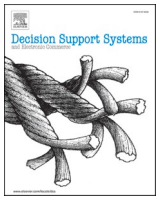
Decision Support Systems 179 (2024) 114173

Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss



To alert or alleviate? A natural experiment on the effect of anti-phishing laws on corporate IT and security investments

Xiaoxiao Wang [a], Wilson Weixun Li [b,*], Alvin Chung Man Leung [a], Wei Thoo Yue [a]

[a] Department of Information Systems, College of Business, City University of Hong Kong, Hong Kong, China
[b] Department of Information Systems and Business Analytics, Deakin Business School, Deakin University, Melbourne, Australia

ARTICLE INFO

Keywords:
Anti-phishing laws
Security investment
IT investment
Signaling effect
Difference-in-difference

ABSTRACT

In the United States, between 2005 and 2017, 23 states enacted anti-phishing laws to prosecute those suspected of phishing. As the primary targets of phishing attacks, firms' interpretations and reactions toward these laws are worth investigating. Utilizing a unique dataset in a natural experimental setting, this study employed the difference-in-differences method to contrast firms' investment decisions related to IT and cybersecurity in states in which such laws had been enacted and those in states without such laws, both before and after their enactment. We found that firms with different operational experiences react to the enactment of the anti-phishing laws in different ways. We further demonstrate the moderating roles of the industry risk landscape and IT capability. Specifically, firms with high-IT increased investments in both IT and cybersecurity while the risk landscape stimulated investments in cybersecurity only. This suggests that the risk landscape facilitates sensitivity to the immediate risk signaled by enactment of the laws, and IT capability further enables the alignment between IT investments and security objectives. This study also discusses the policy implications of our findings.

1. Introduction

Phishing is considered one of the most common methods for attackers to breach organizations [1]. The 2020 "State of the Phish" report stated around 57% of organizations experienced phishing attacks [2]. Phishing attacks across the globe cause millions of dollars of losses per year [3], often in the form of damage to firms' reputation and loss of customer confidence [4,5]. Furthermore, phishing is often used as the initial attack vector to launch other attacks such as data breaches and malware [6,7]. Phishing is challenging to curb because it costs almost nothing for "phishers" to execute attacks [8], and such attacks often target unsuspecting end users [9,10].

In the United States, California was the first state to pass legislation targeting phishing in 2005. Since then, 23 states have enacted anti-phishing laws. These laws formally define phishing and dictate punishment for attackers. For example, Michigan's anti-phishing laws focus on the use of false electronic communication or webpages representing a business to solicit personal information, whereas Oregon's laws emphasize the false representation of a third person to solicit personal information, with specific conditions for law enforcement (as shown in Table B in Appendix B). Unlike anti-phishing laws, certain other cybersecurity legislations like Data Breach Notification Laws (DBNLs) and Consumer Privacy Acts impose regulatory obligations directly on entities, pushing firms toward enhanced investments in security and IT infrastructure to ensure compliance [11]. These laws not only signal the escalating threat landscape but also mandate or incentivize firms to bolster their security measures, showcasing a direct, tangible impact on firms' operational landscape. Moreover, statewide cybersecurity task forces, by enhancing state cybersecurity infrastructure and fostering a collaborative ecosystem, provide positive incentives that spur firms to bolster their security and IT investments [12]. These proactive efforts send a strong, positive signal, potentially confounding the threat signals perceived by firms. Therefore, it's pivotal to discern the nuanced signaling effects of various cybersecurity laws and measures. Anti-phishing laws, focusing on legal recourse against adversaries, serve as a more straightforward signal of threat to firms, contrasting with laws like DBNLs and Consumer Privacy Acts which mandate firms to enhance security measures. This distinct focus simplifies the investigation of signaling effect of anti-phishing laws, allowing for a more precise examination amidst the dynamic threat landscape.

Given cybersecurity laws are constantly evolving to adapt to cybercriminals' tactics, and vice versa, the implementation of anti-phishing

* Corresponding authors.
E-mail addresses: xxwang25-c@my.cityu.edu.hk (X. Wang), wilson.li@deakin.edu.au (W.W. Li), acmleung@cityu.edu.hk (A.C.M. Leung), Wei.T.Yue@cityu.edu.hk (W.T. Yue).

https://doi.org/10.1016/j.dss.2024.114173
Received 29 January 2023; Received in revised form 25 December 2023; Accepted 3 January 2024
Available online 4 January 2024

laws provides us with a unique setting in which to examine whether such laws extend to influencing the behaviors of firms that attackers target.[1] We conjecture two possible firm reactions: First, anti-phishing laws may give firms a misleading comfort in digital safety, potentially fostering complacency in cybersecurity—a reflection of the 'Peltzman effect' [13]. To illustrate, while airbags are designed to enhance passenger safety in vehicles, there is evidence suggesting that their presence may encourage some drivers to take more risks, under the assumption that they are better protected [14]. As a result, firms may regard such anti-phishing laws as a substitute for investments in new security measures. Second, anti-phishing legislation demonstrates the government's serious commitment to tackling phishing crimes. Hence, such laws may serve as a threat-signaling mechanism for firms and encourage them to recognize the clear threat posed by phishing crimes. For example, De Silva and Torgler [15] found medical marijuana laws have a signaling effect that draws people's attention to the risks of using marijuana. These two competing mechanisms may influence how firms deploy resources to fight phishing, specifically, and cybersecurity attacks, in general.

To protect users against phishing, firms often rely on conventional measures like security awareness training, firewalls, and spam filters, which have been criticized as being insufficient to combat sophisticated phishing threats.[2,3] Security experts advocate firms consider comprehensive solutions, such as integrating security into IT designs and leveraging advanced technologies to combat phishing threats [16,17]. Thus, in this study, we examine how the implementation of anti-phishing laws affects firms' IT and security investment decisions. We further contrast single-state firms and multi-state firms to understand the role of institutional factors (e.g., cybersecurity-related scope and experience). Prior studies have identified displacement effects [18] of the laws from the "attacker's side," which means more attacks are shifted toward less protected digital assets, and a larger scope of businesses could be affected if these "weakest links" are compromised. Considering this, our subsequent analysis seeks to address the 'spillover effect,' examining whether firms should enhance site-specific security or overall safeguards to mitigate broader risks from displacement strategies.

We used panel data, collected between 2010 and 2017, from approximately 400,000 firms. The study period began five years after the 2005 enactment of the first anti-phishing legislation in the United States, which ensures most firms had already become aware of phishing attacks and anti-phishing laws. During the research period, four U.S. states (i.e., Michigan, Alabama, Oregon, and Arizona) enacted state-level anti-phishing laws in 2011, 2012, 2015, and 2016, respectively. However, Alabama and Arizona also enacted other cybersecurity-related acts to address denial of service attacks or spyware in the same year. To alleviate the potential confounding effects, we only considered firms in Michigan and Oregon as treatment firms.

