H. R. 2015. "Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications," *MIS quarterly* (39:1), pp. 91-112.
Wang, P., and Ramiller, N. C. 2009. "Community Learning in Information Technology Innovation," *MIS*

quarterly), pp. 709-734.
Wang, T., and Bansal, P. 2012. "Social Responsibility in New Ventures: Profiting from a Long-Term Orientation," *Strategic Management Journal* (33:10), pp. 1135-1153.
Warkentin, M., and Willison, R. 2009. "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," *European Journal of Information Systems* (18:2), pp. 101-105.
Weigelt, C., and Sarkar, M. B. 2009. "Learning from Supply-Side Agents: The Impact of Technology Solution Providers' Experiential Diversity on Clients' Innovation Adoption," *Academy of Management Journal* (52:1), pp. 37-60.
Whitler, K. A., and Farris, P. W. 2017. "The Impact of Cyber Attacks on Brand Image: Why Proactive Marketing Expertise Is Needed for Managing Data Breaches," *Journal of Advertising Research* (57:1), pp. 3-9.
Whitman, M. E., and Mattord, H. J. 2011. *Principles of Information Security*. Cengage Learning.
Wiengarten, F., Fan, D., Lo, C. K., and Pagell, M. 2017. "The Differing Impacts of Operational and Financial Slack on Occupational Safety in Varying Market Conditions," *Journal of Operations Management*).
Wiengarten, F., Fan, D., Pagell, M., and Lo, C. K. 2019. "Deviations from Aspirational Target Levels and Environmental and Safety Performance: Implications for Operations Managers Acting Irresponsibly," *Journal of Operations Management* (65:6), pp. 490-516.
Willison, R., and Warkentin, M. 2013. "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *MIS quarterly*), pp. 1-20.
Willison, R., Warkentin, M., and Johnston, A. C. 2018. "Examining Employee Computer Abuse Intentions: Insights from Justice, Deterrence and Neutralization Perspectives," *Information Systems Journal* (28:2), pp. 266-293.
Wooldridge, J. 2003. "Introductory Econometrics Mason," *OH: Thomson/South Western*).
Xue, L., Ray, G., and Gu, B. 2011. "Environmental Uncertainty and It Infrastructure Governance: A Curvilinear Relationship," *Information Systems Research* (22:2), pp. 389-399.
Xue, L., Ray, G., and Sambamurthy, V. 2012. "Efficiency or Innovation: How Do Industry Environments Moderate the Effects of Firms'it Asset Portfolios?," *Mis Quarterly* (36:2).
Xue, L., Ray, G., and Sambamurthy, V. 2013. "Efficiency or Innovation: How Do Industry Environments Moderate the Effects of Firms' It Asset Portfolios,").
Xue, L., Ray, G., and Zhao, X. 2017. "Managerial Incentives and It Strategic Posture," *Information Systems Research* (28:1), pp. 180-198.
Yoo, C. W., Goo, J., and Rao, H. R. 2020. "Is Cybersecurity a Team Sport? A Multilevel Examination of Workgroup Information Security Effectiveness," *MIS Quarterly* (44:2).
Zajac, E. J., and Westphal, J. D. 1994. "The Costs and Benefits of Managerial Incentives and Monitoring in Large Us Corporations: When Is More Not Better?," *Strategic management journal* (15:S1), pp. 121-142.
Zaltman, G., Duncan, R., and Holbek, J. 1973. *Innovations and Organizations*. John Wiley & Sons.
Zollo, M., and Winter, S. G. 2002. "Deliberate Learning and the Evolution of Dynamic Capabilities," *Organization science* (13:3), pp. 339-351.

