CAN YOU HAVE YOUR CAKE AND EAT IT TOO? A TALE OF CYBERSECURITY AND OPERATIONAL EFFICIENCY

RUIQI LIU

PhD

The Hong Kong Polytechnic University

2022

The Hong Kong Polytechnic University

School of Accounting and Finance

Can You Have Your Cake and Eat It Too? A Tale of Cybersecurity and Operational Efficiency

Ruiqi LIU

A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy

October 2021

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)

Ruiqi LIU (Name of student)

Abstract

Information security has become the chief concern among corporate executives in the digital age, while the operational efficiency has been the primary concern of the corporate executives for a long history. This study would like to investigate the tale of cybersecurity and firms' operational efficiency – when the companies experience the data breaches, the firms' operational efficiency may be impacted and managers would be reminded of the significance of cybersecurity and pay more attention to the related issues. The attention based-view (ABV) of firms suggests that the managers have limited attention and they will allocate their attention according to the salience of different problems. Thus managers may put more additional resources, such as financial resources and employees, into the recovery issues from the damage of the data breaches. With the distraction of managers' attention and other operational resources to the cybersecurity and recovery issues, operational efficiency would decrease. Using a unique longitudinal data set of US listed firms from 2006 to 2016 and employing the PSM-DiD method, this paper shows that firms would experience a significant operational efficiency decrease after data breaches. The results are robust to a variety of tests on variable definitions, selection and endogeneity issues. Further dynamic DiD tests show that this deterioration effect only lasts for one year after data breaches. Besides, under the three premises of the ABV, focus of attention, structural distribution of attention, and situated attention, this paper finds that the negative relation between data breaches and operational efficiency would be ameliorated under different conditions in individual, organizational, and social levels respectively. Specifically, this paper finds that managerial risk-taking incentives, financial slack, and highly product competitive market would weaken the attention-distraction channel and the negative breach-efficiency relation. Taken together, the findings reveal the negative effect of data breaches on operational efficiency and firms' trade-off between cybersecurity and operational efficiency with limited managers' attention.

Keywords: information security, data breach, operational efficiency, attention-based view

JEL classification: M11, M12, M15

Acknowledgement

I appreciate the guidance and support from my chief-supervisor, Dr. Yong Jimmy Jin, and co-supervisors, Prof. C.S. Agnes Cheng, and Dr. Yangyang Fan; and the valuable comments, suggestions and help from Dr. Yang Duan, and Dr. Qian Wang. I also acknowledge the support of the Hong Kong PhD Fellowship from Hong Kong Research Grants Council (RGC) during my PhD study period. All errors are my own.

Table of contents

1. Introduction

In the era of ubiquitous computing, the volume of data breaches has been exponentially increasing every year as technology and electronic data spread the roots deeply in day-to-day business and operations. The Identity Theft Resource Center (ITRC) reports that the number of data breaches in 2019 increased by 17% over 2018. During the unique year of 2020, the COVID-19 pandemic forced firms worldwide to accelerate their pace of digital transformation in the attempt to emerge from the crisis ahead of their competitors. However, the accelerated deployment of digital processes and technologies has generally overburdened firms' existing strained security protections, triggering an even stronger wave of cybersecurity threats (Lallie et al., 2020; Williams et al., 2020).[1]

Anecdotal evidence has extensively suggested the serious impact for firms if they suffer from cyberattacks or data breaches, while we note that the academic research that has investigated the impact of cyberattacks or data breaches is relatively limited in scope. Previous research has studied the influence of data breaches on market value. Accordingly, we understand that data breaches cause firms' negative market reactions (Bharadwaj et al., 2009; Goldstein et al., 2011; Kamiya et al., 2020), particularly in certain contexts, such as in Internet or financial industries (Cavusoglu et al., 2004), prior to the 9/11 attacks (Gordon et al., 2011), or in large-scale breaches (Malhotra and Kubowicz Malhotra, 2011). In addition, some studies have investigated how data breaches impact firms' reputation, and found that breaches will cause firm reputation damage (Janakiraman et al.,

[1] MonsterCloud (https://monstercloud.com/) reports that the number of ransomware attacks has increased by approximately 800% during the COVID-19 pandemic.

2018; Syed, 2019), decline in brand value (Whitler and Farris, 2017), and the loss of customers (Kwon and Johnson, 2015).

However, the operational implications of data breaches have not been well understood. Against this backdrop, some related questions emerged: Will data breaches affect firms' operational efficiency? If so, what are the sources of the impact and do they have long-term impacts? Although the extant research offers no empirical answers to these questions, answering these questions would provide firms with critical comprehensive and systemic understanding of the short- and long-term impact of data breaches, which could help firms take the appropriate "next steps" following data breaches to mitigate their negative impacts. Accordingly, this paper proposes the first research question: (1) *How do data breaches impact firms' operational efficiency?*

This paper attempts to answer this preceding question on the theoretical basis of the attention-based view (ABV) of firms (Barnett, 2008; Ocasio, 1997). An ABV accounts for the fact that firms' decision makers have limited attentional capacity. Thus, they have bounded ability and rationality to handle the large portfolio of problems often confronting them. Given that attention resources are scarce and valuable, different problems eventually compete for limited attention in firms (Sullivan, 2010). Decision makers focus their attention on different problems separately, according to the salience of each problem, which is distinct under varying conditions (Ocasio, 2011; Ocasio et al., 2018). With the attention flowing into certain salient problems in a specific context, firms tend to invest additional resources (e.g., employee efforts, financial resources, technology systems) in these problem domains to develop solutions (Ocasio, 1997). In our context, managers in normal situations (i.e., in the absence of data breaches) tend to heavily prioritize maximizing the economic wealth of shareholders (Kayworth and Whitten, 2010; Lazonick and O'sullivan, 2000) through maintaining and improving firms' operational efficiency. However, data breaches, which represent

a shock to decision makers' cognition, invoke at least two aspects of firm problems. We argue that either problem may negatively impact operational efficiency by diverting decision makers' attention away from their normal concerns toward identifying solutions to these problems.

First, the occurrence of data breaches functions as a shock to decision makers and punctuates them the importance of information security. Situated in the context, information security becomes particularly salient and directs decision makers' attention toward rethinking the related problems (Fowler, 2016). With the attention and resources flowing into security, the curtailed attention and resources available for operational efficiency will lead to reduced operational efficiency. Moreover, considerable security attention and increased security investments tend to tighten firm security posture. The literature has suggested that tightened security will constrain employees' work routines, make them feel overloaded, and increase their pressure in operations (Bulgurcu et al., 2010; D'Arcy et al., 2014; D'Arcy and Teh, 2019; Herath and Rao, 2009a; Post and Kagan, 2007; Puhakainen and Siponen, 2010), thereby leading to reduced operational efficiency.

Second, the negative impacts of data breaches, such as damage to reputations, loss of customers, and massive fines, force firms to make recovery effort in numerous aspects (e.g., law, market, information technology (IT) system) (Goode et al., 2017; Gwebu et al., 2018; Masuch et al., 2020). Evidently, these recovery actions will subdivide decision makers' attention flow from improving operational efficiency toward these acute issues, thereby leading to reduced efficient operation.

Overall, security and recovery problems tend to be salient following breaches. These problems may distract decision makers, causing them to devote their attention to the acute problems at hand, which may lead to compromised operational efficiency. This attention-distraction channel motives our prediction that data breaches decrease firms' operational efficiency.

To further enhance our theoretical model and test the causal mechanism at play, this paper considers a set of contextual factors that moderate this primary relation. In particular, Ocasio (1997) suggests that a complete ABV framework involves three premises: (1) focus of attention, (2) structural distribution of attention, and (3) situated attention. In other words, how decision makers channel and distribute attention in a specific situation depends on these contextual constraints, which exist at individual, organizational, and social levels respectively.

First, an individual level ABV premise (i.e., focus of attention) suggests that how decision makers attend to a particular context is conditioned on their respective characteristics and cognition (Ocasio, 1997). Along this premise, this paper focuses on the moderator of managerial risk-taking incentives. We particularly argue that the focus of such a moderator could serve to determine the plausibility of our proposed channel (i.e., attention-distraction channel). That is, if this channel truly drives the breach-efficiency relation, then risk-tolerant managers tend to be less concerned about future security risks and recovery issues in the wake of data breaches (Holt and Laury, 2002; Ross, 2004), thus weakening the attention-distraction channel and mitigating breach-efficiency relation.

Second, the organizational level ABV premise (i.e., structural distribution of attention) suggests that the allocation of decision makers' attention depends on the firms' resource structure (Ocasio, 1997). Accordingly, this paper focuses on the moderator of financial slack, which also serves as an examiner of the attention-distraction channel. That is, if such a channel is true, then firms with considerable surplus resources tend to have sufficient resources to maintain efficient operations even if the firm's attention has been substantially distracted to addressing cybersecurity and recovery problems following data breaches (Azadegan et al., 2013; Voss et al., 2008). Hence, this condition mitigates the attention-distraction channel and breach-efficiency association.

Third, the social level ABV premise (i.e., situated attention) suggests that how decision makers channel and distribute attention is dependent on their external environment and social cognition (Ocasio, 1997). In terms of this premise, this paper focuses on the moderating role of product market competition. If the attention-distraction channel indeed drives our main finding, then firms located in a fiercely competitive market will likely continue to focus on urgent market problems such as pressure from rivals and customers, and be less likely to divert their attention away from maintaining efficiency, even following a breach (McCann and Bahl, 2017; Sullivan, 2010). Consequently, the attention-distraction channel is mitigated and the breach-efficiency association is weakened.

This paper explores the above predictions regarding the moderators through our second research question: (2) *How do managerial risk-taking incentives, financial slack, and product market competition individually moderate the relation between data breaches and operational efficiency?*

This paper examines these research questions through an empirical analysis of a unique data set of US-listed firms from 2006 to 2016. Considering selection bias concerns from both observable and unobservable factors, this paper adopted a propensity score matching (PSM) approach in our analysis to address selection bias concerns from observable factors, and adopted a difference-in-differences (DiD) analysis to resolve bias concerns related to unobservable factors. Combining a PSM approach with a DiD approach in our baseline analysis yielded results that are substantially consistent with our hypotheses: i.e., data breaches reduce firms' operational efficiency but this effect is weakened under certain conditions, e.g., when top managers are risk averse, when considerable surplus resources are stocked, or when the external market is fiercely competitive. This paper also found consistent results after performing a battery of robustness

checks, including a dynamic DiD test, a subsample test on exogenous breaches, alternative measures, and a placebo test to scrutinize the potential impact of "fake" breaches.

This study contributes to the literature in several ways. First, this study contributes to the extant literature on the influence of data breaches. A key research question emerging over the past two decades interrogates the impact of data breaches. Although there is ample research devoted to this question, its focus is largely limited to the scope of market response and reputation damage. The present study seeks to generate new insights by identifying the negative association between data breaches and operational efficiency. In addition, this paper builds a finer-grained understanding of the link between data breaches and operational efficiency by testing whether this relation is long-term or short-term, which represents an effective means for advancing knowledge.

Second, this paper contributes to the security technostress literature, a security behavioral research stream that has recently been attracting increasing academic interest (D'Arcy et al., 2014; D'Arcy and Teh, 2019; Ho-Jin and Cho, 2016; Hwang and Cha, 2018). Theories and findings in the literature accentuate the negative impact of security requirements and infrastructures on employees' behaviors and firm productivity. This paper is among the first to apply and provide an indirect test of the knowledge through a firm-level study.

Third, this research theoretically contributes to security literature by introducing attention-based view (ABV) as an explanation for economic efficiency-security tradeoff given the core viewpoint of ABV is that different problems compete for firm attentions and resources (Ocasio, 2011; Sullivan, 2010). Such an introduction has important implications given the limited number of theories employed thus far in the discourse investigating the impact of data breaches. Thus, this paper severs as a useful complement to ongoing research efforts and generates new ideas and

knowledge by linking two developed streams of research, namely, ABV and security literatures, that have not been connected previously.

Finally, the boundary condition analysis further unpacks the security-efficiency relation, makes the relationship more transparent, and complements the potential "missing links" in applying the ABV to the information security context. This paper determined that the breach-efficiency association is moderated by managerial risk-taking incentives, financial slack, and external market environment. Such findings are consistent with the ABV that decision-makers' attention allocation is conditional on individual, organizational, and social contextual constraints (Ocasio, 1997). In particular, the findings concerning slack also resonate with resource slack research, which suggests that surplus resources function as "a buffer of internal resources which allows firms to avoid the tradeoff they may face when handling multiple competitive objectives" (Modi and Mishra, 2011, p. 255).

The remainder of the paper is organized as follows. The next section is literature review. Section 3 discusses the theoretical background and hypothesis development. Section 4 describes the data and sample. The empirical results are presented in section 5. Section 6 discusses the empirical results, limitations and future research. Finally, section 7 concludes with a discussion of the implications and a summary of the empirical results.

2. Literature Review

There are three streams of literature that are directly related to this study: (1) the consequences of data breaches, (2) security technostress, and (3) determinants of operational efficiency.

2.1 Consequences of Data Breaches

In the digital era, data has become one of the most critical components of an enterprise. A data breach ensues when confidential or private information has been intentionally or inadvertently accessed by unauthorized parties (Cheng et al., 2017; Sen and Borle, 2015). Given the exponential growth in the volume of data and the severe business dependence upon the Internet, data breaches have been occurring more frequently than ever before and are attracting growing attention from executives.

Against such a backdrop, the past two decades have witnessed a proliferation of research exploring the consequences of data breaches. These studies can be classified along three lines: First, the earliest related studies investigated how data breaches influence firms' market values (Andoh-Baidoo and Osei-Bryson, 2007; Campbell et al., 2003; Garg et al., 2003; Hovav and D'Arcy, 2003; Hovav and D'Arcy, 2004; Png et al., 2008; Telang and Wattal, 2007; Yayla and Hu, 2011). However, the empirical findings of these studies are conflicting despite a solid theoretical basis for assuming negative economic impacts associated with data breach announcements. Second, emerging research has focused on firms' reputation-related impacts after breaches. Findings in the research include that the cumulative effect of breach events over a long time period reduces customers' visits (Kwon and Johnson, 2015), the announcement of data breaches decreases customer' spending levels (Janakiraman et al., 2018), and firm reputation threats are dependent on the type of data breach encountered (Syed, 2019). Third, several recent studies have found that firms tend to change strategies after experiencing a data breach; for example, firms may improve board-level IT governance (Benaroch and Chernobai, 2017), invest in corporate social responsibility (CSR) (Akey et al., 2018; Lending et al., 2018), or change executives (Nordlund, 2019).

Taken together, the preceding literature review indicates growing academic attention devoted to the consequences of data breaches. However, the related investigations remain limited in scope and there are relatively few theories employed in the discourse.

2.2 Security Technostress

Emerging behavioral information security literature has scrutinized employees' emotional and behavioral responses to security requirements (e.g., policies, IT controls and procedures). While the literature offers important insights into how security requirements can improve employees' security compliance behaviors, the literature also emphasizes the potential adverse effects of such implementations on employees and on firms' operations in the form of security technostress. (Chen et al., 2012; Herath and Rao, 2009a; Herath and Rao, 2009b; Johnston and Warkentin, 2010; Puhakainen and Siponen, 2010; Spears and Barki, 2010). D'Arcy et al. (2014) draw on deterrence theory to propose the concept of "security requirement stress" and suggest that firms' application of security requirements tends to increase employees' overload, complexity, and uncertainty in operations. D'Arcy and Teh (2019) further scrutinize security requirement stress, and suggest that security requirements tend to increase employees' frustration and fatigue in terms of managing operations. Posey et al. (2011) and Pienta et al. (2018) suggest the negative influence of security requirements on employees' working emotions; they find that the implementation of security requirements increases employees' perception of distrust (Posey et al., 2011) and betrayal (Pienta et al., 2018). Post and Kagan (2007) suggests a tradeoff between security and usability, and highlights the notion that tightening security by making systems more inaccessible can hinder employees and make them less productive. Jenkins et al. (2016) determined that system-generated alerts, which are beneficial for security, tend to impede employees' ability to rapidly switch attention among multiple tasks, thereby potentially compromising their operational efficiency.