This study makes several important contributions to current information security literature and holds several important implications for practice: First, we enrich the existing research on the signaling effect of laws by demonstrating with empirical evidence that firms perceive the enactment of anti-phishing laws as a signal of increasing threats. Second, we explain the disparate organizational behaviors of single- and multi-state firms in cybersecurity. Third, our findings suggest that policymakers should pay greater attention to the possible side effects of anti-phishing laws, as well as that appropriate legislation can help firms implement proactive security management by providing proper IT support.

The study is structured as follows: In Section 2, we review the related literature and develop our conceptual model and hypotheses. Section 3 describes our data source and the methodology we undertook. In Section 4, we present our analysis and discuss the results. In the final section, we provide the conclusions. We present the results of various additional analysis in Appendix A and C and the details of the anti-phishing acts in Michigan and Oregon in Appendix B.

2. Literature review and hypotheses development

Our work is closely related to the following four streams of literature: the indirect effect of regulations and law enactments; the effect of cybersecurity-related laws and policies; firm-level factors affecting security investments; and the spillover effect in cybersecurity research. We summarize and discuss the related concepts of each stream of research below.

The indirect effect[4] of regulations and laws often refers to the effect on unregulated entities [19]. For example, Zhang [20] identifies that affirmative action bans enforced on public sectors also affect private-sector executives' decision-making in regard to recruiting minorities. Peukert et al. [21] found the enactment of the general data protection regulation (GDPR) reduces the interactions between websites and web technology providers; the relationship is even extended to those firms that are not regulated by GDPR. Prior studies propose two mechanisms to explain the indirect effect. The first is sending a signal to the unregulated entities [21,20], and the second is altering the market structure [19]. The unregulated entities may interpret the policies as a signal, indicating a similar future regulation [21] or as revealing social norms [20], which ultimately motivate and change the unregulated entities' behaviors. Regardless of the unregulated entities' interpretation, some policies enforced on regulated entities directly change the market structure. For example, The Sarbanes–Oxley Act of 2002 places stricter requirements on public firms' internal controls, which stimulates the demand for auditing services but also increases the audit fees for unregulated nonprofit organizations [19]. In the context of this work, we consider firms to be unregulated entities, as the anti-phishing laws penalize the adversaries launching phishing attacks (as shown in Table B in Appendix B), and the mechanism of the indirect effect is more aligned with the signaling effect argument and less relevant to the context of altering the market structure. The enactment of anti-phishing laws serves as a clear signal of an escalating threat landscape. As risks become more tangible, firms prompt reassessment and necessary adjustments to IT and security infrastructures [22,23]. In addition, the enactment strengthens the signal to the market by defining crimes and penalties, guiding firms to align their practices and policies to prevent potential brand damage.

Regarding the research on cybersecurity-related laws and policies, scholars mainly focus on firm-specific regulations, like GDPR, DBNL, and the Cybersecurity Information Sharing Act (CISA), which require firms to fulfill privacy protection or security incident disclosure requirements. This stream of studies investigates the effects of the laws on firms' security investments [24] and security outcomes (e.g., rates of identity theft and spam volumes) [25,26]. Furthermore, prior studies have revealed firms may undertake undesirable behaviors when facing related laws, including compromising the readability and details of data breach disclosures [27,28], hoarding bad news, strategically timing data breach disclosures [29,30], or slowing down digitalization [11].

1 Cybersecurity problems have long been regarded as a "cat and mouse" game involving attackers, target firms, and their mutual expectations [113] H. Cavusoglu, B. Mishra, S. Raghunathan, The value of intrusion detection systems in information technology security architecture, Information Systems Research, 16(1) (2005), 28–46.

2 Although security awareness training has been widely adopted to deter phishing, surveys show solely relying on security awareness training may make things worse, as false positives overwhelm security teams (https://www.agari.com/email-security-blog/businesses-waste-millions-false-positives/).

3 Conventional filters that look for specific content or keywords can be easily fooled by slightly changed phishing elements (https://blog.devolutions.net/2021/09/the-evolution-of-phishing-why-its-getting-worse-how-to-fight-back/).

4 The indirect effect is also called the "spillover effect" or "externalities." To avoid confusion, we refer to it as the "indirect effect" to distinguish it from the (intrafirm) spillover effect examined in the additional analysis.

However, firms' responses to regulations are mainly understood from the perspective of complying with regulations and reducing (or transferring) compliance costs. There is little discussion regarding how firms interpret the laws and shape their understanding of the risk landscape—or what factors moderate firms' interpretations and reactions to such laws. Overlooking firms' interpretations may undermine the importance of firms' proactively leveraging regulations and policies to advocate for more cybersecurity attention and resources [31]. Moreover, law enforcement signals a national commitment to ensuring a secure environment, which can also encourage firms to allocate more resources to profit reinvestment [32,33]. Thus, investigating how firms interpret law enforcement and what factors moderate the process is important to the development of a comprehensive understanding regarding the interaction between policymakers and firms, as well as provide more insight into future cybersecurity-related legislation.

Firms' interpretations of and reactions toward legislation can be dependent upon their capabilities and prior experience. Prior literature identifies firm-level factors like senior management's degree of commitment to security and the security awareness of top managers as important for firms' implementation of security solutions [34,35,36]. Moreover, firm understanding of security threats and technology solutions has been shown to positively affect the firm's security management [37,38]. According to organizational learning literature [39,40,41], security awareness and capabilities can be nurtured during the process of addressing relevant issues. In the context of this work, firms operating in multiple states have richer security-related experience than single-state firms because multi-state firms have encountered a wider scope of security issues and security-related regulations. Conceptually, multi-state firms can leverage prior experience and quickly adapt in response to new legislation.

The spillover effect in cybersecurity research focuses on market reactions, including the non-breached firms, in response to data breach incidents. Islam et al. [42] and Kelton and Pennington [43] find investment contagion effects on non-breached rivals due to the uncertainties caused by the breached firms. Li et al. [44] note that non-breached firms adjust their security strategies when industrial peers experience security breaches. Jeong et al. [45] observe the market interprets the security investment of one firm after a breach, which can increase the overall security level in the industry. The spillover effect further extends to other business behaviors such as increasing cash holdings [46]. These findings support the view that the dynamic risk landscape signaled by the actual incidents or the market can affect firms' actions. Kelton and Pennington [43] and Kashmiri et al. [47] conclude firms with extensive understanding of security issues can effectively respond to evolving threats and act to mitigate negative spillover effects. However, such a viewpoint has not been extended to the context of security-related policies.