APPENDICES
APPENDIX A. Variable Description

Table A. Variable Descriptions

Panel A. Variable Descriptions for Study 1

Variable	Notation	Description	Source
Data breach risk	$BREACH_{ij}$	An indicator variable equals 1 if firm *i* has a reported breach in year *j* or *j* + 1, and 0 otherwise.	PRC, ITRC
IT innovativeness	$INNO_{ij}$	The weighted sum of firm *i*'s implemented ITs in year *j*, with the weight of each IT being the percentage of firms that *do not* implement the IT in the same year, as in Karahanna et al. (2019) and Spetz and Maiuro (2004).	CI database
Managerial Ability	MA_{ij}	Managerial ability score of firm *i* in year *j* from Demerjian (2012). The score was computed using the DEA method, where total sales are optimized using a comprehensive vector of inputs.[56]	Peter Demerjian data
Environmental dynamism	DYN_{ij}	Regressing firm *i*'s industry sales on a five-year period in year *j*, and standardizing the resulting standard error of the regression coefficient by the average industry sale for each four-digit SIC code, as in Keats and Hitt (1988).	COMPUSTAT
Environmental complexity	COM_{ij}	The opposite of the quadratic sum of firms' market shares in firm *i*'s industry in year *j*, as in Hou and Robinson (2006) and Mithas et al. (2013).	COMPUSTAT
Firm size	$SIZE_{ij}$	The natural logarithm of firm *i* 's value of total assets (in $millions) in year *j*.	COMPUSTAT
R&D expense	$R\&D_{ij}$	The natural logarithm of the R&D expenses (in $millions) of firm *i* in year *j*.	COMPUSTAT
Firm Loss	$LOSS_{ij}$	An indicator variable equal to 1 if firm *i* reported negative net income in year *j*.	COMPUSTAT
Firm leverage	$LEVERAGE_{ij}$	The natural logarithm of division between the beginning total liabilities and the beginning total assets of firm *i* in year *j*.	COMPUSTAT
Business Scope	$BUSN_{ij}$	Number of segments operated by firm *i* in year *j*, as in Silhan and Thomas (1986).	COMPUSTAT
Previously Accumulated Number of Breaches	$BREACH\_PRE_{ij}$	Total number of previous breaches that have been compromised by firm *i* to the end of year *j*.[57]	PRC, ITRC
Total product similarity	$SIMILARITY_{ij}$	Total sum of product similarity of firm *i* with other firms within its industry in year *j*, as in Kim et al. (2016).	TNIC database
IT innovativeness (alternative measure)	$INNO\_DUMMY_{ij}$	An indicator variable equals to 1 if firm *i* is included on the IW500 list in year *j*.	IW500
Data breach risk (alternative measure)	$BREACH\_NUM_{ij}$	The accumulated number of data breaches reported by firm *i* in year *j* and *j* + 1.	PRC, ITRC
Internal Breach Risk	$BREACH\_IN_{ij}$	An indicator variable equals to 1 if firm *i* has a reported data breach caused by its insiders (e.g., employee or vendors) in year *j* or *j* + 1, and 0 otherwise.	PRC, ITRC

[56] The vector of inputs includes the cost of goods sold and inventory, SG&A expenses, PP&E, operating lease, R&D expenditures, goodwill, and other fixed or intangible assets.
[57] Only the breaches in my sample period are considered in calculating *BREACH_PRE.*

External Breach Risk	$BREACH\_EX_{ij}$	An indicator variable equal to 1 if firm *i* has a reported breach that its caused by its outsiders (e.g., burglars or hackers) in year *j* or *j* + 1, and 0 otherwise.	PRC, ITRC