The preceding studies have collectively suggested that firms' implementation of security requirements is a double-edged sword; that is, although such an implementation may play a role in protecting enterprise security, it is also vulnerable to cause considerable operational challenges, thereby hindering employees' efficiency. Given firms are reasonably expected to tighten their security requirements after the incidences of information security failures, it's consequently suggesting that there are opportunities to provide new insights into the focal literature by investigating whether data breaches may influence firms' operational efficiency. In addition, the perspective of security requirement stress provides useful insights into our understanding of this influence.

2.3 Determinants of Operational Efficiency

Prior studies indicate that a firm's relative performance with respect to operational efficiency could be explained by three major factors: firm's resources, routines, and capabilities (Peng et al., 2008; Lam et al., 2016). Of these factors, resources include tangible and intangible productive assets, routines refer to internal corporate governance within an organization, and capabilities consist of information and knowledge exchange across management and organizations (Kusunoki et al., 1998). Regarding the resources channel, many literatures have discussed about how the firms leverage the resources they possess to generate stronger positional advanteges and competitive outcomes (Hitt et al., 2016; Song et al., 2011; Parmigiani et al., 2011). As for the routines channel, Cheng et al. (2018) finds that operational efficiency is significantly lower among firms with material weakness in internal control and remediation of material weaknesses leads to an improvement in operational efficiency. Besides, Lam et al. (2016) find that firms' social media initiatives positively impact firms' operational efficiency by facilitating information flow and

knowledge sharing within and across organizations, supporting the routines and capacities channels.

Managers' attention is an important intangible productive assets for firms. Managers focus their attention on different problems separately according to the salience of each problem. Besides, other operational resources, such as employee efforts, financial resources, and technology systems, would also be putted into the corresponding problem together with the flow of managers' attention. In this study, we mainly focus on the resources channel for operational efficiency and argue that the cybersecurity problems and recovery issues emerged from data breaches distract mangers' attention and other resources from the operational efficiency, resulting in a decrease of operational efficiency after data breaches. We will provide a more detailed explanation below and develop our hypotheses accordingly.

3. Theoretical Background and Hypothesis Development

3.1 Attention Based View (ABV)

Attention based-view (ABV) represents a classical theory in organizational behavioral studies. The intellectual heritage of the ABV can be traced to Simon (1947), and has been developed in March and Herbert (1958), Cyert and March (1963), Cohen et al. (1972), March et al. (1976), Kiesler and Sproull (1982). These studies have adopted a similar viewpoint and updated Simon's (1947) structuring of attention by focusing on the distinct manner in which decision makers allocate and channel attention, such as, by routines (Cyert and March, 1963), through organized anarchy (Cohen et al., 1972), and via enactment processes (Weick, 2015).

Ocasio (1997) presented the explicit structure of the ABV. In this ABV, attention is defined as "the noticing, encoding, interpreting, and focusing of time and effort by organizational decision-

makers" on issues and answers (Ocasio, 1997, p. 189). This ABV fundamentally focuses on how firm decision makers distribute their attention to the virtually unlimited problems surrounding them (Barnett, 2008). Since decision makers have limited attentional resources, their ability to devote attention is bounded and may not be sufficient to focus on each firm problem that arises (Sullivan, 2010).

The ABV highlights three centered concepts in particular. First, the ABV suggests that "problems from different domains compete for attention" (Sullivan, 2010, p. 446), given that decision makers' attention is a valuable and limited firm resource. Therefore, attention gains in one problem domain should be accompanied by the attention loss in other problem domains (Ocasio, 2011; Sullivan, 2010). Second, the ABV highlights that the problem that decision makers "focus on depends on the specific situation" (Ocasio, 1997, p. 187). That is, decision makers' attention allocation actions are not predictable based on previous knowledge but are derived from the contexts in which they find themselves (Barnett, 2008). Third, the ABV emphasizes the concept that "what decision-makers do depends on what issues and answers they focus their attention on" (Ocasio, 1997, p. 187). In other words, when decision makers look for solutions to problems, they tend to deploy relevant resources to the problem domain where their attention is directed. Thus, decision makers' attention is a key driver of firm resource allocation (Ocasio, 1997; Sullivan, 2010). Our theorizing integrates such perspectives, as we describe next.

3.2 Data Breach and Attention Distraction

In normal situations (i.e., absent data breaches), decision makers tend to focus particularly on the aspect of firms' economic performance, which is their main responsibility because it provides returns to shareholders (Connelly et al., 2020). Thus, decision makers generally seek to demonstrate their success in terms of the related issues (e.g., increasing operational efficiency and

productivity), which are thus likely to dominate their attention. In normal situations, decision makers may also devote some attention to issues related to security and disruption recovery. However, decision makers tend to be overconfident and sanguine about the security state of the firm (Colwill, 2009) and are inclined to expect positive outcomes in terms of future firm operations (Fiske and Taylor, 2013). Thus, decision makers' focus on security and disruption recovery problems is often insufficient.

However, when firms experience a data breach, it sends a shock to decision makers and creates cognitive dissonance, meaning that their optimistic belief that their firm will continuously operate in a secure manner is disrupted. In the wake of data breaches, a variety of problems become further salient and divert decision makers' attention away from issues related to operational efficiency. This paper discusses such an attention-distraction mechanism of data breaches from two perspectives—security and recovery—and discusses their respective impacts on operational efficiency.

3.2.1 Attention Distraction by Cybersecurity Problems

This research proposes that decision makers' attention tend to be distracted by security problems following data breaches. The occurrence of data breaches, as an expectancy violation, exposes the security gaps of firms and remind decision makers that protecting security is important. Therefore, firms' security problems will emerge following breaches and force decision makers to specifically attend to these problems.

The ABV suggests that the allocation of firm resources tends to follow such an attentional direction and will—in this case, flow into security problems and the search for solutions (Ocasio, 1997; Sullivan, 2010). For example, breached firms may attempt to solve their security problems by implementing security trainings, updating security policies, investing in IT security

infrastructures, and hiring additional security IT experts (Benaroch and Chernobai, 2017; Gwebu et al., 2018). However, these actions consume resources that could have been utilized to maintain or improve operational efficiency (Sullivan, 2010, p. 446). Thus, firms' capability to increase operational efficiency is compromised.

More importantly, firms' intense focus on security following breaches may even drive significant efficiency gaps (D'Arcy et al., 2014; D'Arcy and Teh, 2019; Post and Kagan, 2007). IT experts have crystalized this phenomenon by noting that security and productivity are two forces in a continual tug of war. When pull too hard in the direction of security, worker productivity is likely to suffer. Maximizing efficiency requires convenient operations, such as easy access in any location on any device. However, protecting security entails complex, sophisticated, and meticulous settings that give employees only minimum access privileges and restrict user access to IT facilities. The divergent requirements required to maximize efficiency versus protect security create a security-efficiency tradeoff.

To further clarify the security-efficiency tradeoff, we draw from the security technostress literature and propose the reasons for this tradeoff in two aspects. On the one hand, protecting security may cause considerable inconveniences and may thereby reduce efficiency (Post and Kagan, 2007). For example, zero trust security model is recommended as one of the important steps after data breaches.[2] A zero trust strategy can help protect data and resources security through mutual authentication, including checking the identity and integrity of devices without respect to location, and providing access to applications and services based on the confidence of device identity and device health in combination with user authentication[3]. However, such an access

[2] See IBM Cost of a Data Breach Report 2021
[3] See https://en.wikipedia.org/wiki/Zero_trust_security_model

constraint may negatively impact productivity. Employees may also encounter substantial time and effort consumption by understanding new policies and deciding how to act. In addition, tight security controls may result in employees encountering additional obstacles, such as lost passwords, additional steps needed to perform routine tasks, difficulties accessing data, and even processing or network slowdowns from overhead imposed by security systems. These difficulties will also directly reduce employees' work efficiency.

On the other hand, protecting security may also introduce cognitive pressures on employees, thereby reducing efficiency. Prior literature has suggested that security requirements (i.e., policies, procedures, and technical controls) may cause information security technostress because of the complexity and uncertainty of these requirements (D'Arcy et al., 2014; D'Arcy and Teh, 2019). Employees may feel anxious while working because they have to consider whether they act appropriatedly following security protocols. Complying with security requirements may also engender a sense of work overload, causing employees to feel disengaged or overworked. We use one of the most common examples to simplify the understanding of the phenomenon: locked computers are annoying and create additional work but they are crucial for security. As D'Arcy et al. (2014, p. 289) explain, negative emotions regarding security protocols may reduce employees' efficiency because "employees view many security requirements as laborious and unnecessary overhead that impedes their productivity."

Overall, the evidence suggests that attention distraction via security problems in the wake of data breaches reduces firms' operational efficiency.

3.2.2 Attention Distraction by Recovery Problems

We further argue that decision makers' attention is also likely to be distracted by recovery problems following data breaches. Breached firms often suffer substantially from these incidents,

and may face lawsuits, stock plunges, damaged reputations, brand value declines, and customer losses (Brown, 2016; Fowler, 2016; Gwebu et al., 2018). Accordingly, firms typically find it necessary to engage in breach recovery actions. For example, firms my have to address legal issues following a breach, such as lawsuits, penalties, and compensating customers with compromised information. On a system level, breached firms may also have to repair systems that were damaged by the breach. Even after normal operations have resumed, firms may need to perform additional cleanup, determine the causes of the breaches, or assist external assets in this process. In market terms, breached firms may have to make additional investments to restore customer and investor confidence.

From the ABV perspective, as long as firm attention is consumed by recovery issues, the attention and resources that could have been devoted to efficiency are relatively reduced (Ocasio, 1997, p. 189; Sullivan, 2010, p. 446). Thus, we anticipate that attention distraction by recovery problems after breaches tends to negatively impact firms' operational efficiency.

The preceding discussion suggests that data breaches cause firms to focus on security and recovery problems and direct decision makers' attention flow into identifying solutions, thereby exerting a negative influence on firms' operational efficiency. Accordingly, we formulate the following hypothesis:

HYPOTHESIS 1 (H1). *The occurrences of data breaches would reduce firm's operational efficiency.*

3.3 Establishing Boundary Conditions

Ocasio's (1997) attention-based view (ABV) begins with the central viewpoint that what decision makers do is a function of their attention allocation; however, this theoretical perspective goes

further by suggesting three premises of decision makers' attention allocation in specific contexts: focus of attention, structural distribution of attention, and situated attention. Thus, we are provided with a framework to gain an improved understanding of the breach-efficiency relation. Following each of the three premises of ABV, we focus a moderator to probe the boundary conditions under which such a breach-efficiency relationship may or may not hold. Given that our theory suggests that an attention-distraction channel drives the breach-efficiency relationship, we predict each moderating role by analyzing how each moderator influences this channel.

3.3.1 Boundary Condition: Managerial Risk-Taking Incentives

The "focus of attention" premise of ABV is proposed in an individual level (Ocasio, 1997, p. 188). This premise suggests that decision makers' attention distraction by a certain problem is influenced by their own cognition. Besides, the preceding discussion about attention-distraction channel is mainly focus on reducing future risks. Accordingly, we focus on the moderator of managerial risk-taking incentives. Firms can increase top decision makers' (top managers') risk tolerance by providing them managerial risk-taking incentives. We contend that the attention-distraction channel is weakened if decision makers' risk tolerance is high. We believe this to be so for two reasons.

First, risk-tolerant top managers are less motivated to reduce future security risks (Holt and Laury, 2002; Ross, 2004). Thus, they tend to devote less attention to the security problems that emerge in the wake of a data breach, which thereby leaves sufficient attention available for operational efficiency. Second, if decision makers are risk tolerant, they tend to be less concerned about potential subsequent threats regardless of the domain of the threat invoked by the data breaches (e.g., business: customer loss; law: lawsuits; or technology: system interruption). In addition, risk tolerant decision makers may less worry that their inappropriate or insufficient

recovery efforts could intensity the negative impacts, and thus be less motivated to minimize future threats and engage in recovery efforts following a breach. In such situations, relatively less attention will be diverted from improving operational efficiency into recovery efforts, leading to a weakened attention-distraction channel.

In summary, we propose that if decision makers are provided with sufficient risk-taking incentives (with a relatively high degree of risk tolerance), the degree of attention distraction by means of security or recovery issues is low, thereby weakening the breach-efficiency association:

HYPOTHESIS 2 (H2). *Managerial risk-taking incentives weaken the negative relation between data breaches and operational efficiency*.

3.3.2 Boundary Condition: Financial Slack

The "structural distribution of attention" premise of ABV is proposed in an organizational level and emphasizes that decision-makers' attention allocation is dependent upon firm internal resources (Ocasio, 1997, p. 188). Accordingly, we focus on the moderator of financial slack, which represents "excess uncommitted financial resources, including cash and receivables" (Kim et al., 2008, p. 405). We focus on financial slack, rather than any absorbed slack (e.g., operational or human resource slack), because excess financial resources are highly flexible and decision makers often have great freedom in directing their allocation following a breach (Kim et al., 2008; Lungeanu et al., 2016; Nohria and Gulati, 1996).

For firms with a high level of excess financial resources, we contend that the attention-distraction channel is weakened following data breaches. Financial slack is currently uncommitted in firms and can be readily available for redeployment within firms (Kim et al., 2008; Vanacker et al., 2017; Wiengarten et al., 2017). Prior research has extensively suggested that firms' excess

resources, particularly the unabsorbed financial ones, help improve their recovery capabilities (Bourgeois, 1981; Latham and Braun, 2008). Accordingly, academic findings have shown that resource slack helps mitigate firms' negative market response to supply chain disruptions (Hendricks et al., 2009) and toy recalls (Wood et al., 2017).

Thus, we may reasonably expect that, following data breaches, surplus financial resources can be immediately redeployed to buffer against fluctuation and ensure operation continuity. That is, we expect that breached firms with sufficient financial slack can easily deploy their extra financial resources to ensure efficient operations, even if their attention and resources have been considerably distracted by the need to solve security and recovery problems. As a result, we predict that financial slack weakens the attention-distraction channel and mitigates the breach-efficiency association.

HYPOTHESIS 3 (H3). *Financial slack weakens the negative relation between data breaches and operational efficiency.*

3.3.3 Boundary Condition: Product Market Competition

The "situated attention" premise of ABV is proposed at a social level and highlights that external environmental context shapes the extent to which any given stimulus will attract attention and action (Ocasio, 1997, p. 188). As one of the important external environmental context, product market competition has been proved to have significant effect on managerial incentives, managerial slack, corporate governance, and financial policies (Schmidt, 1997; Karuna, 2007; Giroud and Mueller, 2011; Hoberg et al., 2014). Thus, this paper focuses the moderator of product market competition, which refers to firms' rivalry among the peer entities (Kim et al., 2016; Li and Zhan, 2019).

We argue that fiercely competitive markets tend to weaken the effect of the attention-distraction channel in the wake of data breaches. In highly competitive markets, firms' attention tends to be highly focused on urgent market problems, such as pressure from rivals and customer losses (Bennett et al., 2013; Dey et al., 2014). Thus, for the breached firms situated in the environment, ascribed to the great fear of being rapidly outcompeted, they tend to unable and unmotivated to afford a high level of attention flowing into security and recovery with sacrificing their operational efficiency, thereby weakening the attention-distraction channel and the breach-efficiency relation.

Furthermore, in intensively competitive markets, similarity between a firm's products and those of its peers tends to be high (Kim et al., 2016; Li and Zhan, 2018). High levels of similarity among different firms' products may reduce customers' product loyalty (Gremler and Brown, 1996; Karunaratna and Kumara, 2018). Thus, breached firms in highly competitive environments may not be motivated to make necessary recovery efforts in order to retain their current customers, who are relatively with a low degree of loyalty.

Based on this logic, it is reasonable to expect a weakened attention-distraction channel if firms are located in highly competitive markets, and thus, the influence of data breaches on firm operational efficiency is mitigated in the environment. Accordingly, we hypothesize:

HYPOTHESIS 4 (H4). *Product market competition weakens the negative relation between data breaches and operational efficiency*.