Building on previous research, in the current study, we seek to develop a conceptual model to examine the signaling effect of anti-phishing laws on firms' investment decisions in IT and security. We highlight the importance of the moderating role played by firms' multi-state operational experience, which facilitates knowledge-sharing among sites and sensitivity to evolving threats. Fig. 1 presents our conceptual model.

2.1. Signaling effect

As discussed, we base the conceptual model on the signaling effects of the laws, as identified in previous studies [21,20]. A distinctive feature of anti-phishing laws is their classification under civil jurisdiction in two-thirds of states, leading to financial penalties for adversaries rather than imprisonment, unlike other computer crime statutes which are typically criminal across states.[5] For instance, laws against hacking, unauthorized access, and other cybercrimes fall under criminal jurisdiction.[v] On the other hand, spyware laws exhibit a split, with an equal division between civil and criminal categorization across states.[v] Anti-phishing laws, with their slant toward civil penalties such as fines, may seem less intimidating to businesses because the consequences for cybercriminals aren't as harsh. This perception may shape how companies invest in security differently than they would under more stringent cybersecurity regulations.

Building on the discussion of perceived deterrence, there's a realm of law-induced 'false' sense of security as illustrated by [48,49]. For instance, the Adam Walsh Child Protection and Safety Act, which targets low-risk offenders but sometimes misses high-risk culprits, could give a misleading signal about the relative safety of certain environments [48]. Translating this to the realm of cybersecurity, one might assume that firms would perceive anti-phishing laws as providing an adequate shield and thereby become passive about ramping up their security investments. However, the adequacy of civil penalties as deterrents is debatable [50,51], especially when compared with the potential lucrative gains from successful cyberattacks. Beyond individual laws, the broader legal framework encompassing new cybersecurity laws, irrespective of their punitive nature, also echoes across the business landscape, heightening stakeholder threat awareness [52], leading to a cascading impact on the corporate world. The signaling effect combined with regulatory compliance has been known to spike the demand for security products [53]. Similarly, researchers have argued higher risk awareness at the organizational level can motivate users to seek additional measures to manage risks [54].

Given the nuances and the weight of the signaling effect, especially in the backdrop of these laws being civil in nature, we hypothesize that enacting anti-phishing laws will amplify the security consciousness of firms operating in states with such regulations, prompting them to bolster their security investments.

H1a. ***Anti-phishing laws motivate firms operating in anti-phishing law states to increase security investments.***

2.2. Integration of IT and security investment strategies

Rather than solely focusing on security investment, firms must strengthen IT competency to counteract threats effectively. This perspective aligns with the resource-based view emphasizing that proper IT competency requires implementing all facets of IT practices [40]. General IT investment, aimed at holistically enhancing a firm's IT infrastructure, fosters a more robust strategy in handling security challenges [55,56].

Previous studies underline the crucial role of IT within security management, broadening firms' avenues for tackling security challenges [57,58,59]. This view is supported by several essential insights. First, IT plays a vital role in pinpointing and remedying vulnerabilities rooted in flawed design [60,61]. Second, strong IT infrastructures facilitate the alignment of IT and security objectives [62,63]. Li et al. [64] suggest a lack of such alignment might undermine the effectiveness of security measures. Third, various IT solutions can nurture a security-conscious culture, reducing errors in IT execution [65] and bridging the existing divide between IT and security [66,35]. Specifically, Li et al. [67] provides empirical support that firms are investing more in general IT following heightened threat awareness, which not only addresses immediate security needs but also strengthens the overall IT framework to prevent future incidents.

In light of previous empirical findings [66,65,67], we propose that anti-phishing laws may elevate firms' security consciousness, leading to

[5] We manually checked whether each law is civil law or criminal law in Lexis Advance (US Research System) database.

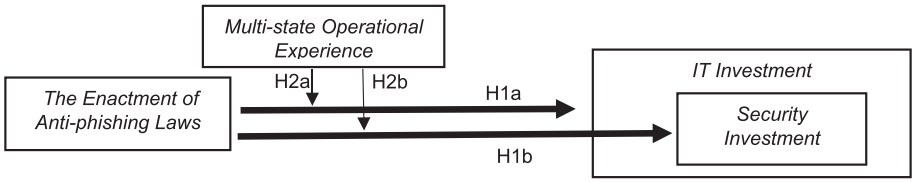


Fig. 1. Conceptual model.

an increased investment in IT infrastructure. These investments represent a strategic move toward a unified approach to security management, recognizing the interdependence of IT and security measures.

H1b. ***Anti-phishing laws motivate firms operating in anti-phishing law states to increase general IT investments.***

2.3. The moderating role of multi-state operational experience

Firms operating across multiple states face a complex regulatory environment, which often necessitates increased investment in IT security, fostering heightened resilience to cyber threats. Three perspectives shape this necessity: the broader spectrum of security risks and experience gained in handling them; prior experience with similar regulations and acts across different jurisdictions; and knowledge sharing among operational units in various states [68,69,70]. The expansive operational footprint exposes multi-state firms to diverse risks, which drives them to develop comprehensive risk assessments and management [69]. With prior experience enabling swift alignment to new regulatory changes, such firms are more likely to pool resources to counter significant risks in more efficient ways. Knowledge sharing within a firm's diverse units leads to the quick dissemination of best practices and effective risk management strategies [68,71,72], emphasizing the need for careful security measures [70]. Consequently, we posit multi-state operation experience has a positive moderating effect on security investment.

H2a. ***Multi-state operation positively moderates the positive effect of the anti-phishing laws on security investments.***

Multi-state operational experience could significantly influence firms' approach to IT investment decisions, extending beyond mere security measures. Such firms are poised to leverage their diverse regulatory exposure to sharpen their IT strategies [61]. This advantage fosters a preventive investment focus, addressing the foundational IT issues rather than transient problems. This broader, insight-driven approach to IT planning echoes the preventative ethos found in prior research on security awareness and comprehensive cybersecurity investment [67]. Thus, we propose that multi-state operation experience has a positive moderating effect on IT investment.