Panel B. Variable Descriptions for Study 2

Variable	Notation	Description	Source
Data breach risk	$BREACH_{ij}$	The accumulated number of data breaches reported by firm *i* in year *j* + 1.	PRC, ITRC
Data breach risk (the first alternative measure)	$BREACH\_LAG2_{ij}$	The accumulated number of data breaches reported by firm *i* in year *j* + 1 or year *j*+2.	PRC, ITRC
Data breach risk (the second alternative measure)	$BREACH\_DUMMY_{ij}$	An indicator variable equals 1 if firm *i* has a reported breach in year *j* + 1 and 0 otherwise.	PRC, ITRC
Employee-related CSR	$EMPLOYEE\_CSR_{ij}$	The standardized sum of employee-related strength ratings minus the standardized sum of employee-related concern ratings of firm *i* in year *j*. Only consistent rating items in the employee dimension are considered in the calculation.	KLD database
Employee-related CSR (the alternative measure)	$EM\_CSR\_UNSTD_{ij}$	The sum of employee-related strength ratings minus the sum of employee-related concern ratings of firm *i* in year *j*. Only consistent rating items in the employee dimension are considered in the calculation.	KLD database
Negative performance	NEG_PER_{ij}	The average of firms' historical and social negative performances of firm *i* in year *j*.	COMPUSTAT
Environmental dynamism	DYN_{ij}	Regressing firm *i*'s industry sales on a five-year period in year *j*, and standardizing the resulting standard error of the regression coefficient by the average industry sale for each four-digit SIC code.	COMPUSTAT
Product similarity	$TNIC3TSIMM_{ij}$	Total sum of product similarity of firm *i* with other firms within its industry in year *j*.	TNIC data
Firm size	$SIZE_{ij}$	The natural logarithm of firm *i* 's value of total assets (in $millions) in year *j*.	COMPUSTAT
Sales growth	$GROWTH_{ij}$	The division between the difference between the current and preceding year's sales and the current year's sales of firm *i* in year *j*.	COMPUSTAT
Firm leverage	$LEVERAGE_{ij}$	The natural logarithm of the ratio of the beginning total liabilities divided by the beginning total assets of firm *i* in year *j*.	COMPUSTAT
Firm age	AGE_{ij}	The number of years since firm *i* has been established to year *j*.	COMPUSTAT
R&D expense	$R\&D_{ij}$	The natural logarithm of the R&D expenses (in $millions) of firm *i* in year *j*.	COMPUSTAT
Advertising intensity	$ADVERTISING_{ij}$	The advertising expense scaled by the total assets of firm *i* in year *j*.	COMPUSTAT
IT capability	IT_CAPA_{ij}	An indicator variable equals 1 if firm *i* is included on the IW500 list in year *j*.	IW500
Operational slack	OP_SLACK_{ij}	The natural logarithm of industry adjusted ratio of annual sales to tangible assets of firm *i* in year *j*.	COMPUSTAT
Society-facing CSR	EN_CSR_{ij}/CO_CSR_{ij}/ DI_CSR_{ij}/PR_CSR_{ij}/	The sum of environment/ccommunity/governance/product -related strength scores minus the sum of environment-related of firm *i* in year *j*.	KLD database

Panel C. Variable Descriptions for Study 3

Variable	Notation	Description	Source
Data Breach Risk	$BREACH_{ij}$	An indicator variable equal to 1 if firm *i* reported a breach in the year *j* or *j+1*.	PRC
Total Diversification	TD_{ij}	Total diversification degree of firm *i*'s operations in different industries in year *j*, as in Chari et al. (2008) and Dewan et al. (1998).	COMPUSTAT
Related Diversification	RD_{ij}	Diversification degree of firm *i*'s operations in different related industries in year *j*, as in Chari et al. (2008) and Dewan et al. (1998).	COMPUSTAT
Unrelated Diversification	UD_{ij}	Diversification degree of firm *i*'s operations in different unrelated industries in year *j*, as in Chari et al. (2008) and Dewan et al. (1998).	COMPUSTAT
Managerial Ability	MA_{ij}	Managerial ability score of firm *i* in year *j* from Demerjian (2012). The score was computed using the DEA method, where total sales are optimized using a comprehensive vector of inputs.[58]	Peter Demerjian data
Product Market Competition	$TNIC3TSIMM_{ij}$	Total sum of the product similarity of firm *i* with other firms within its industry in year *j* from Hoberg and Phillips (2016).	Hoberg−Phillips TNIC data
Firm Size	$SIZE_{ij}$	Natural logarithm of firm *i*'s value of total assets in fiscal year *j*.	COMPUSTAT
Firm Loss	$LOSS_{ij}$	Indicator variable equal to 1 if firm *i* reported negative net income in year *j* or 0 otherwise.	COMPUSTAT
Firm Leverage	$LEVERAGE_{ij}$	Ratio of the beginning total liabilities divided by the beginning total assets of firm *i* in year *j*.	COMPUSTAT
Return on Assets	ROA_{ij}	Return on assets of firm *i* in year *j*.	COMPUSTAT
Operational Slack	OP_SLACK_{ij}	Natural logarithm of industry adjusted ratio of annual sales to tangible assets of firm *i* in year *j*, as in Azadegan et al. (2013).	COMPUSTAT
Previously Accumulated Number of Breaches	$BREACH\_PRE_{ij}$	Total accumulated number of previous breaches that have been compromised by firm *i* to the end of year *j−1*.[59]	PRC, ITRC
IT capability	IT_CAPA_{ij}	Indicator variable equals 1 if firm *i* is included on the IW500 list in year *j*.	IW500
Data Breach Risk (alternative measure)	$BREACH\_NUM_{ij}$	Accumulated number of data breaches reported by firm *i* in years *j* and *j+1*.	