4. Data and Research Methods

4.1 Data and Sample Selection

Our data breach reports are collected from the Privacy Rights Clearinghouse (PRC) and Identity Theft Resource Center (ITRC), which are nonprofit organizations. PRC was established in 1992 and was commonly adopted by empirical information security research that focuses on US publicly traded firms (D'Arcy et al., 2020; Higgs et al., 2016; Kamiya et al., 2020). While the data breach reports in PRC is limited, we also collected data breach reports in ITRC, which has been publicly offering data breach reports since 2005, to offer a more robust representation of data breach sample. By combining all the data breach reports in the two databases, the data breach sample starts from 2006 and ends in 2016. After collecting the data breach reports, we manually matched the firm names in the reports with the firm names in COMPUSTAT to identify the ticker code of firms. If the names in reports could not entirely matched with the names in COMPUSTAT, we searched the firms' websites and other sources to further ensure a proper matching.

Firms' financial information and managers' compensation data are obtained from the COMPUSTAT database. Data on stock returns are retrieved from the Center for Research in Security Prices (CRSP) files. Risk free rates are get from Federal Reserve Bank database. After merging the aforementioned data, we exclude firms in financial industry (SIC codes 6000 - 6999)[4]. Observations with missing variables used in the regressions are also excluded. In sum, we finally get 157 firms with 285 data breach events between 2006 and 2016. Appendix A shows the distribution of the data breach firms over time and across industries. Appendix B shows the distribution of the data breach events over time and across industries.

4.2 Variables

[4] The definitions of asset and debt, thus the meaning of high leverage, are different between financial firms and other firms (Fama and French, 1992). We exclude firms in financial industries here.

We define our independent variable, *After_Data_Breach*, as a dummy variable which equals one if the observation is in the year of or after the first data breach during our sample period, and equals zero otherwise.

To measure operational efficiency, we use the Stochastic Frontier Estimation (SFE) methodology by following previous studies (Battese and Coelli, 1988; Li et al., 2010; Lam et al., 2016; Yiu et al., 2020). As for the SFE model, it models the relation between firms' operational inputs and outputs as shown in model (1). The number of employees, the cost of goods sold, and the capital expenditure are all operational inputs, and operating income is the operational output:

$$ln\,(Operating\ Income)_{ijt} = b_0 + b_1 ln(Number\ of\ Employees)_{ijt} + b_2 ln(Cost\ of\ Goods\ Sold)_{ijt} + b_3 ln(Capital\ Expenditure)_{ijt} + \varepsilon_{ijt} - h_{ijt} \quad (1)$$

The residual item in the model has two parts: random error and loss of efficiency. ε_{ijt} is the random error based on stochastic modeling, and h_{ijt} represents the loss of efficiency by firm i relative to industry j in year t (estimates based on two-digit SIC industry). h_{ijt} ranges from 0 to 1, and a high value indicates a high loss in efficiency (i.e., low operational efficiency). Then the operational efficiency of a firm relative to its industry is measured by:

$$Operational\ Efficiency_{ijt} = 1 - h_{ijt} \quad (2)$$

In order to increase the robustness of the measure, we firstly follow Battese and Coelli (1988) and estimates h_{ijt} based on the panel data structure model with half-normal distribution and get the corresponding operational efficiency for firm i in year t (*Operational Efficiency 1*$_{i,t}$). Then we follow the cross-sectional model in which firm effects have half-normal distribution (Jondrow et al., 1982) to get another estimates of h_{ijt} and compute the corresponding operational efficiency (*Operational Efficiency 2*$_{i,t}$) for firm i in year t.

Following prior studies on operational efficiency (Lam et al., 2016; Kortmann et al., 2014; Wu et al., 2010), we include firm size (*Ln(Assets)*, which represents the natural logarithm of a firm's total assets), firm leverage (*Leverage*, which represents a firm's total liability divided by total assets), firm profitability (*ROA*, which represents a firm's return on assets), firm R&D intensity (*R&D*, which represents the firm's R&D expenditures divided by total assets, where missing R&D expenses are treated as zeros), firm IT capability (*IT_Capability*, which equals one if the firm i in year t is included in the annual InformationWeek 500 (IW 500) list[5]), firm diversity (*Diversity*, which represents the natural logarithm of the number of firm's geographic segments), firm institutional ownership (*Institutional Ownership*, which represents the ratio of shares hold by institutional investors to firm's total outstanding shares in percentage), firm management ability (*Managerial Ability*, which represents managerial ability score of firm i in year t following Demerjian et al., (2012)), firm environment complexity (*Environmental Complexity*, which represents the opposite of concentration ratios for the top four firms in the firm's four-digit SIC industry, as in Keats and Hitt (1988)), firm environmental dynamism (*Environmental Dynamism*, which is measured by regressing an observation's industry sales on a five-year period, 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)), and firm environmental munificence (*Environmental Munificence*, which represents the availability of environmental resources to support growth. It equals the slope coefficient of the regression equation for calculating the

[5] InformationWeek 500 (IW 500) would identify the top users of information technology every year. If a firm is selected into the IW500 list, it is considered to have strong IT capabilities. The assessment is about how the firm configures and customizes generic IT resources to its specific business, and how the firm achieves technological, procedural, and organizational innovations with IT resources. The annual IW 500 list could get from https://www.informationweek.com/iw500.

environmental dynamism of the observation divided by the average sales of the industry, as in Keats and Hitt (1988)). Appendix C presents the variable descriptions.

4.3 Matched Control Firms

By no means do firms randomly occur data breaches. Rather, many factors, including IT applications (McLeod and Dolezel, 2018; Wang et al., 2015) and society-facing activities (D'Arcy et al., 2020), affect a firm's risk of experiencing a data breach. These factors, at the same time, also correlate with operational efficiency (Balabanis et al., 1998; Bharadwaj, 2000). So our estimated effect of data breaches on operational efficiency is subject to selection biases. To mitigate this concern, we matched each data breach event with an observation from firms with no data breaches in our sample period. Throughout the empirical tests, we use the matched sample to conduct our analysis.

To construct the matched sample, we used the PSM method to model the probability of data breaches. Specifically, we estimated the following logit model by using the data from one year prior to each data breach event for the treated firms (firms that have at least one data breach event during our sample period), and the data in all sample period years for non-breached firms:

$$
\begin{aligned}
Logit(Data\_Breach_{it} = 1) \\
&= \alpha_0 + \alpha_1 Ln(Assets_{i,t-1}) + \alpha_2 Leverage_{,i,t-1} + \alpha_3 ROA_{t-1} + \alpha_4 R\&D_{t-1} \\
&+ \alpha_5 IT\_Capability_{i,t-1} + \alpha_6 Diversity_{i,t-1} + \alpha_7 Institutional\ Ownership_{i,t-1} \\
&+ \alpha_8 Managerial\ Ability_{i,t-1} + \alpha_9 Environmental\ Complexity_{i,t-1} \\
&+ \alpha_{10} Environmental\ Dynamism_{i,t-1} \\
&+ \alpha_{11} Environmental\ Munificence_{i,t-1} + \alpha_{12} Loss\ Dummy_{i,t-1} \\
&+ Industry\ Dummies + Year\ Dummies \qquad (3)
\end{aligned}
$$

By matching each data breach observation with the control observation that had the closest propensity score within firms without data breach events, we identified our treated firms and

control firms. The firm-year observations of all treated and control firms in the 2006-2016 time frame without non-missing variables constructed our final sample, comprising 378 firms and 3,255 firm-year observations.The results of our estimation probability of data breach occurrences with model (3) are reported in Table 1. Panel A (Table 1) shows the results of the estimation of the probability of data breach occurrences with model (3). The *pseudo-R^2* of 0.379 indicates that explanatory variables can predict the occurrences of data breaches reasonably well. Panel B (Table 1) compares the characteristics of breached firms with matched non-breached firms prior to each data breach event. The results indicate that before the data breach events, breached firms and matched non-breached firms are similar for all the control variables, suggesting that these characteristics are unlikely to drive the difference in operational efficiency following a data breach.

[Insert Table 1 Here]

Panel A of Table 2 shows the sample selection process. Panels B and C (Table 2) show the sample distributions by year and by industry after employing PSM.

[Insert Table 2 Here]

4.4 Summary Statistics

Table 3 presents the summary statistics of our final matched sample. All continuous variables are winsorized at the 1% level and 99% level. On average, 27.3% of our sample had experienced data breaches. Our matched sample is larger than the pre-matched sample (mean of *Ln(Assets)* is 8.843 for the matched sample and is 6.254 for the pre-matching sample), which means that larger firms are more likely to experience data breaches.

[Insert Table 3 Here]

5. Empirical Results

5.1 The Baseline Results

We conduct multivariate regression analysis using the following Difference-in-Differences (DiD) model[6]:

$$\begin{aligned} Operational\ Efficiency_{i,t+1} &= \alpha_0 + \alpha_1 After\_Data\_Breach_{i,t} + \alpha_2 Operational\ Efficiency_{i,t} \\ &+ \alpha_3 Ln(Assets_{i,t}) + \alpha_4 Leverage_{i,t} + \alpha_5 ROA_{i,t} + \alpha_6 R\&D_{i,t} \\ &+ \alpha_7 IT\_Capability_{i,t} + \alpha_8 Diversity_{i,t} + \alpha_9 Institutional\ Ownership_{i,t} \\ &+ \alpha_{10} Managerial\ Ability_{i,t} + \alpha_{11} Environmental\ Complexity_{i,t} \\ &+ \alpha_{12} Environmental\ Dynamism_{i,t} + \alpha_{13} Environmental\ Munificence_{i,t} \\ &+ Firm\ Dummies + Year\ Dummies + \varepsilon_{i,t} \quad (4) \end{aligned}$$

where *Operational Efficiency*$_{i,t+1}$ represents our operational efficiency measure (*Operational Efficiency 1* and *Operational Efficiency 2*) for firm i in year t+1. The key independent variable is *After_Data_Breach*$_{i,t}$, which equals one if firm i has occurred data breach events in year t or previous years. α_1 captures the DiD effect due to data breaches. Following previous studies (Lam et al., 2016), we control the operational efficiency for firm i in year t. Other control variables are described in section 4.2 and are all measured at year t in the regressions. We include the firm fixed effects to control for the impact of unobservable time-invariant firm characteristics. Year fixed effects are also included to control for the aggregate time variation in operational efficiency.

[6] A typical DiD model in our setting should be: $Operational\ Efficiency_{i,t+1} = \alpha_0 + \alpha_1 Breach\ Firm_{i,t} + \alpha_2 Post_{i,t} + \alpha_3 Breach\ Firm_{i,t} \times Post_{i,t} + Controls + \varepsilon_{i,t}$, where *Breach Firm* is treatment variable that equals one if a firm has occurred data breaches during our sample period, and zero otherwise. *Post* is the post-treatment indicator which equals one in the post-data-breach period, and zero otherwise. *Breach Firm*×*Post* = *After_Data_Breach* by construction. When year and firm fixed effects are included, the inclusion of the *Breach Firm* and *Post* dummy variables is unnecessary. The DiD model is then reduced to Equation (4).

The baseline regression results are shown in Table 4. Columns (1) and (2) present the results for the *Operational Efficiency 1* following Battese and Coelli (1988), where column (1) is the result without control variables and column (2) is the result with control variables. Columns (3) and (4) present the results for the *Operational Efficiency 2* following Jondrow et al., (1982), where column (3) is the result without control variables and column (4) is the result with control variables. In all columns, the coefficients of *After_Data_Breach* are negative and statistically significant (*t*-statistics = -2.118, -2.227 in columns (1) and (3) without control variables, respectively, and *t*-statistics = -2.275, -2.385 in columns (2) and (4) with control variables, respectively), suggesting that compared with non-data-breach firms, data breach firms experience significantly decrease in operational efficiency after data breaches. Economically, the coefficient of *After_Data_Breach* in column (2) implies that by controlling other factors, after data breaches, on average, the breached firms would experience 6.24% (6.18%) decrease of mean (median) operational efficiency compared with the non-data-breach firms. Similarly, the coefficient of *After_Data_Breach* in column (4) implies that after data breaches, the breached firms would experience 6.93% (6.99%) decrease of mean (median) operational efficiency compared with the non-data-breach firms.

The coefficients of control variables are largely consistent with the prior studies. For instance, firms with higher operational efficiency are more likely to continue the higher operational efficiency in next year (Lam et al., 2016). Firms in a higher munificence environment are likely to have higher operational efficiency (Keats and Hitt, 1988).

[Insert Table 4 Here]

5.2 Additional Tests on Endogeneity

Despite our use of the PSM-matched sample and the DiD method in the baseline regression, the relationship between data breaches and operational efficiency may be subject to some endogeneity

issues (i.e., the occurrence of data breaches is likely endogenous). In this section, we will conduct several other analyses to further address the endogeneity issues.

5.2.1 Dynamic DiD Test

One endogeneity issue concerns reverse causality. For instance, if firms experience a decrease in operational efficiency, then managers need to invest more attention and resources into the recovery of operational efficiency, which means that less attention and resources can be devoted to security, resulting in a higher likelihood of data breaches. In our baseline results, the dependent variable is operational efficiency in the year following the data breach, meaning that the decrease in operational efficiency occured after the data breach. Thus, reverse causality concerns could be relatively mitigated.

Beyond that, we conducted dynamic DiD test to examine operational efficiency change trends in years surrounding data breach events in order to further address the issue of reverse causality. Specifically, we replaced *After_Data_Breach* in the baseline regression (equation [4]) with seven year indicators, namely, *Pre-3rd Year*, *Pre-2nd Year, Pre-1st Year, Year 0*, *Post-1st Year*, *Post-2nd Year*, and *Post-3rd year*. *Pre-jth Year* (*Post-jth Year*) equals 1 in the *pre-jth year* (*post-jth year*) relative to the year in which a data breach event occurred, and 0 otherwise. *Year 0* equals 1 in the data breach event year and 0 otherwise. The results are shown in Table 5. Columns (1) and (2) show the results for *Operational Efficiency 1* and *Operational Efficiency 2*, respectively. The coefficients of the pre-year indicators show that, prior to the data breach events, the treatment firms did not experience significant decreases in operational efficiency, compared with control firms, which further ameliorates the reverse causality concern.

In addition, the coefficients of post-year in the dynamic DiD tests are also not significant. Only the coefficients of *Year 0*, the data breach year, are significant. Based on these results, it is

clear that the effect of data breaches on operational efficiency is a short-term effect, thereby implying that managers devote more attention and resources to security and recovery issues immediately following a data breach. However, in the long term, they will not substantially compromise operational efficiency for security or recovery issues.

Furthermore, Table 5 shows that the coefficients of *Pre-3rd Year*, *Pre-2nd Year*, and *Pre-1st Year* are insignificant, thereby suggests that the parallel trends assumption is not violated.

[Insert Table 5 Here]

5.2.2 Subsample Test on Exogenous Data Breaches

Another endogeneity concern is about the omitted variables. The decrease of operational efficiency and data breach occurrences could be driven by some uncontrolled factors that could affect them simultaneously. For example, corporate governance deterioration or resources decrease could result in the decrease of operational efficiency; at the same time, information security could also be negatively affected by the governance deterioration and the resources decrease, leading to a high risk of data breaches.

To mitigate the potential endogeneity concerns, we applied the PSM combined DiD approach by merely considering the data breaches which are exogenous; we defined the data breaches which are caused by outsiders (e.g., hackers, and physical thieves) as exogenous. We aruge that such exogenous data breaches are less likely to be driven by firms' internal issues that are related with operational efficiency. Such an analysis yields consistent results. Table 6 shows that the coefficients of *After_Exogenous_Data_Breach* are significant in all columns, which implies that the negative relationship between data breaches and operational efficiency is not driven by any

internal factors capable of simultaneously decreasing operational efficiency and information security.