H2b. ***Multi-state operation positively moderates the positive effect of the anti-phishing laws on general IT investments.***

3. Data and methodology

3.1. Data

We obtained annual IT and security investment data from >400,000 organizations located in the United States from Harte-Hanks Market Intelligence. Our data set contains each site's annual IT-related investments, currently installed IT, and anticipated future IT purchases from 2010 to 2017. A site refers to a representative office or a branch office of a firm. Referring to reports by the National Conference of State Legislatures, we identified 23 states with anti-phishing laws. Nineteen states had implemented anti-phishing laws prior to the study period, that is, before 2010.[6] We focused on firms (i.e., treatment firms) that have sites in two states that enacted anti-phishing laws after 2010, which are Michigan (enacted in 2011) and Oregon (enacted in 2015). The laws in these two states do not mandate that firms implement anti-phishing measures or make specific IT investments. Following previous studies utilizing DID model [73,74], we used data from three years (the year before the enactment year, the enactment year, and the year after the enactment year) to study the law's impacts. We aggregated site-level data for a firm in each state to construct firm-state-level data.[7] The firm-state-level data enables us to analyze the effect of the legislation on firms' investment decisions within a state and to conduct additional analysis on the spillover and displacement effects. Based on firms' operating locations, we divided treatment firms into four cases to compare the investment decisions of firms in different locations to test our hypotheses. We chose our control firms from firms operating in the 27 states without anti-phishing laws. Table 1 illustrates these details. We provide the details of the matching process in the next subsection.

Table 2 summarizes the variables in this study. We used the total IT budget to measure IT investments. To measure security investments, we applied principal component analysis (PCA) to aggregate the purchase likelihood score (PLS) of security software and the PLS of antivirus software following the method suggested by Santhanam et al. [75].[8] Antivirus software, which includes email spam filters, is considered to help deter attacks and detect hacking launched by emails [76]. Table 3 shows the summary statistics of the four cases from before and after the enactment of anti-phishing laws.

3.2. Propensity score matching

Although our research context provides a natural experiment setting for examining the impacts of anti-phishing laws, each firm's specific characteristics, such as revenue and firm size, may influence firms' investment decisions. To eliminate the influence of external factors [77] and satisfy the parallel trend assumption [78,79], we applied the propensity score matching (PSM) method to identify the control firms that resembled the treatment firms in all relevant attributes before enactment of the anti-phishing laws. In the matching process, we used data from the year before the law was enacted. We applied a *logit* model when

[6] We begin analysis from 2010 due to the confounding influence of various other cybersecurity regulations enacted in the initial five years post first anti-phishing legislation, which, combined with businesses' adaptation period, might skew results.

[7] For continuous variables, such as the number of employees and estimated revenue, we aggregated the value of a firm's sites in a state, divided the sum by the total number of the firm's sites in the state, and obtained a logarithm. For dummy variables, such as headquarters, if the firm has a site whose value of the variable is one, the aggregate value of these variables equals to one. To facilitate comparison, we standardized all continuous variables in a three-year window for each state.

[8] We also calculated the average of two purchase likelihood scores instead of PCA and arrived at consistent regression results.

Table 1
The treatment groups and control groups in four cases.

Cases	Treatment groups	Control groups
Single-state firms	The firms are only operating in one of the two states with anti-phishing laws passed between 2010 and 2017.	The firms are only operating in one of the states not enacting anti-phishing laws.
Multi-state firms in focal states	The firms are operating in one of the two states with anti-phishing laws passed between 2010 and 2017, and have sites in other states.	The firms are operating in more than one states not enacting anti-phishing laws.
Multi-state firms in other phishing law state	The firms are operating in states enacting anti-phishing laws before 2010, and have sites in other states that include one of the two states with anti-phishing laws passed between 2010 and 2017.	The firms are operating in more than one states not enacting anti-phishing laws.
Multi-state firms in other non-phishing law states	The firms are operating in states not enacting anti-phishing laws, and have sites in other states that include one of the two states with anti-phishing laws passed between 2010 and 2017.	The firms are operating in more than one states not enacting anti-phishing laws.

applying the PSM because the treatment (the enactment of the law) is binary. The variables used in the matching process include the number of employees, revenue, the number of IT staff, and "*hq*" (see Table 2 for further details). We used these control variables in PSM to reflect firm size and firm capability, which may influence firms' subsequent investment decisions. Moreover, headquarters and subsidiaries may have different reactions [80], and subsidiaries' decisions may be influenced differently [81]. We applied exact matching to control "*hq*", which means the variables of the matched group should have the same value as those of the treatment group. We subsequently estimated the propensity score. In each case and industry, we separately matched the firms from the two target states. For example, for single-state firms, we matched the IT industry firms in Michigan with control firms of IT industry, and so on. To identify more control firms and ensure consistency, we applied 1:30 nearest neighbor matching to identify the matched group with the most similar estimated propensity score. Meanwhile, we set the caliper (the maximum allowable difference between two participants) to equal to or <0.05. About 75% of treated firms were successfully matched. After implementing PSM, we ran a *t*-test to check the similarity of the matching results by comparing the means of each matching characteristics variable in the treatment group and the matched group. We also obtained the standardized percentage bias, which measures the percentage of the sample means in the treated and matched samples [82]. As shown in Table 4, the standardized percentage biases were $<10\%$, and the *t*-test results show an insignificant difference between the two groups, indicating the treated and matched samples are quite similar. We created charts to compare the changing trends of the treatment and control groups before the enactment year. The parallel trend assumption argues the treatment and control groups have similar trends in the absence impact from the implementation of anti-phishing laws. Fig. 2 shows the trends of total IT investments and the aggregated security investments of firms in anti-phishing law states and the matched control firms. "*Year*" equals zero if it is the year of implementation of anti-phishing laws. Other cases also show parallel trends between the treatment and control groups.

Table 3
Summary statistics of treatment firms in four cases.

	Before the law was enforced		After the law was enforced	
Variables	Mean	Std. Dev.	Mean	Std. Dev.
Single-state firms				
Security investment	0.6551	0.9371	0.2944	0.8029
IT investment	0.4306	0.6752	0.0227	0.6035
Multi-state firms in focal states				
Security investment	0.2366	0.9221	0.2848	0.9309
IT investment	0.1750	0.7052	0.2664	0.7529
Multi-state firms in the other phishing law states				
Security investment	0.2103	0.9189	0.3894	1.0524
IT investment	0.1528	0.7032	0.4328	0.8347
Multi-state firms in the other non-phishing law states				
Security investment	0.1692	0.8983	0.3237	1.0560
IT investment	0.1272	0.6971	0.3844	0.8627

3.3. Difference in differences model

After applying PSM, we performed the difference in differences (DID) model to test our hypotheses. The DID model can eliminate invariant estimation bias and is widely used to estimate causal relationship [83,84]. We used $Antiph_i$ as the treatment dummy, which equals one if the firm *i* is in a state with an anti-phishing law. We used $timeD_t$ as the time dummy, which equals one if the year *t* is equal to or larger than the year when an anti-phishing law was enacted in a particular state. The interaction term "$Antiph_i \times timeD_t$" captures the interaction effect.

Table 2
The definition of variables.