[58] The vector of inputs includes the cost of goods sold and inventory, SG&A expenses, PP&E, operating lease, R&D expenditures, goodwill, and other fixed or intangible assets.

[59] Only the breaches in my sample period are considered in calculating *BREACH_PRE.*

Appendix B.

Table B. List of IT Applications and Their Saidin Weight

Technology Name	Saidin weight (2012)	Saidin weight (2013)	Saidin weight (2014)	Saidin weight (2015)
Accounting Software	0.43	0.48	0.48	0.48
Application Consolidation or EAI Software	0.93	0.95	0.95	0.95
Sever Computing Software	0.88	0.92	0.92	0.92
Asset Management Software	0.80	0.86	0.86	0.86
Business Intelligence (BI) Software	0.86	0.90	0.90	0.91
Call or Contact Center	0.80	0.85	0.85	0.85
Site's Mobile Service Include Data Features	0.80	0.85	0.85	0.85
Collaborative Software	0.88	0.90	0.90	0.90
Color Printers	0.56	0.67	0.67	0.67
CRM/SFA Software	0.86	0.83	0.83	0.83
Data Center or Data Warehouse Software	0.86	0.90	0.90	0.90
Database Management Software (DBMS)	0.57	0.63	0.63	0.63
Desktop Virtualization	0.99	0.99	0.99	0.99
Application Development Software	0.75	0.82	0.82	0.82
Document Management Software	0.84	0.89	0.89	0.89
e-Commerce via the Internet	0.90	0.93	0.93	0.93
Enterprise Management Software	0.81	0.86	0.86	0.87
Enterprise Resource Planning (ERP) Software	0.76	0.92	0.91	0.91
Google Applications, other than a web searching	1.00	1.00	1.00	1.00
Groupware Software	0.34	0.36	0.36	0.37
Handset or Smartphone	1.00	1.00	1.00	1.00
High Volume Printer	0.95	0.97	0.97	0.97
Human Resource Software	0.70	0.79	0.79	0.79
IBM Compatible Midrange Servers	0.90	0.93	0.93	0.93
IBM Compatible Mainframe	0.98	0.99	0.99	0.99
ID/Access Software	0.82	0.87	0.87	0.88
Multifunction Printers	0.58	0.69	0.69	0.69
Network Lines	0.45	0.50	0.49	0.50
Network Services, (MPLS, ATM, etc.)	0.78	0.84	0.84	0.85
3rd Party Data Center Management	0.95	0.95	0.95	0.95
3rd Part Disaster Recovery	0.97	0.98	0.98	0.98
3rd Party Firewall Services	0.95	0.97	0.97	0.97
3rd Party Hardware Maintenance	0.97	0.98	0.98	0.98
3rd Party Hardware Services	0.96	0.97	0.96	0.97
3rd Party Intrusion Detection Services (IDS)	0.79	0.84	0.84	0.84
3rd Party LAN Management Services	0.96	0.97	0.97	0.97
3rd Party Phone System Maintenance	0.88	0.91	0.91	0.91
3rd Party Server Maintenance	0.96	0.97	0.97	0.97
3rd Party Storage Management	0.95	0.96	0.96	0.96