[Insert Table 6 Here]

5.2.3 Placebo Test

After showing that the negative relationship between data breaches and operational efficiency is not caused by reverse causality or other factors capable of simultaneously decreasing operational efficiency and information security, another possibility is that the decrease of operational efficiency is entirely driven by chance or by other latent factors in the time series. To alleviate this concern, we conducted a placebo test. Specifically, we defined a pseudo treatment *Placebo_Data_Breach*, which equals 1 in the three years prior to the actual data breach events, and then ran the DiD test again by using the pseudo treatment as the key independent variable. If the decrease in operational efficiency is not driven by chance or other latent factors in the time series, *Placebo_Data_Breach* should not affect operational efficiency in a significant way.

The empirical results are presented in Table 7; Columns (1) and (2) show the results for *Operational Efficiency 1* and *Operational Efficiency 2*, respectively. From the coefficients of the two columns, we observe that *Placebo_Data_Breach* does not significantly affect operational efficiency, which indicates that the negative relationship between data breaches and operational efficiency is unlikely to be driven by chance or other time series latent factors.

[Insert Table 7 Here]

5.3 Moderators Tests

The baseline results in terms of the main effect support our hypothesis that data breaches damage firms' operational efficiency, which is plausibly driven by the diversion of managers' attention

and the resources to firm security and recovery. Based on the attention-based view (ABV), there are three premises of decision makers' attention allocation in specific contexts: focus of attention, structural distribution of attention, and situated attention. We thus further tested our three hypotheses according to these three premises, respectively, in order to investigate the relationship between data breaches and operational efficiency under different situations—namely, risk-taking incentives, financial slack, and product market competition. In this subsection, we conduct moderator analyses to test the three hypotheses.

5.3.1 Managerial Risk-Taking Incentives

The "focus of attention" premise of ABV is proposed in an individual level, which means that decision makers' attention distraction is influenced by their own cognition. Since data breaches are in the firm's cybersecurity field, so we focus on the managers' risk-taking incentives. We argue that managers with higher risk-taking incentives would have low incentives to reduce the future risk, therefore the negative relation between data breaches and operational efficiency would be less significant for firms with higher risk-incentive managers. (H2. *Managerial risk-taking incentives weaken the negative relation between data breaches and operational efficiency*.)

Following prior studies (Core and Guay, 2002; Coles et al., 2006; Xue et al., 2017), we use CEO's vega as the proxy for managerial risk-taking incentives. Vega is measured as the change in the manager's overall option value for a 0.01 change in the annualized standard deviation of stock returns. So a higher vega implies that manager's option value would increase more when the return of the underlying stock becomes more volatile, or the market risk of the firm increases. Thus managers can gain more from firm risk. Therefore the CEO with a higher vega has higher risk-taking incentives.

To test the relation between data breaches and operational efficiency in different firms with lower managerial risk-taking incentives and higher managerial risk-taking incentives respectively, we divide the sample into two subsamples based on the ranking of CEO vega for firm i in year t relative to the firms in the same two-digit SIC industry in year t. A firm is defined as with higher (lower) managerial risk-taking incentives if its CEO vega is larger (smaller) than the industry-year median. Then we run the DiD test (Equation [4]) using the two subsamples respectively. The results are shown in Table 8. Columns (1) and (3) show the results in lower managerial risk-taking incentives firms for *Operational Efficiency 1* and *Operational Efficiency 2*, respectively. Columns (2) and (4) show the results in higher managerial risk-taking incentives firms for *Operational Efficiency 1* and *Operational Efficiency 2*, respectively. From the table we can see that the coefficients of *After_Data_Breach* are significant only in firms with lower managerial risk-taking incentives, which implies that firms with higher managerial risk-taking incentives do not distract much attention from the operational efficiency to the recovery and security problems emerged in data breaches. The results support our hypothesis that managerial risk-taking incentives weaken the negative relation between data breaches and operational efficiency.

[Insert Table 8 Here]

5.3.2 Financial Slack

The second premise of ABV is "structural distribution of attention", which is proposed in an organizational level. The "structural distribution of attention" emphasizes that decision-makers' attention allocation is dependent upon firm internal resources. Here we focus on the financial slack, which is the unabsorbed slack that is highly flexible and gives decision makers maximized freedom in its alternative allocation after breaches. We argue that financial slack can be immediately redeployed to buffer against fluctuation and ensure operation continuity even if the managers'

attention and firm resource have been distracted to solving cybersecurity and recovery problems. So *Financial slack could weaken the negative relation between data breaches and operational efficiency* (H3).

We partition the sample according to the ranking of financial constraints variables value for firm i in year t relative to the firms in the same two-digit SIC industry in year t. We use two financial constraints variables: Whited and Wu's (2006) financial constraints index (the *WW index*[7]) and the Altman's (1968) Z-score (*Z-score*[8]). The lower (higher) the WW index (Z-score), the higher financial slack of a firm. So a firm is defined as higher financial slack if its WW index (Z-score) is smaller (higher) than the industry-year median. Then we run the DiD test (Equation [4]) using the two subsamples respectively. The results are shown in Table 9. Panel A shows the results based on the *WW index* and Panel B shows the results based on *Z-score*. In both panels, columns (1) and (3) show the results in lower financial slack firms for *Operational Efficiency 1* and *Operational Efficiency 2*, respectively. Columns (2) and (4) show the results in higher financial slack firms for *Operational Efficiency 1* and *Operational Efficiency 2*, respectively. From the table we can see that the coefficients of *After_Data_Breach* are significant only in firms with lower financial slack (columns (1) and (3)), which implies that firms with higher financial slack could easily deploy their financial slack to ensure efficient operations although the managers' attention and firm resource have been distracted to solving cybersecurity and recovery problems. So the firms with larger financial slack would not experience significant decrease in operational efficiency after the occurrences of data breach, which supports H3.

[7] The WW index is equal to $-0.091\times$*Cash flow/Assets*$-0.062\times$*Dividend payer indicator*$+0.021\times$*Long-term debt/Assets*$-0.044\times$*Ln(Assets)*$+0.102\times$*Industry median sales growth*$-0.035\times$*Sales growth*. By construction, lower scores of the WW index indicate that firms have more financial slack.

[8] Altman's (1968) Z-score is defined as *(3.3×Pretax income+Sales+1.4×Retained earnings+1.2×[Current assets - Current liabilities])/Assets*. By construction, higher scores of the Z-score indicate that firms have more financial slack.

[Insert Table 9 Here]

5.3.3 Product Market Competition

The third premise of ABV, "situated attention", is proposed at a social level and highlights that external environmental context shapes the extent to which any given stimulus will receive attention and action. We use the product market competition to measure firm's external environmental context. We argue that firms in a highly product market competition environment would put the economic profit and operational efficiency in the first priority. Thus, for breached firms situated in the highly competition environment, they tend to unable to afford a high level of attention flow into cybersecurity and recovery with sacrificing their operational efficiency too much, thereby weakening the attention-distraction channel and the breach-efficiency relation. So we put forward H4: *Product market competition weakens the negative relation between data breaches and operational efficiency*.

To measure the product market competition, we first use the Herfindahl index (*HHI*), which is the sum of squared market shares in sales of a firm's three-digit SIC industry. A higher HHI indicates a lower product market competition level. Besides, following Hoberg and Phillips (2010, 2016), we also use the product similarities (*TNIC3TSIMM*) to proxy the product market competition. We get the TNIC3TSIMM data from the Hoberg−Phillips TNIC data set provided by Hoberg and Phillips (2010, 2016). Hoberg and Phillips (2016) constructed TNIC3TSIMM on the bases of web crawling and text parsing algorithms through processing the text in the business descriptions of 10-K annual filings. Hoberg and Phillips analyzed each firm's 10-K product descriptions and calculated the firm-by-firm pairwise similarity scores using the cosine similarity method. Each firm's own specific set of nearby competitors was identified as firm pairs with textual similarity of their product descriptions that exceeds a threshold. By doing so, each firm was

assigned a unique spatial location. Thereafter, each firm-year's TNIC3TSIMM value is the total sum of the product similarities of a firm with other competitors within its industry. The high TNIC3TSIMM values of firms indicate their low level of product differentiation and the fierce product market competition that they face (Hoberg and Phillips 2010, 2016).

Table 10 shows the results of data breaches and operational efficiency in different product market competition levels. Panel A is the results based on *HHI*. We partition the sample based on the median value of HHI in each year. Firm i in year t is defined as high (low) product market competition firm if its HHI is below (above) the median HHI value in year t. Panel B is the results based on TNIC3TSIMM. A firm is defined as high (low) product market competition firm if its TNIC3TSIMM is higher (lower) than the two-digit industry-year median. In both panels, columns (1) and (3) show the results in low product market competition firms for *Operational Efficiency 1* and *Operational Efficiency 2*, respectively. Columns (2) and (4) show the results in high product market competition firms for *Operational Efficiency 1* and *Operational Efficiency 2*, respectively. From the table we can see that the coefficients of *After_Data_Breach* are significant only in firms in low product market competition environment (columns (1) and (3)), which implies that firms in highly product market competition environment are less likely to distract much attention from operational efficiency to recovery and cybersecurity problems after the occurrences of data breaches. So the product market competition weakens the negative relation between data breaches and operational efficiency, supporting our H4.

[Insert Table 10 Here]

6. Discussion

This paper adopts a markedly rigorous research design to establish causalities. All the tests used PSM combined with DiD, in which PSM constructs a matched group and DiD provides a quasi-experimental setting. Firm- and year-fixed effects are included in all tests to further account for any unobserved heterogeneity or systematic differences across years. In addition, two different measures of operational efficiency are adopted in each test to further ensure robustness. The results of all the tests are discussed as follows.

6.1 Discussion of the Main Effects

The results presented in Table 4 show that the combined PSM-DiD estimate is statistically significant ($p < 0.05$) in terms of both operational efficiency measures, thereby supporting our hypothesis that firms' data breaches reduce their operational efficiency. To further ensure the robustness of this relationship, several tests are adopted to mitigate potential concerns. First, to mitigate endogeneity concerns [i.e., (1) reverse causality and (2) omitted variables], this paper performed a dynamic DiD test (see Table 5) and a subsample test on exogenous breach (see Table 6); the former mitigated the reverse causality concern and the latter prevented unobservable firm heterogeneity from driving our results. The results of both tests are consistent with the baseline results, thereby mitigating heterogeneity concerns for our findings. In particular, the dynamic DiD test also enabled us to evaluate the dynamics of the breach-efficiency relationship, generating the intriguing and important finding that the impact of data breaches on efficiency is significant in the short term but is substantially diminished in the long term.

Second, to allay concerns about spurious correlation in our estimates, this paper conducted a placebo test (see Table 7) to scrutinize the potential impact of "fake" breaches. By examining

changes in firms' efficiency in response to the placebo breach ("fake" treatment), we determined that the coefficient for the "fake" breach is insignificant. Thus, this paper found no evidence indicating that the results on the main effect are driven by the underlying trends of operational efficiency or by certain events other than data breaches.

6.2 Discussion of the Moderating Effects

To further understand the breach-efficiency relations and make it more transparent, we focused on three moderators based on Ocasio's (1997) ABV framework: risk-taking incentives, resource slack, and market competition. These three moderators are proposed along the individual-, organizational-, and social-level premises, respectively, of ABV, and accordingly, we proposed H2, H3, and H4. The baseline analysis (see Tables 8, 9, and 10) provides evidence supporting each hypothesis. That is, the results show that data breaches have pronounced effects on operational efficiency if managers are risk averse, if firms have insufficient financial resource stocks, or if firms are located in an idle market. To further alleviate the concern that these results may be an artifact of our adopted measure, we used alternative measures of the moderators and found consistent results.

In summary, the ABV effectively predicts all focused relationships, each of which is also empirically supported by our longitudinal analyses. Before discussing the implications of our findings, we acknowledge the research limitations that provide beneficial avenues for extension.

6.3 Limitations and Future Research

Like other empirical studies, our results have limitations, which, however, offer fruitful avenues for future research. First, this paper encountered data constraints in relation to data breaches. Although we used two authoritative data breach sources (i.e., PRC and ITRC) to collect breach

data in this study, our sample only includes reported breaches; unfortunately, relying on reported breaches as the source for measuring data breach risk appears to be our only option. Despite such a limitation, we have endeavored to ensure comprehensive cover of the reported breaches in our sample. Different from the prior empirical data breach research (e.g., Huang and Wang, 2021; Kamiya et al., 2020; Sen and Borle, 2015), which has primarily adopted the single data breach source of PRC, our study is among the first to manually integrate data breach information from both PRC and ITRC, thereby offering a substantially more robust representation of data breaches. The implication is that future data breach research may consider using a similar approach to further collect US listed firms' data breach information in a comprehensive manner. Furthermore, because our breach data are limited to US firms, our findings should be US-specific but the impact of breaches may also vary across cultures. Thus, future studies may consider investigating cross-cultural impacts of data breaches.

Second, this study is grounded on ABV and proposes the attention-distraction channel as the potential driver of the breach-efficiency relation. However, we did not empirically qualify the availability of this channel, and a thorough examination of this mechanism is beyond the scope of this study. Thus, future research might consider testing these models using a direct measure of the degree of attention distraction. An additional intriguing research direction would be to determine whether the attention-distraction channel or a security-efficiency tradeoff exerts any spillover effect. For example, future research could explore whether data breach events impact the operational efficiency of a firm's competitors.

Besides, this paper conducts moderation analysis based on the three premises of ABV. However, this paper encountered data constraints in relation to moderators. For example, at the individual-level, it would be more realistic to use Chief Technology Officer (CTO) related

measures (e.g., CTO's risk incentives, CTO-CEO reporting structure) as moderators since CTO is the direct decision maker in the information security domain. At the social-level, in addition to product market competition, there are many other factors (e.g., state-level environment) that can influence the attention-distraction channel. However, we do not have access to these kinds of data currently. Then future research could consider testing the three premises using direct measures. What's more, current results show that managerial risk-taking incentive and product market competition would weaken the negative effect of data breaches on operational efficiency, which are interesting. Future research could consider extending the research about the effect of managerial incentives and product market competition on the operational implications of data breaches.

7. Implications and Conclusions

The current study posits the following research questions:

(1) How do firms' data breaches impact their operational efficiency?

(2) How do managerial risk-taking incentives, financial slack, and product market competition individually moderate the relation between data breaches and operational efficiency?

We devote substantial theoretical and empirical effort to answering these questions. In theoretical terms, we synthesize arguments from both the security and ABV literatures and develop a conceptual framework to predict the relations among data breaches, firm context, and operational efficiency. In empirical terms, we use secondary data in a longitudinal setting as a basis to conduct a rigorous and comprehensive list of tests to establish causality. Accordingly, we achieve empirical results that are entirely consistent with our predictions. Our findings yield substantial theoretical and practical implications, which are discussed as follows.

7.1 Theoretical Implications

This research has several theoretical implications, some of which facilitate the advancement of prior literature and some challenge conventional wisdom. First, although management scholars and economists have frequently speculated on the consequences of data breaches, we note that the scope of the literature is markedly constrained and incommensurate with the profound impact of data breaches. This lack of attention is alarming because the absence of a clear understanding of data breaches' impact may lead to subsequent unwise strategies. This study may help fill in this research gap by quantifying the subsequent drain on firm operational efficiency following data breaches, thereby extending the existing literature and offering new insights. In particular, this study also respones to Massimino et al.'s (2018, p. 1493) research call to that "we envision a vibrant research stream that considers the trade-offs between confidentiality and other operational performance dimensions."

Second, although the behavioral security research has gleaned insight from a variety of theoretical lenses, such as agency theory (Herath and Rao, 2009a), protection motivation (Boss et al., 2015; Johnston et al., 2015; Posey et al., 2015; Posey et al., 2013), deterrence (D'Arcy et al., 2009), neutralization (Siponen and Vance, 2010), rational choice (Bulgurcu et al., 2010; Vance and Siponen, 2012), and accountability (Vance et al., 2013), to discuss the individual-level determinants of data breaches, we note that the theories employed in the discourse on the consequences of data breaches are quite limited. This study may help bridge this research gap by taking the initial step of introducing ABV into the information security literature.