Type	Name	Definition
Control variable (Treatment independent variable)	Emple	The number of employees
	Reven	Estimated revenue
	IT_staff	The number of IT or IS employees
	Internet_users	The number of employees using the Internet
	Storage	Gigabytes used for storage
	Outsourcing/ SaaS	Whether the third-party services (e.g., data center management, disaster recovery, hardware services, server maintenance) or software-as-a-service (SaaS) being used in the firm
	Hq	Whether the firm has a headquarter in the state.
	install_flag	Whether the firm installed any one security-related software (ID/Access software, security software, third-party firewall services, and third-party intrusion detection services) before the law was published
	Breach	Whether the firm experienced data breaches in that year
	Report	The number of data breach reports in the state
	Numsites	The amounts of sites that the firm is operating in the state
Dependent variables	Security Investment	The average PLS of security software and antivirus software
	IT Investment	The total IT budget
Time dummy	$timeD_t$	Equal to 1 if the year *t* is equal to or larger than the year when the anti-phishing law was acted in a certain state
Treatment dummy	$Antiph_i$	Equal to 1 if the firm *i* is in a state with anti-phishing law

Table 4
Covariate comparison before and after matching.

			Mean		Standardized percentage biases	t-stat(*p*-value)
			Treated	Control		
Michigan	Emple*	Unmatched	−0.1529	−0.3226	17.5	0.000
		Matched	−0.1529	−0.1429	−1.0	0.057
	Reven*	Unmatched	−0.0387	−0.1375	12.0	0.000
		Matched	−0.0387	−0.0414	0.3	0.577
	IT Staff*	Unmatched	0.5727	0.5272	12.4	0.000
		Matched	0.5727	0.5689	1.0	0.042
	Hq	Unmatched	0.1036	0.0860	6.0	0.000
		Matched	0.1036	0.1036	0.0	1.000
Oregon	Emple*	Unmatched	0.3244	−0.0449	42.0	0.000
		Matched	0.3244	0.3115	1.5	0.285
	Reven*	Unmatched	0.2761	−0.0431	30.8	0.000
		Matched	0.2761	0.2785	−0.2	0.882
	IT Staff*	Unmatched	0.0379	−0.3189	37.1	0.000
		Matched	0.0379	0.0136	2.5	0.060
	Hq	Unmatched	0.1277	0.1111	5.1	0.000
		Matched	0.1277	0.1277	−0.0	1.000

Note: * Log transformed and standardized.

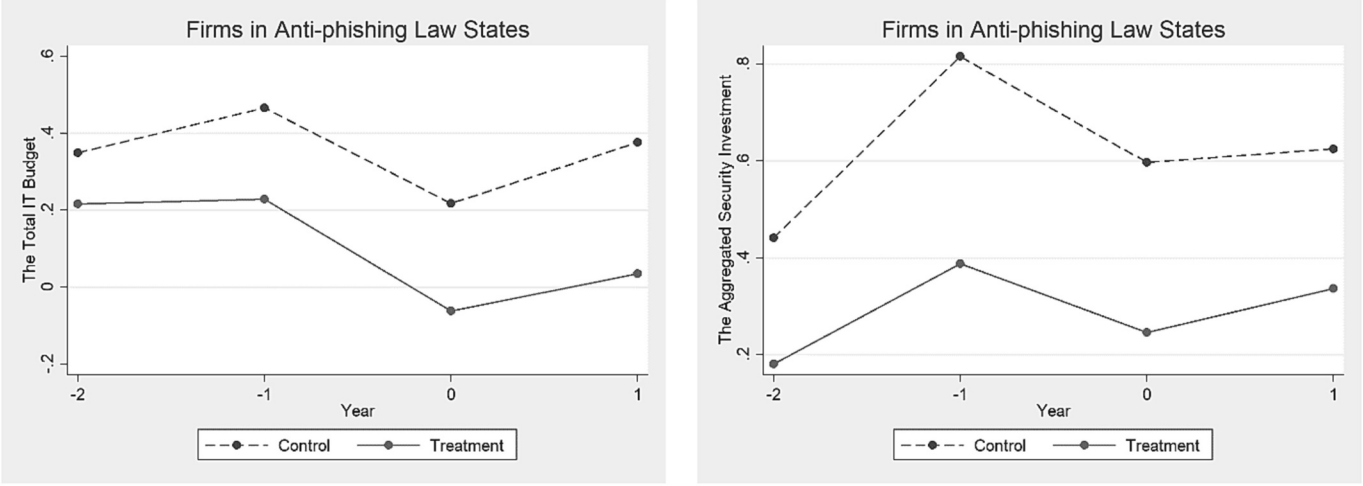


Fig. 2. The change trend of the total IT investment and security investment.

Because our target states enacted anti-phishing laws in different years, we followed Autor [85] and He et al. [86] and built a multiple-period DID model as follows:

$$Dependent\ variables_{i,t} = \beta_0 + \beta_1 Antiph_i \times timeD_t + \gamma_1 Control\ variables_{i,t} + \gamma_2 YearDummy_t + \gamma_3 FirmDummy_i + \varepsilon_{i,t}$$

β_1 is the coefficient estimate of the treatment effect after enactment of an anti-phishing law in a state. It is the main variable of interest in our empirical analyses. We used $YearDummy_t$ to control for time-fixed effects common to all firms and $FirmDummy_i$ to control for mean differences in investments across firms. We included control variables like prior data breach incidents at the state level, as poor security performance may accelerate the enactment of anti-phishing laws. We further controlled the number of sites a firm operates in a state and the firm's present installed software, which may influence a firm's investment strategies when anti-phishing laws are enacted.

4. Results and discussion

4.1. Anti-phishing laws stimulate security investments but dampen IT investments

We first estimated the overall impacts of anti-phishing laws on firms in states that enacted anti-phishing laws. We combined single-state and multi-state firms located in states that enacted anti-phishing laws. Column 1 of Table 5 demonstrates anti-phishing laws had a significant positive effect on firms' security investments, with firms in states that enacted the law increasing their security investments by an additional 0.0205 standard deviations compared to firms in states that did not

Table 5
The impacts of anti-phishing law on IT and security investments.[a]

Results	Dependent variables	
	(1)	(2)
	Security investment	IT investment
Antiph × *timeD*	0.0205**	−0.0795**
	(0.0032)	(0.0025)
Control variables	Yes	Yes
Year dummies	Yes	Yes
Firm dummies	Yes	Yes
N	476,440	476,440
R^2	0.1163	0.1962

Note: Standard errors in parentheses: * denotes $p < 0.05$ and ** denotes $p < 0.01$.

[a] We conducted an additional robustness test clustering standard errors at the firm level, the results are consistent with our main model, which uses the robust estimator of variance

Table 6
The moderating effect of multi-state operation.