3rd Party Software Services	0.91	0.93	0.93	0.93
3rd Party WAN Management Services	0.94	0.96	0.96	0.96
Phone System	0.27	0.27	0.26	0.27
Security Software	0.68	0.75	0.75	0.75
SONet Network Service	0.97	0.98	0.98	0.98
Storage Virtualization	0.98	0.98	0.98	0.98
Supply Chain Management Software	0.86	0.93	0.93	0.93
Software-as-a-Service (SaaS) CRM Software	0.90	0.92	0.90	0.90
Software-as-a-Service (SaaS) Email Software	0.99	0.99	0.99	0.99
Software-as-a-Service (SaaS) ERP Software	0.99	0.99	0.99	0.99
Software-as-a-Service (SaaS) Software	0.93	0.94	0.94	0.94
Software-as-a-Service (SaaS) Software	1.00	1.00	0.99	0.99
Software-as-a-Service (SaaS) Storage Software	0.98	0.98	0.98	0.98
Network Switch	0.64	0.72	0.71	0.72
Unified Communication Service (UCS)	0.97	0.97	0.97	0.97
Unix Servers	0.93	0.95	0.95	0.95
Uninterruptible Power Supply (UPS)	0.62	0.72	0.72	0.72
Video Conferencing Services	0.99	0.99	0.99	0.99
Virtual Private Network (VPN)	0.57	0.62	0.61	0.61
Web Services Software	0.89	0.92	0.92	0.92
Workflow Software	0.75	0.82	0.82	0.82

APPENDIX C. Imbalance Analysis for CEM Matching

Imbalance analysis (pre-matching)
Multivariate L1 distance: 0.9090
Univariate imbalance:

	L1	mean	min	25%	50%	75%	max
SIZE	0.40	2.42	10.62	2.10	2.48	2.38	−0.09
IT_SPEND	0.37	4.90E+07	0.00	4.00E+06	9.00E+07	1.30E+08	0.00
BUSN	0.34	4.22	1.00	0.00	6.00	6.00	−5.00
YEAR	0.57	−0.76	0.00	0.00	−1.00	−1.00	−2.00

Matching summary
Number of strata: 1,415; *Number of matched strata:* 187

	0	1
All	39,281	398
Matched	11,005	384
Unmatched	28,276	14

Multivariate L1 distance: 0.6737; *Univariate imbalance:*

	L1	mean	min	25%	50%	75%	max
SIZE	0.13	0.08	0.34	0.03	0.09	0.12	−0.18
IT_SPEND	0.05	6.30E+06	0.00	5.00E+07	.	.	.
BUSN	0.04	−0.02	0.00	−1.00	−1.00	0.00	0.00
YEAR	0.00	0.00	0.00	0.00	0.00	0.00	.

Appendix D.

Table D. CSR items in the Employee Dimension of KLD[60]

Employee protection strength (*EMP_str*)		**Included in main analysis (Yes/No)**	**Included in robustness check (Yes/No)**
EMP_str_A	Union Relations (from 1991)	Yes	Yes
EMP_str_B	No−Layoff Policy (1991 to 1993)	No	Yes
EMP_str_C	Cash Profit Sharing (from 1991)	Yes	Yes
EMP_str_D	Employee Involvement (from 1991)	Yes	Yes
EMP_str_F	Retirement Benefits Strength (1991 to 2009)	No	Yes
EMP_str_G	Employee Health and Safety (from 2003)	Yes	Yes
EMP_str_H	Supply Chain Labor Standards (from 2002)	Yes	Yes
EMP_str_I	Compensation & Benefits	Yes	Yes
EMP_str_J	Employee Relations	Yes	Yes
EMP_str_K	Professional Development	Yes	Yes
EMP_str_L	Human Capital Management	Yes	Yes
EMP_str_M	Labor Management (EMP−STR−M)	Yes	Yes
EMP_str_N	Controversial Sourcing (From 2013)	No	Yes
EMP_str_num	Total Number of Employee Relations Strengths (1991 to 2013)	No	Yes
EMP_str_X	Emp. Relations Other Strength (from 1991 through 2011)	No	Yes
Employee protection concern (*EMP_con*)			
EMP_con_A	Union Relations (from 1991)	Yes	Yes
EMP_con_B	Employee Health & Safety (from 1991)	Yes	Yes
EMP_con_C	Workforce Reductions (1991 to 2009)	No	Yes
EMP_con_D	Retirement Benefits Concern (1992 to 2009)	No	Yes
EMP_con_F	Supply Chain (from 1998)	Yes	Yes
EMP_con_G	Child Labor	Yes	Yes
EMP_con_H	Labor−Management Relations (EMP−CON−H)	Yes	Yes
EMP_con_num	Total Number of Employee Relations Concerns (1991 to 2013)	No	Yes
EMP_con_X	Labor−Management Relations	Yes	Yes

[60] Refer to MSCI (2015) for the definition of individual items.