Third, by invoking the three premises of ABV, this paper provides an additional fine-grained attack on the contexts that may intervene in the breach-efficiency relation. The related analysis offers a potential "missing link" by applying ABV to information security, and also determines

the plausibility of the fundamental mechanism that connects data breaches to operational efficiency. In addition, the findings that managerial risk-taking incentives, resource slack, and market competition intervene in the relation between data breaches and operational efficiency provide a useful complement to the existing ABV and information security literatures.

Fourth, an interesting and possibly surprising note is that market competition tends to weaken the negative impact of breaches on efficiency. Intuitively, this finding appears to challenge the conventional wisdom that operations in firms with high competitive pressure would be sensitive to negative events. However, this finding, if seen from an ABV perspective, makes sense. That is, in a context of fierce market competition, the pressure imposed by rivals and the constant threat of customer loss tend to highly hinder firms' attention distraction after data breaches, thereby weakening the proposed channel connecting data breaches to efficiency. Such an interpretation of the finding further supports our theory, which is ABV-based.

7.2 Practical Implications

Several meaningful practical implications can also be drawn from this study. First, the findings provide a cautionary tale for firms regarding their strategy designs in the wake of data breaches. That is, firms should particularly focus on the "ripple" effect that their enacted strategies may have on operational efficiency following a data breach. This study also reminds breached firms to seriously consider balancing security and efficiency issues in making their recovery and additional investments. In addition, firms should acknowledge the fact that their data breaches will truly hinder their operational efficiency, and integrate such a knowledge into their data breach prevention strategies.

Second, the findings suggest that the negative impact of breaches on efficiency depends on context. For example, the stock of sufficient resource slack, particularly the unabsorbed one, can

help mitigate the negative impacts of data breach. Our results indicate that top managers' risk orientation also plays a moderating role, thereby providing beneficial knowledge to shareholders and investors to comprehensively evaluate the potential consequences of data breaches for their firms. In addition, our findings may serve to remind risk-averse managers that their firms are highly vulnerable to diminished efficiency after experiencing data breaches.

Finally, based on the striking finding that the negative breach-efficiency relation is significant in the short-term only, we encourage firm managers to specifically and promptly focus their attention on restoring and increasing operational efficiency following data breaches.

7.3 Conclusions

The attention-based perspective of this study offers a powerful and rich lens through which the breach-efficiency relation and its boundary conditions can be better understood and predicted. To establish causality, this paper used an extensive longitudinal data set and adopted a combined PSM-DiD approach. The results indicate a negative breach-efficiency relation, particularly in certain conditions involving risk-averse managers, firms that lack excess resources, or firms that are located in idle markets. This study also provides a battery of tests to ensure the robustness of these findings. For academics, this study clarifies the breach-efficiency relation and reinforces the importance of theorizing in the analysis. For practicing professionals, the results warn of the substantial potential negative impact of data breaches on firms' operational efficiency, particularly in the short term.

Appendix A. Distribution of data breach firms over time and across industries

The sample consists of non-financial firms that report data breaches in the Privacy Rights Clearinghouse (PRC) and Identity Theft Resource Center (ITRC) between 2006 and 2016 without missing variables. Panel A reports the distribution of data breach firms by the first data breach occurrence year. Panel B reports the distribution of data breach firms by one-digit SIC industry.

Panel A: Distribution of data breach firms by first breach year

First breach year	Number of data breach firms	Percentage in all data breach firms
2006	19	12.10%
2007	22	14.01%
2008	17	10.83%
2009	6	3.82%
2010	21	13.38%
2011	8	5.10%
2012	14	8.92%
2013	14	8.92%
2014	18	11.46%
2015	12	7.64%
2016	6	3.82%
Total	157	100%

Panel B: Distribution of data breach firms by one-digit SIC industry

SIC code	Included industries	Number of data breach firms	Percentage in all data breach firms
0	Agricultural production & services; forestry; fishing, hunting and trapping	1	0.64%
1	Mining and construction	4	2.55%
2	Food, tobacco, textile mill, apparel, and lumber and wood products; furniture and fixtures; paper, printing, publishing, and chemical products; petroleum refining, etc.	26	16.56%
3	Rubber and plastic products; leather, stone, clay, glass, concrete, and metal products; machinery, electronic and electrical equipment; transportation equipment, measuring, analyzing, and controlling instruments, etc.	42	25.75%
4	Transportation, communications, electric, gas, and sanitary services	12	7.64%
5	Retail and wholesale trade	37	23.57%
7	Hotels, personal and business services; automotive repair services; motion pictures, amusement and recreation services, etc.	27	17.20%
8	Health, legal, educational, and social services; museums, art galleries, botanical and zoological gardens; membership organizations; engineering, accounting, research, and management services; private households, etc.	6	3.82%
9	Utilities	2	1.27%

Appendix B. Distribution of data breach events over time and across industries

The sample consists of data breach events reported by non-financial firms in the Privacy Rights Clearinghouse (PRC) and Identity Theft Resource Center (ITRC) between 2006 and 2016 without missing variables. Panel A reports the distribution of data breach events by year. Panel B reports the distribution of data breach events by one-digit SIC industry.

Panel A: Distribution of data breach events by year

Year	Number of data breach events	Percentage in all data breach events
2006	19	6.7%
2007	26	9.1%
2008	26	9.1%
2009	15	5.3%
2010	36	12.6%
2011	24	8.4%
2012	29	10.2%
2013	32	11.2%
2014	36	12.6%
2015	25	9.8%
2016	17	6.0%
Total	285	100%

Panel B: Distribution of data breach events by one-digit SIC industry

SIC code	Included industries	Number of data breach events	Percentage in all data breach events
0	Agricultural production & services; forestry; fishing, hunting and trapping	1	0.4%
1	Mining and construction	4	1.4%
2	Food, tobacco, textile mill, apparel, and lumber and wood products; furniture and fixtures; paper, printing, publishing, and chemical products; petroleum refining, etc.	39	13.7%
3	Rubber and plastic products; leather, stone, clay, glass, concrete, and metal products; machinery, electronic and electrical equipment; transportation equipment, measuring, analyzing, and controlling instruments, etc.	67	23.5%
4	Transportation, communications, electric, gas, and sanitary services	33	11.6%
5	Retail and wholesale trade	78	27.4%
7	Hotels, personal and business services; automotive repair services; motion pictures, amusement and recreation services, etc.	47	16.5%
8	Health, legal, educational, and social services; museums, art galleries, botanical and zoological gardens; membership organizations; engineering, accounting, research, and management services; private households, etc.	11	3.9%
9	Utilities	5	1.8%

Appendix C. Variable descriptions

Variable	Description	Data Source
Operational Efficiency 1	An estimation of h_{ijt} based on the panel data structure model with half-normal distribution. A high h_{ijt} estimation suggests a low operational efficiency, following Battese and Coelli (1988).	COMPUSTAT
Operational Efficiency 2	An estimation of h_{ijt} based on the cross-sectional model in which firm effects have half-normal distribution. A high h_{ijt} estimation suggests a low operational efficiency, following Jondrow et al. (1982).	COMPUSTAT
After_Data_Breach	An indicator equals 1 if the observation is in the year of or after a data breach and 0 if the observation is in years before the data breach.	PRC, ITRC
Managerial Risk-Taking Incentive	The change in the CEO's overall option value for a 0.01 change in the annualized standard deviation of stock returns, as in Core and Guay (2002), Coles et al. (2006), and Xue et al. (2017).	Execucomp
Financial Slack	The financial constraints index of the *WW index.* The lower the WW index, the higher financial slack of a firm, following Whited and Wu (2006).	COMPUSTAT
*Financial Slack (*An alternative measure*)*	The financial constraints index of the *Z-score.* The higher the *Z-score*, the higher financial slack of a firm, following Altman (1968).	COMPUSTAT
Product Market Competition	Total sum of product similarity of a firm with its special set of peers in the same industry, following Kim et al. (2016) and Li and Zhan (2018).	Hoberg-Phillips TNIC data
*Product Market Competition (*An alternative measure*)*	The Herfindahl index (*HHI*), which is the sum of squared market shares in sales of a firm's three-digit SIC industry, following Gaspar and Massa (2006) and Gu (2016).	COMPUSTAT
Ln(Assets)	The natural logarithm of total assets.	COMPUSTAT
Leverage	The ratio of the total liabilities to the total assets of a firm.	COMPUSTAT
ROA	The ratio of operating income before depreciation to total assets.	COMPUSTAT
R&D	The natural logarithm of the R&D expenses.	COMPUSTAT
IT Capability	An indicator variable equals 1 if the observation is included on the annual IW500 list, as in Bharadwaj et al. (1999).	IW 500
Business Scope	The natural logarithm of the number of business segments reported, as in Hendricks et al. (2009).	COMPUSTAT
Institutional Ownership	The ratio of shares hold by institutional investors to a firm's total outstanding shares in percentage .	COMPUSTAT
Managerial Ability	Managerial ability score of a firm in the fiscal year from Demerjian (2012). The score was computed using the DEA method, where total sales are optimized using a comprehensive vector of inputs.[9]	Peter Demerjian data

[9] 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.

Appendix C. [Continued] Variable descriptions

Environmental complexity	The concentration ratios for the top four firms in an industry then multiples minus 1, as in Keats and Hitt (1988).	COMPUSTAT
Environmental dynamism	Regressing an observation's industry sales on a five-year period, 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 munificence	The slope coefficient of the regression equation for calculating the environmental dynamism of the observation divided by the average sales of the industry, as in Keats and Hitt (1988).	COMPUSTAT
After_Exogenous_Breach	An indicator equals to 1 if the observation is the year in or after a data breach that was caused by outsiders (e.g., hackers, and physical thieves), and 0 if the observation is 1 year before the data breach.	PRC, ITRC

References

Akey, P., Lewellen, S., & Liskovich, I. (2018). Hacking corporate reputations. *Rotman School of Management Working Paper*, (3143740).

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

Andoh-Baidoo, F. K., & Osei-Bryson, K. M. (2007). Exploring the characteristics of Internet security breaches that impact the market value of breached firms. *Expert Systems with Applications*, *32*(3), 703-725.

Azadegan, A., Patel, P. C., & Parida, V. (2013). Operational slack and venture survival. *Production and Operations Management*, *22*(1), 1-18.

Balabanis, G., Phillips, H. C., & Lyall, J. (1998). Corporate social responsibility and economic performance in the top British companies: are they linked?. *European Business Review*, 98(1), 25-44.

Barnett, M. L. (2008). An attention-based view of real options reasoning. *Academy of Management Review*, *33*(3), 606-628.

Battese, G. E., & Coelli, T. J. (1988). Prediction of firm-level technical efficiencies with a generalized frontier production function and panel data. *Journal of Econometrics*, *38*(3), 387-399.

Benaroch, M., & Chernobai, A. (2017). Operational IT failures, IT value-destruction, and board-level IT governance changes. *MIS Quarterly*, *41*(3), 729-762.

Bennett, V. M., Pierce, L., Snyder, J. A., & Toffel, M. W. (2013). Customer-driven misconduct: How competition corrupts business practices. *Management Science*, *59*(8), 1725-1742.

Bharadwaj, A. S. (2000). A resource-based perspective on information technology capability and firm performance: an empirical investigation. *MIS Quarterly*, 24(1), 169-196.

Bharadwaj, A., Keil, M., & Mähring, M. (2009). Effects of information technology failures on the market value of firms. *The Journal of Strategic Information Systems*, *18*(2), 66-79.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & 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*, 39(4), 837-864.

Bourgeois III, L. J. (1981). On the measurement of organizational slack. *Academy of Management Review*, *6*(1), 29-39.

Brown, H. S. (2016). After the data breach: Managing the crisis and mitigating the impact. *Journal of Business Continuity & Emergency Planning*, *9*(4), 317-328.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3), 523-548.

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

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), 70-104.

Chen, Y., Ramamurthy, K., & Wen, K. W. (2012). Organizations' information security policy compliance: Stick or carrot approach?. *Journal of Management Information Systems*, 29(3), 157-188.

Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *7*(5), e1211.

Cheng, Q., Goh, B. W., & Kim, J. B. (2018). Internal control and operational efficiency. *Contemporary Accounting Research*, *35*(2), 1102-1139.

Cohen, M. D., March, J. G., & Olsen, J. P. (1972). A garbage can model of organizational choice. *Administrative Science Quarterly*, 1-25.

Coles, J. L., Daniel, N. D., & Naveen, L. (2006). Managerial incentives and risk-taking. *Journal of Financial Economics*, *79*(2), 431-468.

Colwill, C. (2009). Human factors in information security: The insider threat–Who can you trust these days?. *Information Security Technical Report*, *14*(4), 186-196.

Connelly, B. L., Shi, W., Walker, H. J., & Hersel, M. C. (2020). Searching for a sign: CEO successor selection in the wake of corporate misconduct. *Journal of Management*, 0149206320924119.

Core, J., & Guay, W. (2002). Estimating the value of employee stock option portfolios and their sensitivities to price and volatility. *Journal of Accounting Research*, *40*(3), 613-630.

Cyert, R.M., & March, J. G. (1963). *A Behavioral Theory of the Firm*. Englewood Cliffs, NJ.

D'Arcy, J., & 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), 103151.

D'Arcy, J., Adjerid, I., Angst, C. M., & Glavas, A. (2020). Too Good to Be True: Firm Social Performance and the Risk of Data Breach. *Information Systems Research*, *31*(4), 1200-1223.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, *31*(2), 285-318.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1), 79-98.

Demerjian, P., Lev, B., & McVay, S. (2012). Quantifying managerial ability: A new measure and validity tests. *Management science*, *58*(7), 1229-1248.

Dey, D., Lahiri, A., & Zhang, G. (2014). Quality competition and market segmentation in the security software market. *MIS Quarterly*, *38*(2), 589-A7.

Fama, E. F., & French, K. R. (1992). The cross-section of expected stock returns. *The Journal of Finance*, 47(2), 427-465.

Fiske, S. T., & Taylor, S. E. (2013). *Social cognition: From brains to culture*. Sage.

Fowler, K. (2016). *Data breach preparation and response: Breaches are certain, impact is not*. Syngress.

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security*, *11*(2), 74-83.

Giroud, X., & Mueller, H. M. (2011). Corporate governance, product market competition, and equity prices. *The Journal of Finance*, 66(2), 563-600.

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

Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). User compensation as a data breach recovery action: An investigation of the Sony PlayStation network breach. *MIS Quarterly*, *41*(3), 703-727.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs?. *Journal of Computer Security*, *19*(1), 33-56.

Gremler, D. D., & Brown, S. W. (1996). Service loyalty: its nature, importance, and implications. *Advancing service quality: A global perspective*, *5*(1), 171-181.

Gwebu, K. L., Wang, J., & Wang, L. (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems*, *35*(2), 683-714.

Hendricks, K. B., Singhal, V. R., & Zhang, R. (2009). The effect of operational slack, diversification, and vertical relatedness on the stock market reaction to supply chain disruptions. *Journal of Operations Management*, *27*(3), 233-246.

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165.

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 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), 79-98.

Hitt, M. A., Xu, K., & Carnes, C. M. (2016). Resource based theory in operations management research. *Journal of Operations Management*, *100*(*41)*, 77-94.

Hoberg, G., & Phillips, G. (2010). Product market synergies and competition in mergers and acquisitions: A text-based analysis. *The Review of Financial Studies*, *23*(10), 3773-3811.

Hoberg, G., & Phillips, G. (2016). Text-based network industries and endogenous product differentiation. *Journal of Political Economy*, *124*(5), 1423-1465.

Hoberg, G., Phillips, G., & Prabhala, N. (2014). Product market threats, payouts, and financial flexibility. *The Journal of Finance*, 69(1), 293-324.

Ho-Jin, P., & 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), 66-75.

Holt, C. A., & Laury, S. K. (2002). Risk aversion and incentive effects. *American Economic Review*, 92(5), 1644-1655.

Hovav, A., & D'Arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review*, *6*(2), 97-121.

Hovav, A., & D'Arcy, J. (2004). The Impact of Virus Attack Announcements on the Market Value of Firms. *Information Systems Security*, *13*(3), 32-40.