Results	Single-state firms		Multi-state firms	
	(1)	(2)	(3)	(4)
	Security investment	IT investment	Security investment	IT investment
Antiph × *timeD*	−0.0005	−0.0986**	0.1287**	0.0127*
	(0.0034)	(0.0027)	(0.0083)	(0.0065)
N	402,386	402,386	74,054	74,054
R^2	0.1233	0.2046	0.0963	0.1667

Note: Standard errors in parentheses: * denotes p < 0.05 and ** denotes $p <$ 0.01. All analyses include control variables, year dummies, and firm dummies.

enact the law ($\beta_1 = 0.0205$, $p < 0.01$). This result indicates the anti-phishing laws raise firms' awareness of security threats, which further drives firms to revisit their security strategies. Firms interpret the legislation's signals as an increasing threat level and react by increasing security investment instead of relying on the government.

In contrast, Column 2 shows firms in states with the anti-phishing law, on average, reduced their IT investments by an additional 0.0795 standard deviations relative to firms in states that did not enact the law ($\beta_1 = -0.0795$, $p < 0.01$). This result shows anti-phishing laws further affect firms' IT investment. Hence, H1a is supported whereas H1b is not. This trend could be attributed to a reactive posture adopted by some firms, aiming to reduce potential losses by minimizing exposure to threats. This posture is often driven by the uncertainties involved in identifying and addressing security weaknesses. Such a strategy is in line with the findings from Li et al. [23], which suggest that higher IT investments might inadvertently lead to increased vulnerabilities exploitable by hackers. Further, Zhang et al. [11] observes that heightened cybersecurity requirements can prompt firms to reassess their IT investment strategies, particularly when these investments heighten the risk of exposing sensitive data. This observation echoes our findings, implying a strategic recalibration of IT and security investments in response to the evolving cybersecurity landscape. The observed negative impact of anti-phishing laws on IT investment may not necessarily be a failure to recognize IT's role in security. Rather, it appears to be a strategic adaptation to reduce risks associated with increased IT vulnerability.

Moreover, the discrepancies between our findings and those of Li et al. [67] could stem from the differences in our analytical focus. Whereas Li et al. [67] delves into actual disclosed firm-level security awareness of materialized data breach incidents, our study centers on examining perceived escalating phishing threats at the state level. This uniform approach to threat perception across firms within a state might explain the noted variance.

4.2. Firms with multi-state operations increase more investments in both security and IT

To estimate the moderating effect of the operational experience of multi-state firms, we compare single-state and multi-state firms' reactions to the enactment of anti-phishing laws after controlling for firm-level characteristics, such as firm size and industry. Columns 1 and 2 in Table 6 reveal that while the anti-phishing laws led single-state firms to slightly decrease their security investments (though not significantly, with $\beta_1 = -0.0005$),[9] they significantly reduced their IT investments by an additional 0.0986 standard deviations ($\beta_1 = -0.0986$, $p < 0.01$). In contrast, Columns 3 and 4 in Table 6 show multi-state firms responded to the laws by significantly ramping up their investments in both security ($\beta_1 = 0.1287$, $p < 0.01$) and IT ($\beta_1 = 0.0127$, $p < 0.05$), increasing them by an additional 0.1287 and 0.0127 standard deviations, respectively. We further conducted a comparison test [87,88] to determine whether the differences between the estimated coefficients of the two groups were significant. The results show significant inter-group differences in both security ($t = -7141.44$, $p < 0.001$) and IT ($t = -7803.28$, $p < 0.001$), indicating the laws' effects on security and IT with respect to single-state firms are smaller than those among multi-state firms. The difference in effects between single-state firms and multi-state firms indicates the moderating role of the multi-state operation. Firms with a larger geographic scope tend to gain more experience in addressing security-related issues, like identifying security loopholes (e.g., lack of multi-factor authentication, failure to configure and update email filters/firewalls) that may lead to phishing attacks and implementing suitable solutions to address the issues. Ultimately, branches with little experience can benefit from such knowledge and invest in security and IT effectively. Therefore, both H2a and H2b are supported.

4.2.1. Spillover effects of anti-phishing laws are stronger among sites located in other states with anti-phishing laws

Analyzing the spillover effects of cybersecurity laws reveals cybersecurity laws' impact on firms' strategies across states, amid known risks of attacker displacement to less-secured assets [18]. In the context of this work, the spillover effect occurs when legislation affects firms in other states in ways like the effect on firms in focal states. For example, firms in focal states and other states both increase (decrease) IT assets, anticipating the security environment will become more secure (risky). In contrast, the displacement effect means the laws have contrary effects on firms in focal states and other states. For example, firms in focal states reallocate their IT assets to other states (or vice versa), anticipating the security environment becoming riskier in the focal states (or other states). Note that, in both cases, "firms" refer to sites of the same enterprise operating in different states.

We first conducted additional analysis on the changes in investments in IT and security among these firms before and after the enactment. According to Table 7, both types of firms—those in states with and without enacted anti-phishing laws—registered significant upticks in IT investments, with increases of 0.0664 standard deviations for firms in non-phishing law states ($\beta_1 = 0.0664$, $p < 0.01$) and 0.0993 standard deviations for firms in phishing law states ($\beta_1 = 0.0993$, p < 0.01). Similarly, security investments rose by 0.0957 standard deviations for firms in non-phishing law states ($\beta_1 = 0.0957$, p < 0.01) and 0.1559 standard deviations for firms in phishing law states ($\beta_1 = 0.1559$, p < 0.01). These significant increases across the board suggest that anti-phishing laws have a ripple effect, influencing multi-state firms even in regions where such laws haven't been legislated. This aligns with our Hypothesis 2, positing that anti-phishing laws intensify the demand for a more secure digital infrastructure, with multi-state firms acting as conduits for disseminating best practices and security knowledge. Furthermore, evidence of the spillover effects indicates a firm-wide scope to

Table 7
The spillover effects of anti-phishing law on IT and security investments.

Results	Multi-state firms in other anti-phishing law states		Multi-state firms in other non-phishing law states	
	(1)	(2)	(3)	(4)
	Security investment	IT investment	Security investment	IT investment
Antiph × *timeD*	0.1559**	0.0993**	0.0957**	0.0664**
	(0.0080)	(0.0055)	(0.0085)	(0.0061)
N	104,375	104,375	90,989	90,989
R^2	0.0782	0.1650	0.0811	0.1584

Notes: Standard errors in parentheses: * denotes $p < 0.05$ and ** denotes $p <$ 0.01. All analyses include control variables, year dummies, and firm dummies.