Huang, H. H., & Wang, C. (2021). Do Banks Price Firms' Data Breaches?. *The Accounting Review*, 96(3), 261-286.

Hwang, I., & Cha, O. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior*, *81*, 282-293.

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing*, *82*(2), 85-105.

Jenkins, J. L., Anderson, B. B., Vance, A., Kirwan, C. B., & Eargle, D. (2016). More harm than good? How messages that interrupt can make us vulnerable. *Information Systems Research*, 27(4), 880-896.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3), 549-566.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An Enhanced Fear Appeal Rhetorical Framework. *MIS Quarterly*, 39(1), 113-134.

Jondrow, J., Lovell, C. K., Materov, I. S., & Schmidt, P. (1982). On the estimation of technical inefficiency in the stochastic frontier production function model. *Journal of Econometrics*, *19*(2-3), 233-238.

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2020). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719-749.

Karuna, C. (2007). Industry product market competition and managerial incentives. *Journal of Accounting and Economics*, 43(2-3), 275-297.

Karunaratna, A. C., & Kumara, P. A. P. (2018). Determinants of customer loyalty: A literature review. *Journal of Customer Behaviour*, *17*(1-2), 49-73.

Kayworth, T, & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly Executive*, 9(3), 2012-52.

Keats, B. W., & Hitt, M. A. (1988). A causal model of linkages among environmental dimensions, macro organizational characteristics, and performance. *Academy of Management Journal*, *31*(3), 570-598.

Kiesler, S., & Sproull, L. (1982). Managerial response to changing environments: Perspectives on problem sensing from social cognition. *Administrative Science Quarterly*, *27*(4), 548-570.

Kim, H., Kim, H., & Lee, P. M. (2008). Ownership structure and the relationship between financial slack and R&D investments: Evidence from Korean firms. *Organization Science, 19*(3), 404-418.

Kim, K., Gopal, A., & Hoberg, G. (2016). Does product market competition drive CVC investment? Evidence from the US IT industry. *Information Systems Research*, *27*(2), 259-281.

Kortmann, S., Gelhard, C., Zimmermann, C., & Piller, F. T. (2014). Linking strategic flexibility and operational efficiency: The mediating role of ambidextrous operational capabilities. *Journal of Operations Management*, *32*(7-8), 475-490.

Kusunoki, K., Nonaka, I., & Nagata, A. (1998). Organizational capabilities in product development of Japanese firms: a conceptual framework and empirical findings. *Organization Science*, 9(6), 699-718.

Kwon, J., & Johnson, M. E. (2015, June). The market effect of healthcare security: Do patients care about data breaches?. In *WEIS*.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2020). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *arXiv preprint arXiv:2006.11929*.

Lam, H. K., Yeung, A. C., & Cheng, T. E. (2016). The impact of firms' social media initiatives on operational efficiency and innovativeness. *Journal of Operations Management*, *47*, 28-43.

Latham, S. F., & Braun, M. R. (2008). The performance implications of financial slack during economic recession and recovery: observations from the software industry (2001-2003). *Journal of Managerial Issues*, 30-50.

Lazonick, W, & O'sullivan, M. (2000). Maximizing shareholder value: a new ideology for corporate governance. *Economy and Society*, 29(1), 13-35.

Lending, C., Minnick, K., & Schorno, P. J. (2018). Corporate governance, social responsibility, and data breaches. *Financial Review*, *53*(2), 413-455.

Li, S., & Zhan, X. (2019). Product market threats and stock crash risk. *Management Science*, *65*(9), 4011-4031.

Li, S., Shang, J. & Slaughter, S. A. (2010). Why do software firms fail? Capabilities, competitive actions, and firm survival in the software industry from 1995 to 2007. *Information Systems Research*, *21*(3), 631-654.

Lungeanu, R., Stern, I., & Zajac, E. J. (2016). When do firms change technology‐sourcing vehicles? The role of poor innovative performance and financial slack. *Strategic Management Journal*, *37*(5), 855-869.

Malhotra, A., & Kubowicz Malhotra, C. (2011). Evaluating customer information breaches as service failures: An event study approach. *Journal of Service Research*, *14*(1), 44-59.

March, J. G., & Herbert, A. (1958). Simon1958 Organizations. *New York: WileyMarchOrganizations1958*.

March, J. G., Olsen, J. P., & Christensen, S. (1976). *Ambiguity and choice in organizations*. Universitetsforlaget.

Massimino, B., Gray, J. V., & Lan, Y. (2018). On the inattention to digital confidentiality in operations and supply chain research. *Production and Operations Management*, 27(8), 1492-1515.

Masuch, K., Greve, M., Cyrenius, J., Wimmel, B., & Trang, S. (2020). Do I Get What I Expect? An Experimental Investigation of Different Data Breach Recovery Actions. In *ECIS*.

McCann, B. T., & Bahl, M. (2017). The influence of competition from informal firms on new product development. *Strategic Management Journal*, 38(7), 1518-1535.

McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, 108, 57-68.

Modi, S. B., & Mishra, S. (2011). What drives financial performance–resource efficiency or resource slack?: Evidence from US based manufacturing firms from 1991 to 2006. *Journal of Operations Management*, *29*(3), 254-273.

Nohria, N., & Gulati, R. (1996). Is slack good or bad for innovation?. *Academy of Management Journal*, *39*(5), 1245-1264.

Nordlund J. (2019). The Role of Experience in the Director Labor Market: Evidence from Cybersecurity Events. *Louisiana State University Working paper*.

Ocasio, W. (1997). Towards an attention-based view of the firm. *Strategic Management Journal*, *18*(S1), 187-206.

Ocasio, W. (2011). Attention to attention. *Organization Science*, *22*(5), 1286-1296.

Ocasio, W., Laamanen, T., & Vaara, E. (2018). Communication and attention dynamics: An attention-based view of strategic change. *Strategic Management Journal*, *39*(1), 155-167.

Parmigiani, A., Klassen, R. D., & Russo, M. V. (2011). Efficiency meets accountability: Performance implications of supply chain configuration, control, and capabilities. *Journal of Operations Management*, *29*(3), 212-223.

Peng, D. X., Schroeder, R. G., & Shah, R. (2008). Linking routines to operations capabilities: A new perspective. *Journal of Operations Management*, 26(6), 730-748.

Pienta, D., Thatcher, J., Sun, H., & George, J. (2018). Information systems betrayal: When cybersecurity systems shift from agents of protection to agents of harm.

Png, I. P., Wang, C. Y., & Wang, Q. H. (2008). The deterrent and displacement effects of information security enforcement: International evidence. *Journal of Management Information Systems*, *25*(2), 125-144.

Posey, C., Bennett, R. J., & Roberts, T. L. (2011). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers & Security*, 30(6-7), 486-497.

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, 32(4), 179-214.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & 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*, 37(4), 1189-1210.

Post, G. V., & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security*, *26*(3), 229-237.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, 34(4), 757-778.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, 757-778.

Ross, S. A. (2004). Compensation, incentives, and the duality of risk aversion and riskiness. *The Journal of Finance*, *59*(1), 207-225.

Schmidt, K. M. (1997). Managerial incentives and product market competition. *The Review of Economic Studies*, 64(2), 191-213.

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, *32*(2), 314-341.

Simon H. A. (1947). *Administrative Behavior: A Study of Decision-Making Processes in Administrative Organizations*. Mac Millan: Chicago.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 34(3), 487-502.

Song, L. Z., Song, M., & Di Benedetto, C. A. (2011). Resources, supplier investment, product launch advantages, and first product performance. *Journal of Operations Management*, *29*(1-2), 86-104.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, 34(3), 503-522.

Sullivan, B. N. (2010). Competition and beyond: Problems and attention allocation in the organizational rulemaking process. *Organization Science*, *21*(2), 432-450.

Syed, R. (2019). Enterprise reputation threats on social media: A case of data breach framing. *The Journal of Strategic Information Systems*, *28*(3), 257-274.

Telang, R., & Wattal, S. (2007). An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Transactions on Software engineering*, *33*(8), 544-557.

Vanacker, T., Collewaert, V., & Zahra, S. A. (2017). Slack resources, firm performance, and the institutional context: evidence from privately held European firms. *Strategic Management Journal*, *38*(6), 1305-1326.

Vance, A., & Siponen, M. T. (2012). IS security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing (JOEUC)*, 24(1), 21-41.

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*, 29(4), 263-290.

Voss, G. B., Sirdeshmukh, D., & Voss, Z. G. (2008). The effects of slack resources and environmentalthreat on product exploration and exploitation. *Academy of Management journal*, *51*(1), 147-164.

Wang, J., Gupta, M., & Rao, H. R. (2015). Insider Threats in a Financial Institution. *MIS Quarterly*, 39(1), 91-112.

Weick, K. E. (2015). The social psychology of organizing. *M@n@gement*, *18*(2), 189.

Whited, T. M., & Wu, G. (2006). Financial constraints risk. *The Review of Financial Studies*, *19*(2), 531-559.

Whitler, K. A., & 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), 3-9.

Wiengarten, F., Fan, D., Lo, C. K., & Pagell, M. (2017). The differing impacts of operational and financial slack on occupational safety in varying market conditions. *Journal of operations Management*, *52*, 30-45.

Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity risks in a pandemic. *Journal of Medical Internet Research*, *22*(9), e23692.

Wood, L. C., Wang, J. X., Olesen, K., & Reiners, T. (2017). The effect of slack, diversification, and time to recall on stock market reaction to toy recalls. *International Journal of Production Economics*, *193*, 244-258.

Wu, S. J., Melnyk, S. A., & Flynn, B. B. (2010). Operational capabilities: The secret ingredient. *Decision Sciences*, *41*(4), 721-754.

Xue, L., Ray, G., & Zhao, X. (2017). Managerial incentives and IT strategic posture. *Information Systems Research*, *28*(1), 180-198.

Yayla, A. A., & Hu, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology*, *26*(1), 60-77.

Yiu, L. D., Lam, H. K., Yeung, A. C., & Cheng, T. C. E. (2020). Enhancing the Financial Returns of R&D Investments through Operations Management. *Production and Operations Management*, 29(7), 1658-1678.

Table 1. The results of Propensity Score Matching (PSM)

The sample includes our data breach firms and all non-data breach firms that are in Compustat during the period 2006 –2016 and have non-missing values for the variables used in the model. Panel A reports the coefficient estimates obtained from estimating a logit model predicting the probability of data breach occurrences. The dependent variable, *Data_Breach*, equals one in the year of data breach events. It equals zero for all non-data breach firms. Observations for data breach firms in years without data breach occurrences are excluded from the analysis. *Ln(Assets)* is the natural logarithm of a firm's total assets; *Leverage* equals a firm's total liability divided by total assets; *ROA* represents a firm's net income divided by total assets; *R&D* is the firm's R&D expenditures divided by total assets (missing R&D expenses are treated as zeros); *IT_Capability* equals one if the firm i in year t is included in the annual InformationWeek 500 (IW 500) list and zero otherwise; *Diversity* is the natural logarithm of the number of firm's geographic segments; *Institutional Ownership* equals the ratio of shares hold by institutional investors to firm's total outstanding shares in percentage; *Managerial Ability* is managerial ability score of firm i in year t following Demerjian et al., (2012); *Environmental Complexity* represents the opposite of concentration ratios for the top four firms in the firm's industry as in Keats and Hitt (1988); *Environmental Dynamism* is measured by regressing an observation's industry sales on a five-year period 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); *Environmental Munificence* equals the slope coefficient of the regression equation for calculating the environmental dynamism of the observation divided by the average sales of the industry, as in Keats and Hitt (1988). *Loss Dummy* equals one if the net income is negative. Constant terms, two-digit SIC industry, and year fixed effects are included in the regression. All the independent variables are measured in year t-1. Standard errors are in robust. Panel B compares the firm characteristics of data breach firms with those of matched non-data breach firms. T-tests are conducted to test for differences in mean values between data breach and non-data breach subsamples. The symbols ∗∗∗, ∗∗, and ∗ denote significance at the 1%, 5%, and 10% levels, respectively.

Panel A: Logit model on the probability of data breach occurrences	
	$Data\_Breach_{i,t}$
	(1)
$Ln(Assets_{i,t-1})$	1.123***
	(19.920)
$Leverage_{i,t-1}$	1.117***
	(4.246)
$ROA_{i,t-1}$	2.765**
	(2.492)
$R\&D_{i,t-1}$	17.626***
	(3.078)
$IT\_Capability_{i,t-1}$	1.104***
	(5.387)
$Diversity_{i,t-1}$	-0.625***
	(-4.710)
$Institutional\ Ownership_{i,t-1}$	1.873***
	(9.782)
$Managerial\ Ability_{i,t-1}$	0.708***
	(3.237)
$Environmental\ Complexity_{i,t-1}$	-1.557
	(-0.792)
$Environmental\ Dynamism_{i,t-1}$	0.021
	(0.030)

Table 1. [Continued] The results of Propensity Score Matching (PSM)

Panel A: Logit model on the probability of data breach occurrences	
	$Data\_Breach_{i,t}$
	(1)
$Environmental\ Munificence_{i,t-1}$	7.060*
	(1.930)
$Loss\ Dummy_{i,t-1}$	0.262
	(1.101)
Intercept	-18.021***
	(-10.699)
Industry and Year Fixed Effects	Yes
Observations	22273
Pseudo R^2	0.379

Panel B: Comparison of firm characteristics prior to data breach events after PSM				
Characteristics	Data breach firms	Matched non-data breach firms	Differences	T-test
Ln(Assets)	9.231	9.016	0.215	1.62
Leverage	0.630	0.604	0.026	1.24
ROA	0.059	0.068	-0.009	-1.40
R&D	0.001	0.002	-0.001	-0.92
IT_Capability	0.144	0.154	-0.010	-0.34
Diversity	2.113	2.074	0.040	0.77
Institutional Ownership	0.627	0.671	-0.044	-1.59
Managerial Ability	0.672	0.692	-0.020	-0.80
Environmental Complexity	-0.426	-0.420	-0.006	-0.43
Environmental Dynamism	0.217	0.220	-0.003	-0.29
Environmental Munificence	0.047	0.048	-0.002	-0.94
Loss Dummy	0.119	0.099	0.019	0.77

Table 2. Distribution of matched sample over time and across industries

We match each data breach observation with one control observation in firms without data breaches through PSM method. After identifying the control firms, our final sample includes all the firm-year observations of the breached firms and control firms during 2006-2016. Panel A reports the sample selection process. Panel B reports the distribution of our matched sample by year. Panel C reports the distribution of matched sample by one-digit SIC industry.

Panel A: Sample selection	
Number of data breaches from 2006 to 2016 reported by PRC or ITRC	13,807
Number of data breaches occurred in a US-listed firm.	1,262
Less: Number of data breaches that are not the first occurrence within one firm-year	(112)
Number of firm-year observations with data breaches	1,150
Less: Number of data breaches lacking data for PSM	(820)
Number of data breaches after PSM	330
330 data breaches (180 firms) + 330 control observations (201 firms)	
Number of firm-year observations for the above 381 firms from 2006 to 2016	3947
Less: Number of observations lacking data for baseline regression	(692)
Final sample (involving 285 data breaches)	3,255

Panel B: Distribution of matched sample by year

Year	Number of observations	Number of after breach observations	Percentage of after breach observations in all observations
2006	292	19	6.5%
2007	302	40	13.2%
2008	312	55	17.6%
2009	309	58	18.8%
2010	308	78	25.3%
2011	303	82	27.1%
2012	308	96	31.2%
2013	314	111	35.4%
2014	291	118	40.5%
2015	285	126	44.2%
2016	231	104	45.0%
Total	3255	887	27.3%

Table 2. [Continued] Distribution of matched sample over time and across industries

Panel C: Distribution of matched sample by one-digit SIC industry

SIC code	Included industries	Number of observations	Number of after breach observations	Percentage of after breach observations in all observations
0	Agricultural production & services; forestry; fishing, hunting and trapping	4	3	75.0%
1	Mining and construction	104	19	18.3%
2	Food, tobacco, textile mill, apparel, and lumber and wood products; furniture and fixtures; paper, printing, publishing, and chemical products; petroleum refining, etc.	539	151	28.0%
3	Rubber and plastic products; leather, stone, clay, glass, concrete, and metal products; machinery, electronic and electrical equipment; transportation equipment, measuring, analyzing, and controlling instruments, etc.	911	260	28.5%
4	Transportation, communications, electric, gas, and sanitary services	243	83	34.2%
5	Retail and wholesale trade	655	182	27.8%
7	Hotels, personal and business services; automotive repair services; motion pictures, amusement and recreation services, etc.	595	132	22.2%
8	Health, legal, educational, and social services; museums, art galleries, botanical and zoological gardens; membership organizations; engineering, accounting, research, and management services; private households, etc.	152	35	23.0%
9	Utilities	52	22	42.3%

Table 3 Summary statistics.

The sample includes all the non-financial data breach firms being covered in the Privacy Rights Clearinghouse (PRC) and Identity Theft Resource Center (ITRC) and the matched non-data-breach firms during 2006-2016. *Operational Efficiency 1* and *Operational Efficiency 2* is firm's operational efficiency measured in Stochastic Frontier Estimation (SFE) model following Battese and Coelli (1988) and Jondrow et al. (1982), respectively. *After_Data_Breach* is a dummy variable which equals one if the observation is in the year of or after the first data breach during our sample period and equals zero otherwise. *Ln(Assets)* is the natural logarithm of a firm's total assets; *Leverage* equals a firm's total liability divided by total assets; *ROA* represents a firm's net income divided by total assets; *R&D* is the firm's R&D expenditures divided by total assets (missing R&D expenses are treated as zeros); *IT_Capability* equals one if the firm i in year t is included in the annual InformationWeek 500 (IW 500) list and zero otherwise; *Diversity* is the natural logarithm of the number of firm's geographic segments; *Institutional Ownership* equals the ratio of shares hold by institutional investors to firm's total outstanding shares in percentage; *Managerial Ability* is managerial ability score of firm i in year t following Demerjian et al., (2012); *Environmental Complexity* represents the opposite of concentration ratios for the top four firms in the firm's industry as in Keats and Hitt (1988); *Environmental Dynamism* is measured by regressing an observation's industry sales on a five-year period 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); *Environmental Munificence* equals the slope coefficient of the regression equation for calculating the environmental dynamism of the observation divided by the average sales of the industry, as in Keats and Hitt (1988).

Variables	Observations	Mean	Standard deviation	Minimum	Q1	Median	Q3	Maximum
Operational Efficiency 1	3255	0.529	0.257	0.014	0.348	0.534	0.687	1.000
Operational Efficiency 2	3255	0.505	0.261	0.011	0.317	0.501	0.662	1.000
After_Data_Breach	3255	0.273	0.445	0.000	0.000	0.000	1.000	1.000
Ln(Assets)	3255	8.843	1.677	4.977	7.622	8.893	10.090	12.500
Leverage	3255	0.601	0.244	0.136	0.439	0.582	0.731	1.568
ROA	3255	0.054	0.076	-0.278	0.023	0.055	0.093	0.250
R&D	3255	0.001	0.002	0.000	0.000	0.000	0.000	0.017
IT_Capability	3255	0.094	0.292	0.000	0.000	0.000	0.000	1.000
Diversity	3255	2.220	0.627	1.099	1.792	2.303	2.773	3.664
Institutional Ownership	3255	0.631	0.364	0.000	0.398	0.776	0.894	1.147
Managerial Ability	3255	0.617	0.313	0.100	0.300	0.700	0.900	1.000
Environmental Complexity	3255	-0.414	0.174	-0.864	-0.486	-0.366	-0.291	-0.185
Environmental Dynamism	3255	0.232	0.122	0.068	0.164	0.188	0.272	0.722
Environmental Munificence	3255	0.045	0.022	-0.028	0.034	0.047	0.060	0.088

Table 4. Data Breach and Operational Efficiency

This table reports the results of DiD test of the effect of data breach on operational efficiency. The sample consists of the non-financial data breach firms being covered in the Privacy Rights Clearinghouse (PRC) and Identity Theft Resource Center (ITRC) and the matched non-data-breach firms during 2006-2016. *Operational Efficiency 1* and *Operational Efficiency 2* is firm's operational efficiency measured in Stochastic Frontier Estimation (SFE) model following Battese and Coelli (1988) and Jondrow et al. (1982), respectively. The operational efficiency is measured in year t+1. *After_Data_Breach* is a dummy variable which equals one if the observation is in the year of or after the first data breach during our sample period and equals zero otherwise. *Ln(Assets)* is the natural logarithm of a firm's total assets; *Leverage* equals a firm's total liability divided by total assets; *ROA* represents a firm's net income divided by total assets; *R&D* is the firm's R&D expenditures divided by total assets (missing R&D expenses are treated as zeros); *IT_Capability* equals one if the firm i in year t is included in the annual InformationWeek 500 (IW 500) list and zero otherwise; *Diversity* is the natural logarithm of the number of firm's geographic segments; *Institutional Ownership* equals the ratio of shares hold by institutional investors to firm's total outstanding shares in percentage; *Managerial Ability* is managerial ability score of firm i in year t following Demerjian et al., (2012); *Environmental Complexity* represents the opposite of concentration ratios for the top four firms in the firm's industry as in Keats and Hitt (1988); *Environmental Dynamism* is measured by regressing an observation's industry sales on a five-year period 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); *Environmental Munificence* equals the slope coefficient of the regression equation for calculating the environmental dynamism of the observation divided by the average sales of the industry, as in Keats and Hitt (1988). All the independent variables are measured in year t. Firm and year fixed effects are included in the regression. The *t*-statistics in parentheses are calculated from the robust standard. The symbols ∗∗∗, ∗∗, and ∗ denote significance at the 1%, 5%, and 10% levels, respectively.

	***Operational Efficiency 1*$_{i,t+1}$**		***Operational Efficiency 2*$_{i,t+1}$**	
	(1)	(2)	(3)	(4)
***After_Data_Breach*$_{i,t}$**	**-0.032****	**-0.033****	**-0.034****	**-0.035****
	(-2.118)	**(-2.275)**	**(-2.227)**	**(-2.385)**
Operational Efficiency 1$_{i,t}$		0.256***		
		(10.364)		
Operational Efficiency 2$_{i,t}$				0.245***
				(9.778)
Ln(Assets$_{i,t}$*)*		-0.008		-0.010
		(-0.651)		(-0.805)
Leverage$_{i,t}$		0.035		0.034
		(0.952)		(0.889)
ROA$_{i,t}$		0.068		0.069
		(1.034)		(1.028)
R&D$_{i,t}$		2.571		2.796
		(0.585)		(0.631)
IT_Capability$_{i,t}$		0.008		0.010
		(0.464)		(0.598)
Diversity$_{i,t}$		-0.037**		-0.037**
		(-2.100)		(-2.072)
Institutional Ownership$_{i,t}$		-0.028		-0.032
		(-1.268)		(-1.433)
Managerial Ability$_{i,t}$		0.004		0.003
		(0.225)		(0.204)

Table 4. [Continued] Data Breach and Operational Efficiency

	Operational Efficiency 1 $_{i,t+1}$		***Operational Efficiency 2*** $_{i,t+1}$	
	(1)	(2)	(3)	(4)
Environmental Complexity$_{i,t}$		-0.069		-0.088
		(-0.565)		(-0.705)
Environmental Dynamism$_{i,t}$		0.001		0.005
		(0.022)		(0.068)
Environmental Munificence$_{i,t}$		1.224*		1.259*
		(1.856)		(1.870)
Intercept	0.515***	0.436***	0.491***	0.435***
	(40.889)	(3.476)	(38.418)	(3.405)
Firm and Year Fixed Effect	Yes	Yes	Yes	Yes
Observations	3255	3255	3255	3255
Adjusted_R^2	0.399	0.440	0.396	0.435

Table 5. Dynamic DiD Test

This table reports the results of dynamic DiD test. The sample consists of the non-financial data breach firms being covered in the Privacy Rights Clearinghouse (PRC) and Identity Theft Resource Center (ITRC) and the matched non-data-breach firms during 2006-2016. *Operational Efficiency 1* and *Operational Efficiency 2* are firm's operational efficiency measured in Stochastic Frontier Estimation (SFE) model following Battese and Coelli (1988) and Jondrow et al. (1982), respectively. The operational efficiency is measured in year t+1. *Pre-jth Year* (*Post-jth Year*) equals one in the pre-jth year (post-jth year) relative to the year of data breach events, and zero otherwise. *Year 0* equals one in the data breach event year and zero otherwise. All the control variables are the same as those used in Table 4. All the independent variables are measured in year t. Firm and year fixed effects are included in the regression. The *t*-statistics in parentheses are calculated from the robust standard. The symbols ∗∗∗, ∗∗, and ∗ denote significance at the 1%, 5%, and 10% levels, respectively.

	Operational Efficiency 1$_{i,t+1}$	***Operational Efficiency 2***$_{i,t+1}$
	(1)	(2)
Pre-3rd Year$_{i,t}$	**-0.027**	**-0.026**
	(-1.256)	**(-1.173)**
Pre-2nd Year$_{i,t}$	**-0.019**	**-0.018**
	(-0.934)	**(-0.857)**
Pre-1stYear$_{i,t}$	**-0.019**	**-0.020**
	(-1.092)	**(-1.115)**
Year 0$_{i,t}$	**-0.028***	**-0.030***
	(-1.699)	**(-1.748)**
Post-1st Year$_{i,t}$	**-0.007**	**-0.007**
	(-0.350)	**(-0.347)**
Post-2nd Year$_{i,t}$	**-0.035**	**-0.036**
	(-1.537)	**(-1.566)**
Post-3rd Year$_{i,t}$	**-0.041**	**-0.040**
	(-1.492)	**(-1.440)**
Operational Efficiency 1$_{i,t}$	0.256***	
	(10.364)	
Operational Efficiency 2$_{i,t}$		0.245***
		(9.788)
Ln(Assets$_{i,t}$*)*	-0.009	-0.011
	(-0.756)	(-0.909)
Leverage$_{i,t}$	0.033	0.031
	(0.874)	(0.806)
ROA$_{i,t}$	0.072	0.073
	(1.086)	(1.081)
R&D$_{i,t}$	2.191	2.416
	(0.499)	(0.547)
IT_Capability$_{i,t}$	0.009	0.011
	(0.531)	(0.660)
Diversity$_{i,t}$	-0.034*	-0.034*
	(-1.926)	(-1.893)
Institutional Ownership$_{i,t}$	-0.023	-0.027
	(-1.017)	(-1.176)
Managerial Ability$_{i,t}$	0.004	0.003
	(0.237)	(0.212)

Table 5. [Continued] Dynamic DiD Test

	Operational Efficiency 1 $_{i,t+1}$	***Operational Efficiency 2*** $_{i,t+1}$
	(1)	(2)
Environmental Complexity$_{i,t}$	-0.066	-0.085
	(-0.538)	(-0.680)
Environmental Dynamism$_{i,t}$	0.008	0.012
	(0.125)	(0.171)
Environmental Munificence$_{i,t}$	1.142*	1.177*
	(1.730)	(1.747)
Intercept	0.445***	0.444***
	(3.536)	(3.461)
Firm and Year Fixed Effect	Yes	Yes
Observations	3255	3255
Adjusted_R^2	0.439	0.434

Table 6. Subsample Test on Exogenous Breaches

This table reports the results of DiD test by using OLS regression analysis of the effect of exogenous breaches on operational efficiency. We define the data breaches which are caused by outsiders (e.g., hackers, and physical thieves) as exogenous. We used the PSM approach for one-to-one matching as in the baseline analysis. The sample consists of 2,580 firm-years from 2006 to 2016. *Operational Efficiency 1* and *Operational Efficiency 2* are firm's operational efficiency measured in Stochastic Frontier Estimation (SFE) model following Battese and Coelli (1988) and Jondrow et al. (1982), respectively. The operational efficiency is measured in year t+1. All the control variables are the same as those used in Table 4. All the independent variables are measured in year t. Firm and year fixed effects are included in the regression. The *t*-statistics in parentheses are calculated from the robust standard. The symbols ∗∗∗, ∗∗, and ∗ denote significance at the 1%, 5%, and 10% levels, respectively.

	Operational Efficiency 1$_{i,t+1}$		***Operational Efficiency 2$_{i,t+1}$***	
	(1)	(2)	(3)	(4)
After_Exogenous_ Data_Breach$_{i,t}$	**-0.031***	**-0.033****	**-0.032****	**-0.034****
	(-1.935)	**(-2.141)**	**(-2.005)**	**(-2.194)**
Operational Efficiency 1$_{i,t}$		0.218***		
		(7.939)		
Operational Efficiency 2$_{i,t}$				0.209***
				(7.568)
Ln(Assets$_{i,t}$)		-0.005		-0.007
		(-0.332)		(-0.453)
Leverage$_{i,t}$		0.024		0.022
		(0.607)		(0.559)
ROA$_{i,t}$		0.035		0.039
		(0.469)		(0.499)
R&D$_{i,t}$		2.670		3.110
		(0.691)		(0.803)
IT_Capability$_{i,t}$		0.008		0.011
		(0.459)		(0.567)
Diversity$_{i,t}$		-0.031		-0.030
		(-1.601)		(-1.532)
Institutional Ownership$_{i,t}$		-0.015		-0.017
		(-0.532)		(-0.605)
Managerial Ability$_{i,t}$		-0.003		-0.001
		(-0.142)		(-0.070)
Environmental Complexity$_{i,t}$		-0.246*		-0.255*
		(-1.838)		(-1.877)
Environmental Dynamism$_{i,t}$		-0.017		-0.018
		(-0.203)		(-0.206)
Environmental Munificence$_{i,t}$		2.125***		2.119***
		(3.336)		(3.280)
Intercept	0.512***	0.488***	0.310**	0.306**
	(36.154)	(33.914)	(2.192)	(2.148)
Firm and Year Fixed Effect	Yes	Yes	Yes	Yes
Observations	2,580	2,580	2,580	2,580
Adjusted_R^2	0.377	0.376	0.410	0.406

Table 7. Placebo Test

This table reports the results of placebo test. *Operational Efficiency 1* and *Operational Efficiency 2* are firm's operational efficiency measured in Stochastic Frontier Estimation (SFE) model following Battese and Coelli (1988) and Jondrow et al. (1982), respectively. The operational efficiency is measured in year t+1. *Placebo_Data_Breach* is the pseudo treatment dummy which equals one in the three years earlier than the actual data breach events and equals zero otherwise. All the control variables are the same as those used in Table 4. All the independent variables are measured in year t. Firm and year fixed effects are included in the regression. The *t*-statistics in parentheses are calculated from the robust standard. The symbols ∗∗∗, ∗∗, and ∗ denote significance at the 1%, 5%, and 10% levels, respectively.

	Operational Efficiency 1$_{i,t+1}$	***Operational Efficiency 2***$_{i,t+1}$
	(1)	(2)
Placebo_Data_Breach$_{i,t}$	**-0.007**	**-0.007**
	(-0.634)	**(-0.562)**
Operational Efficiency 1$_{i,t}$	0.257***	
	(10.386)	
Operational Efficiency 2$_{i,t}$		0.246***
		(9.807)
Ln(Assets$_{i,t}$*)*	-0.010	-0.012
	(-0.774)	(-0.926)
Leverage$_{i,t}$	0.030	0.028
	(0.794)	(0.727)
ROA$_{i,t}$	0.072	0.073
	(1.093)	(1.085)
R&D$_{i,t}$	2.155	2.369
	(0.490)	(0.535)
IT_Capability$_{i,t}$	0.009	0.011
	(0.539)	(0.676)
Diversity$_{i,t}$	-0.034*	-0.034*
	(-1.908)	(-1.877)
Institutional Ownership$_{i,t}$	-0.023	-0.027
	(-1.025)	(-1.181)
Managerial Ability$_{i,t}$	0.003	0.003
	(0.201)	(0.179)
Environmental Complexity$_{i,t}$	-0.058	-0.076
	(-0.469)	(-0.607)
Environmental Dynamism$_{i,t}$	0.007	0.010
	(0.107)	(0.155)
Environmental Munificence$_{i,t}$	1.118*	1.148*
	(1.701)	(1.712)
Intercept	0.449***	0.448***
	(3.566)	(3.493)
Firm and Year Fixed Effect	Yes	Yes
Observations	3255	3255
Adjusted_R^2	0.439	0.434

Table 8. Moderators Test: Managerial Risk-Taking Incentives

This table reports the results of moderator test on managerial risk-taking incentives. A firm is assigned to the higher (lower) managerial risk-taking incentives group if its CEO vega in year t is larger (smaller) than the two-digit SIC industry-year median. Vega is measured as the change in the manager's overall option value for a 0.01 change in the annualized standard deviation of stock returns following Core and Guay (2002) and Coles et al. (2006). Other variables are the same as those used in Table 4. Firm and year fixed effects are included in the regression. The *t*-statistics in parentheses are calculated from the robust standard. The symbols ∗∗∗, ∗∗, and ∗ denote significance at the 1%, 5%, and 10% levels, respectively.