[9] Our robustness analysis, detailed in Panel B of Table 8, suggests that excluding control states with additional cybersecurity laws reveals a significant positive impact of anti-phishing laws on security investments in single-state firms, potentially indicating an underestimation in our main results.

address security threats among multi-state firms. Thus, multi-state firms interpret the state-level laws as a signal of global threats more than local threats (i.e., within the focal states). In contrast, multi-state firms consider firm-wide efforts to address phishing threats, given adversaries may leverage the interconnectedness of the sites to target the weakest links (i.e., the most vulnerable sites) and compromise the firm. Therefore, firms in both focal states and other states must work together to consolidate their security strategies.

Moreover, the comparison test shows multi-state firms in other anti-phishing law states increase their IT investments ($t = 1253.43$, $p < 0.01$) and security investments ($t = 1611.45$, $p < 0.01$) significantly more than those in non-anti-phishing law states. The results corroborate previous research findings that firms with accumulated technology adoption experience can more effectively shorten the learning curve and reduce uncertainty in adopting new technologies [89,90], thereby promoting IT implementation [91,92]. In contrast, firms without experience may hesitate to invest in IT, and the spillover effect is not so promising. Note we are comparing sites of the same firm operating in different states—hence, the major differences are the experience with earlier enactment of a law and the capabilities nurtured during the process.

4.2.2. Robustness tests

We conducted two robustness tests to validate our main findings. First, we utilized a seemingly unrelated regression (SUR) model [93] to take into account that firms' decision on security investment, and IT investment is correlated instead of being an independent decision. As shown in Panel A of Table 8, all results are consistent with the results in Table 6, except that anti-phishing laws had a positive but not significant effect on multi-state firms' IT investments. The results indicate a less salient effect on IT investments, and such an effect is less than security investments. One possible reason for this is that firms perceive phishing as an immediate and significant threat, thereby maintaining a focus on specific security measures like encryption, two-factor authentication, or intrusion detection systems. Additionally, the strategy within many firms could be more focused on training existing IT personnel to deal with phishing threats, rather than investing in new technologies. This training might not be captured by IT investments. We further conducted a comparison test to determine whether the differences between the estimated coefficients of the two groups were significant. The results show significant inter-group differences in both security ($t = -5241.71$, $p < 0.001$) and IT ($t = -6409.75$, $p < 0.001$), indicating the laws' effects on security and IT with respect to single-state firms are smaller than those among multi-state firms.

Concerning potential influences from other cybersecurity regulations on our DID analysis: our thorough review revealed that only Nevada, among control states, enacted a relevant law in 2011 (the same year as Michigan's Anti-phishing Act), with 11 others doing so within a year before or after. While this might affect the perceived significance of our treatment, it does not undermine our overall findings. To ensure robustness, we conducted an analysis excluding all control states that had introduced any additional cybersecurity laws and regulations during the analysis window. The results from this subsample analysis, presented in Panel B of Table 8, align consistently with those reported in Table 6—except anti-phishing laws had a positive and significant effect on single-state firms' security investments. This variance suggests that our main results might underestimate the anti-phishing acts' impact on single-state firms' security investments. This could be due to other cybersecurity regulations influencing control group firms. By isolating these confounding factors, we offer a clearer assessment of anti-phishing laws' effects on such firms' security investments. Additionally, the comparison test shows multi-state firms increased their security ($t = -1691.99$, $p < 0.01$) and IT investments ($t = -3037.94$, $p < 0.01$) more than single-state firms, which corroborates our main findings.

To construct a more comparable control group, we focused on six states with the closest internet crime complaint rates to each treated state[10] based on the data collected from the Internet Crime Complaint Center [94]. Panel C of Table 8 shows the results of the subsample analysis, and all results are consistent with the results in Table 6—except anti-phishing laws had a negative and not significant effect on multi-state firms' IT investments. This result further emphasizes the distinction between the impacts of anti-phishing laws on security measures and broader IT investments, reflecting firms' prioritization of immediate security threats over general technological enhancements. The comparison test shows multi-state firms increased their security ($t = -3017.36$, $p < 0.01$) and IT investments ($t = -1523.39$, $p < 0.01$) more than single-state firms, which corroborates our main findings.

5. Conclusion

Phishing attacks are known to cause severe financial loss [95,96]. Considering cyberattacks, which include phishing, are ubiquitous and difficult to prevent, developing appropriate countermeasures is extremely important. To achieve this goal, all involved parties must cooperate to improve the overall cybersecurity risk landscape. Previous studies mainly highlight the important role of firms in so doing [45,97]. This study extends the discussion by examining the indispensable role of the government in affecting firms' security investment strategies. We find that firms interpret the enactment of cybersecurity-related policies as a signal of the overall threat landscape and adjust their investment strategies accordingly. Furthermore, firms' interpretations and reactions depend on a firm's characteristics. Specifically, multi-state operation has positive moderating effects in stimulating proactive strategies, such as increasing investments in both IT and security. We thus enrich the understanding of firms' security strategies by revealing the interactions between legislative action and firms' interpretations thereof. Such insights can inform planning and coordination to ensure successful collective efforts in the collective fight against cybersecurity risks. Table 9 summarizes the results of the hypothesis testing.

5.1. Limitations and future research

This study has several limitations: First, it only considers investments in security and IT. Future researchers could further the discussion by investigating the effects of other non-monetary approaches (e.g., adopting new security or information privacy policies, mandating training), if such data are available. Second, because of the limitations of the data sources, we measured firms' information security investments according to purchase intentions rather than actual budgets. However, such measurements do not invalidate our analysis because we did not compare security with IT. Additionally, we considered Michigan and Oregon as treatment groups to rule out other state-level legislations, enhancing the validity of our approach at the cost of generalizability. Future researchers could explore these aspects further, broadening the scope of our findings. Third, in this study, we reveal the laws' signaling effect on the threat landscape. However, because of data limitations, we did not capture the effect of laws as instruments, such as reducing phishing incidents. Future researchers could develop a more comprehensive understanding if such data are available. It would also be interesting to investigate how laws play a mediating role between the threat landscape and firms' behavior changes, which could provide

[10] The six states with the closest internet crime complaints to Michigan were North Carolina, Maryland, Colorado, Ohio, Pennsylvania, and New Jersey; the six states with closest internet crime complaints to Oregon were Kansas, South Carolina, Alaska, Missouri, Nevada, and Wisconsin.

Table 8
Robustness tests results.