	Operational Efficiency 1$_{i,t+1}$		***Operational Efficiency 2$_{i,t+1}$***	
	(1) Low Managerial Risk-Taking Incentives (low CEO vega) Group	(2) High Managerial Risk-Taking Incentives (high CEO vega) Group	(3) Low Managerial Risk-Taking Incentives (low CEO vega) Group	(4) High Managerial Risk-Taking Incentives (high CEO vega) Group
After_Data_Breach$_{i,t}$	**-0.063***	**-0.016**	**-0.068***	**-0.016**
	(-1.758)	**(-0.712)**	**(-1.823)**	**(-0.718)**
Operational Efficiency 1$_{i,t}$	0.232***	0.201***		
	(4.825)	(5.045)		
Operational Efficiency 2$_{i,t}$			0.222***	0.191***
			(4.568)	(4.731)
Ln(Assets$_{i,t}$)	-0.019	-0.029	-0.022	-0.029
	(-0.820)	(-1.375)	(-0.911)	(-1.365)
Leverage$_{i,t}$	0.098	0.036	0.094	0.039
	(1.408)	(0.531)	(1.304)	(0.556)
ROA$_{i,t}$	-0.093	0.029	-0.090	0.026
	(-0.873)	(0.239)	(-0.824)	(0.209)
R&D$_{i,t}$	3.344	-4.447	3.577	-4.450
	(0.383)	(-0.916)	(0.403)	(-0.927)
IT_Capability$_{i,t}$	0.024	-0.005	0.028	-0.003
	(0.848)	(-0.198)	(0.970)	(-0.099)
Diversity$_{i,t}$	-0.029	-0.083**	-0.025	-0.083**
	(-0.861)	(-2.550)	(-0.732)	(-2.493)
Institutional Ownership$_{i,t}$	-0.010	-0.015	-0.012	-0.021
	(-0.295)	(-0.332)	(-0.370)	(-0.451)
Managerial Ability$_{i,t}$	0.008	0.020	0.008	0.021
	(0.280)	(0.748)	(0.276)	(0.770)
Environmental Complexity$_{i,t}$	0.055	-0.323*	0.022	-0.333*
	(0.213)	(-1.704)	(0.085)	(-1.709)
Environmental Dynamism$_{i,t}$	-0.033	0.051	-0.021	0.048
	(-0.239)	(0.517)	(-0.149)	(0.482)
Environmental Munificence$_{i,t}$	2.746***	-0.881	2.795***	-0.889
	(2.905)	(-0.635)	(2.867)	(-0.642)
Intercept	0.474**	0.740***	0.459**	0.728***
	(2.123)	(3.523)	(2.002)	(3.417)
Firm and Year Fixed Effect	Yes	Yes	Yes	Yes
Observations	1107	1331	1107	1331
Adjusted_R^2	0.429	0.457	0.415	0.451

Table 9. Moderators Test: Financial Slack

This table reports the results of moderator test on financial slack. Panel A reports the results based on WW index, and Panel B reports the results based on Altman's Z-score. A firm is assigned to the higher financial slack group if its WW index (Altman's Z-score) is smaller (higher) than the two-digit SIC industry-year median, and vice versa. Other variables are the same as those used in Table 4. Firm and year fixed effects are included in the regression. The *t*-statistics in parentheses are calculated from the robust standard. The symbols ∗∗∗, ∗∗, and ∗ denote significance at the 1%, 5%, and 10% levels, respectively.

Panel A: Results based on the WW index

	Operational Efficiency 1$_{i,t+1}$		***Operational Efficiency 2$_{i,t+1}$***	
	(1)	(2)	(3)	(4)
	Low Financial slack (high WW index) Group	High Financial slack (low WW index) Group	Low Financial slack (high WW index) Group	High Financial slack (low WW index) Group
After_Data_Breach$_{i,t}$	**-0.071*****	**-0.028**	**-0.073*****	**-0.028**
	(-2.700)	**(-0.911)**	**(-2.731)**	**(-0.905)**
Operational Efficiency 1$_{i,t}$	0.199***	0.218***		
	(4.365)	(4.262)		
Operational Efficiency 2$_{i,t}$			0.189***	0.202***
			(4.101)	(3.933)
Ln(Assets$_{i,t}$)	-0.037	0.016	-0.039	0.013
	(-1.502)	(0.417)	(-1.547)	(0.354)
Leverage$_{i,t}$	-0.034	0.224**	-0.038	0.233**
	(-0.442)	(2.424)	(-0.498)	(2.476)
ROA$_{i,t}$	0.143	-0.041	0.142	-0.043
	(1.115)	(-0.207)	(1.099)	(-0.214)
R&D$_{i,t}$	-13.613*	132.838	-13.944*	136.981
	(-1.956)	(0.951)	(-1.914)	(0.970)
IT_Capability$_{i,t}$	0.038	-0.033	0.043	-0.032
	(1.377)	(-1.131)	(1.497)	(-1.108)
Diversity$_{i,t}$	-0.006	-0.056*	-0.005	-0.062*
	(-0.184)	(-1.657)	(-0.144)	(-1.758)
Institutional Ownership$_{i,t}$	-0.039	0.066	-0.046	0.066
	(-0.773)	(1.022)	(-0.889)	(1.020)
Managerial Ability$_{i,t}$	-0.012	0.049	-0.011	0.050
	(-0.459)	(1.578)	(-0.422)	(1.585)
Environmental Complexity$_{i,t}$	-0.349*	0.304	-0.366*	0.316
	(-1.721)	(1.202)	(-1.821)	(1.225)
Environmental Dynamism$_{i,t}$	0.113	0.215	0.114	0.237*
	(1.384)	(1.550)	(1.351)	(1.690)
Environmental Munificence$_{i,t}$	0.320	1.684	0.369	1.587
	(0.354)	(0.972)	(0.394)	(0.908)
Intercept	0.608***	0.191	0.603***	0.211
	(2.799)	(0.485)	(2.735)	(0.528)
Firm and Year Fixed Effect	Yes	Yes	Yes	Yes
Observations	1126	884	1126	884
Adjusted_R^2	0.417	0.419	0.407	0.417

Table 9. [Continued] Moderators Test: Financial Slack

Panel B: Results based on the Altman's Z-score				
	Operational Efficiency 1$_{i,t+1}$		***Operational Efficiency 2$_{i,t+1}$***	
	(1)	(2)	(3)	(4)
	Low Financial slack (low Z-score) Group	High Financial slack (high Z-score) Group	Low Financial slack (low Z-score) Group	High Financial slack (high Z-score) Group
After_Data_Breach$_{i,t}$	**-0.047****	**-0.019**	**-0.052****	**-0.018**
	(-2.031)	**(-0.853)**	**(-2.208)**	**(-0.801)**
Operational Efficiency 1$_{i,t}$	0.222***	0.221***		
	(5.769)	(5.783)		
Operational Efficiency 2$_{i,t}$			0.208***	0.209***
			(5.269)	(5.430)
Ln(Assets$_{i,t}$)	-0.003	0.006	-0.004	0.003
	(-0.168)	(0.263)	(-0.211)	(0.113)
Leverage$_{i,t}$	-0.007	0.013	-0.001	0.005
	(-0.112)	(0.205)	(-0.020)	(0.076)
ROA$_{i,t}$	0.088	-0.017	0.091	-0.018
	(0.892)	(-0.135)	(0.906)	(-0.137)
R&D$_{i,t}$	13.235*	-10.955*	13.354*	-10.425*
	(1.831)	(-1.761)	(1.814)	(-1.674)
IT_Capability$_{i,t}$	0.028	-0.001	0.029	0.003
	(1.059)	(-0.053)	(1.066)	(0.126)
Diversity$_{i,t}$	-0.038	-0.048*	-0.037	-0.049*
	(-1.237)	(-1.812)	(-1.170)	(-1.836)
Institutional Ownership$_{i,t}$	-0.020	-0.020	-0.027	-0.025
	(-0.594)	(-0.560)	(-0.772)	(-0.687)
Managerial Ability$_{i,t}$	-0.041	0.025	-0.045	0.027
	(-1.483)	(1.016)	(-1.597)	(1.084)
Environmental Complexity$_{i,t}$	-0.354*	0.107	-0.388*	0.103
	(-1.686)	(0.552)	(-1.818)	(0.524)
Environmental Dynamism$_{i,t}$	0.058	-0.055	0.067	-0.054
	(0.557)	(-0.548)	(0.607)	(-0.538)
Environmental Munificence$_{i,t}$	1.223	0.662	1.312	0.676
	(1.265)	(0.538)	(1.323)	(0.526)
Intercept	0.298	0.486**	0.273	0.507**
	(1.438)	(2.207)	(1.287)	(2.262)
Firm and Year Fixed Effect	Yes	Yes	Yes	Yes
Observations	1439	1665	1439	1665
Adjusted_R^2	0.462	0.407	0.457	0.401

Table 10. Moderators Test: Product Market Competition

This table reports the results of moderator test on product market competition. Panel A reports the results based on Herfindahl index (*HHI)*, and Panel B reports the results based on product similarities (*TNIC3TSIMM)*. A firm is assigned to the higher (lower) product market competition group if its *HHI* is below (above) the year median (or its *TNIC3TSIMM* is above (below) the two-digit SIC industry-year median). Other variables are the same as those used in Table 4. Firm and year fixed effects are included in the regression. The *t*-statistics in parentheses are calculated from the robust standard. The symbols ∗∗∗, ∗∗, and ∗ denote significance at the 1%, 5%, and 10% levels, respectively.

Panel A: Results based on the three-digit industry Herfindahl index (HHI)

	Operational Efficiency 1$_{i,t+1}$		***Operational Efficiency 2$_{i,t+1}$***	
	(1)	(2)	(3)	(4)
	Low Product Market Competition (high HHI) Group	High Product Market Competition (low HHI) Group	Low Product Market Competition (high HHI) Group	High Product Market Competition (low HHI) Group
After_Data_Breach$_{i,t}$	**-0.062*****	**-0.008**	**-0.064*****	**-0.012**
	(-2.978)	**(-0.415)**	**(-2.975)**	**(-0.563)**
Operational Efficiency 1$_{i,t}$	0.225***	0.273***		
	(6.235)	(7.755)		
Operational Efficiency 2$_{i,t}$			0.217***	0.258***
			(5.931)	(7.203)
Ln(Assets$_{i,t}$)	-0.038*	0.016	-0.041**	0.015
	(-1.882)	(0.966)	(-1.968)	(0.884)
Leverage$_{i,t}$	0.103	0.011	0.103	0.010
	(1.545)	(0.246)	(1.520)	(0.209)
ROA$_{i,t}$	0.197*	0.020	0.198*	0.023
	(1.717)	(0.243)	(1.673)	(0.280)
R&D$_{i,t}$	1.804	4.919	1.810	5.515
	(0.303)	(0.774)	(0.300)	(0.875)
IT_Capability$_{i,t}$	0.029	-0.003	0.033	-0.002
	(1.284)	(-0.149)	(1.432)	(-0.096)
Diversity$_{i,t}$	-0.025	-0.033	-0.024	-0.034
	(-0.964)	(-1.306)	(-0.927)	(-1.328)
Institutional Ownership$_{i,t}$	-0.036	-0.010	-0.037	-0.015
	(-1.034)	(-0.318)	(-1.066)	(-0.475)
Managerial Ability$_{i,t}$	0.001	0.013	0.000	0.014
	(0.024)	(0.574)	(0.012)	(0.575)
Environmental Complexity$_{i,t}$	-0.217	-0.039	-0.248	-0.034
	(-1.324)	(-0.192)	(-1.477)	(-0.165)
Environmental Dynamism$_{i,t}$	-0.048	0.112	-0.057	0.127
	(-0.558)	(1.056)	(-0.622)	(1.188)
Environmental Munificence$_{i,t}$	0.561	1.815**	0.648	1.855**
	(0.522)	(2.095)	(0.580)	(2.090)
Intercept	0.608***	0.160	0.601***	0.162
	(3.133)	(0.896)	(3.017)	(0.891)
Firm and Year Fixed Effect	Yes	Yes	Yes	Yes
Observations	1630	1625	1630	1625
Adjusted_R^2	0.436	0.451	0.427	0.450

Table 10. [Continued] Moderators Test: Product Market Competition

Panel B: Results based on the product similarities (TNIC3TSIMM)				
	Operational Efficiency 1$_{i,t+1}$		***Operational Efficiency 2$_{i,t+1}$***	
	(1)	(2)	(3)	(4)
	Low Product Market Competition (low TNIC3TSIMM) Group	High Product Market Competition (high TNIC3TSIMM) Group	Low Product Market Competition (low TNIC3TSIMM) Group	High Product Market Competition (high TNIC3TSIMM) Group
After_Data_Breach$_{i,t}$	**-0.062****	**-0.003**	**-0.063****	**-0.008**
	(-2.575)	**(-0.143)**	**(-2.572)**	**(-0.313)**
Operational Efficiency 1$_{i,t}$	0.241***	0.228***		
	(5.375)	(6.334)		
Operational Efficiency 2$_{i,t}$			0.235***	0.216***
			(5.125)	(5.981)
Ln(Assets$_{i,t}$)	-0.038	0.007	-0.038	0.006
	(-1.519)	(0.419)	(-1.482)	(0.349)
Leverage$_{i,t}$	0.037	-0.002	0.038	-0.002
	(0.657)	(-0.038)	(0.662)	(-0.033)
ROA$_{i,t}$	-0.085	0.079	-0.070	0.077
	(-0.782)	(0.775)	(-0.620)	(0.745)
R&D$_{i,t}$	-8.756	11.970	-9.140	12.971
	(-1.475)	(1.423)	(-1.507)	(1.505)
IT_Capability$_{i,t}$	0.012	0.006	0.015	0.007
	(0.477)	(0.244)	(0.570)	(0.322)
Diversity$_{i,t}$	-0.075**	-0.013	-0.077**	-0.010
	(-2.422)	(-0.426)	(-2.425)	(-0.319)
Institutional Ownership$_{i,t}$	0.007	-0.025	-0.000	-0.029
	(0.172)	(-0.838)	(-0.000)	(-0.936)
Managerial Ability$_{i,t}$	0.022	-0.002	0.022	-0.001
	(0.779)	(-0.104)	(0.752)	(-0.047)
Environmental Complexity$_{i,t}$	-0.251	-0.041	-0.291	-0.046
	(-1.195)	(-0.218)	(-1.350)	(-0.243)
Environmental Dynamism$_{i,t}$	-0.046	-0.159	-0.045	-0.182
	(-0.370)	(-1.048)	(-0.352)	(-1.132)
Environmental Munificence$_{i,t}$	1.975**	1.713	2.033**	1.791
	(2.447)	(1.037)	(2.398)	(1.070)
Intercept	0.687***	0.313	0.662***	0.302
	(3.070)	(1.632)	(2.862)	(1.551)
Firm and Year Fixed Effect	Yes	Yes	Yes	Yes
Observations	1303	1522	1303	1522
Adjusted_R^2	0.453	0.437	0.446	0.431