Results	All firms		Single-state firms		Multi-state firms	
	(1)	(2)	(3)	(4)	(5)	(6)
	Security investment	IT investment	Security investment	IT investment	Security investment	IT investment
Panel A Seemingly Unrelated Regression Estimation						
Antiph × *timeD*	0.0205**	−0.0794**	−0.0005	−0.0986**	0.1287**	0.0126
	(0.0040)	(0.0029)	(0.0043)	(0.0031)	(0.0120)	(0.0083)
N	476,440	476,440	402,386	402,386	74,054	74,054
Panel B Matched Sample without Enacting Cybersecurity Regulations during the Analysis Window						
Antiph × *timeD*	0.1987**	−0.0132**	0.1913**	−0.0425**	0.2749**	0.0682**
	(0.006)	(0.0045)	(0.0076)	(0.0055)	(0.0115)	(0.0087)
N	170,913	170,913	130,450	130,450	40,463	40,463
R^2	0.084	0.1135	0.0803	0.109	0.1085	0.1400
Panel C Matched Sample with Internet Crime Complaints Rate closest to Treated States						
Antiph × *timeD*	0.1105**	−0.0237**	0.0081	−0.0793**	0.2055**	−0.0039
	(0.0075)	(0.0058)	(0.0103)	(0.0075)	(0.0112)	(0.0089)
N	112,854	112,854	70,376	70,376	42,478	42,478
R^2	0.1088	0.2384	0.1198	0.2783	0.1038	0.1834

Note: Standard errors in parentheses: * denotes $p < 0.05$ and ** denotes $p < 0.01$. All analyses include control variables, year dummies, and firm dummies.

Table 9
Summary of hypothesis results.

H1a: Anti-phishing laws motivate firms operating in anti-phishing law states to increase security investments.	Supported
H1b: Anti-phishing laws motivate firms operating in anti-phishing law states to increase general IT investments.	NOT Supported
H2a: Multi-state operation positively stimulates the positive effect of the anti-phishing laws on security investments.	Supported
H2b: Multi-state operation positively stimulates the positive effect of the anti-phishing laws on general IT investments.	Supported

deeper insights into the complex relationship among legal frameworks, security threats, and organizational responses. Finally, future researchers could consider analyzing the signaling effect of anti-phishing laws on employees and consumers because end-users are on the front line of phishing deterrence and must work to avoid succumbing to phishing schemes. Previous researchers mainly analyzed employees' attitudes toward information security rules implemented within the company [98,99]. Therefore, studying the impact of state and federal laws on employee behavior could provide additional insights into this topic.

5.2. Theoretical contributions

Our findings lend support to the argument regarding the positive effect of cybersecurity laws [52] by revealing the laws' role in raising firms' awareness of threats. In addition, prior studies primarily investigated the effects of cybersecurity laws on firms or attackers that are directly affected by the respective regulations [100,27]. However, the anti-phishing laws we studied are mainly designed to deter attackers; therefore, the reactions we observed from firms—the targets of phishing attacks—demonstrate the indirect effects of such laws. These insights broaden our understanding of the laws' impacts and contribute to this body of research.

We further demonstrate that firms' institutional factors, such as their operational scope, significantly moderate their reactions to anti-phishing laws. Our research enriches the literature by revealing that the effect of regulatory changes on IT and security investments is not uniformly distributed but is contingent on a firm's operational breadth and accumulated experience. Single-state firms adopt a narrow approach by intensifying security measures while curtailing IT investments. In contrast, multi-state firms take a more proactive and comprehensive stance by intertwining security with IT investments. This divergence in investment strategies adds depth to the discourse on how a firm's operational expanse, akin to the concept of threat awareness highlighted by Li et al. [67], is pivotal in informing comprehensive IT and security investment decisions.

This study reveals the intra-firm spillover effects induced by cybersecurity laws, which complement information security literature on the interfirm spillover effects induced by data breach incidents [42,43]. Our findings demonstrate cybersecurity laws can raise firms' sensitivity to security threats and drive firms to consolidate their security at the firm level. Such a holistic view of firms' IT is essential to deter attacks targeted at the firms' IT systems' "weakest links." This is especially true in light of evidence showing cybersecurity laws induce more attacks on digital assets with little protection (i.e., displacement effects on attackers) [100,18]. Thus, future researchers could provide further insights into the reasons behind the different behaviors of firms and attackers.

5.3. Practical contributions

We found some firms proactively increase security and IT investments in response to the enactment of anti-phishing laws. Moreover, we found some firms, such as single-state firms, become reluctant and reactive in investing in security and IT, possibly due to lack of experience and capability in dealing with phishing threats. Previous studies have indicated proactive security investments can improve security performance [97,79], and a reactive approach may hurt firms' future performance in security and business [35,97]. Meanwhile, it should be noted that arresting phishers is generally difficult [101], partly because attackers are adept at adjusting their tactics according to the changing environment. For example, because of COVID-19, more people work from home, which provides opportunities for attackers and causes an increase in cybercrime [1]. Taken together, these present implications for both policymakers and firms.

Policymakers should pay attention to the diverse effects of proposed policies on all stakeholders. To alleviate undesirable side effects (e.g., discouraging IT investment), policymakers should inform stakeholders (e.g., firms' senior management) about the latest threats and encourage firms to implement protections against them. In this regard, policymakers can facilitate knowledge- and experience-sharing workshops/summits to assist inexperienced firms. Firms should recognize the importance of being informed about the practices of peer firms, and the industry as whole, in developing security solutions. Baselining and

benchmarking their own practices with respect to others can facilitate a broader perspective of cybersecurity issues.

CRediT authorship contribution statement

Xiaoxiao Wang: Data curation, Formal analysis. **Wilson Weixun Li:** Data curation, Formal analysis, Methodology. **Alvin Chung Man Leung:** Writing – original draft, Writing – review & editing, Conceptualization, Methodology, Supervision. **Wei Thoo Yue:** Supervision, Writing – original draft, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Appendix A. Additional analysis of the moderating effects of risk landscape and IT capability

A.1. Risk landscape heightens firms' sensitivity to threats signals

Firms operating in a complex risk landscape are considered to have nurtured a sense of threat, prompting risk reduction [69]. This is evident as they become more vigilant with new technology use when faced with elevated security risks [102]. This heightened attentiveness aligns with previous research that correlates higher risk perception with increased preventive actions [69,103]. With cybersecurity regulations indicating an increased threat level, one would expect such firms to respond more robustly.

Specifically, financial and IT sectors, acknowledged as high-risk for phishing [104], were studied to assess how the risk landscape affects their response to anti-phishing laws. A DID analysis differentiated the responses of these high-risk firms from those in low-risk sectors. Panel A of Table A showed that high-risk firms were prompted by anti-phishing laws to boost security investments substantially ($\beta_1 = 0.2181$, $p < 0.01$), yet these laws didn't significantly change their IT investments ($\beta_1 = -0.0046$, $p > 0.10$). Conversely, low-risk firms raised security investments marginally ($\beta_1 = 0.0067$, $p < 0.05$) but decrease IT investments ($\beta_1 = -0.0631$, $p < 0.01$). Comparative analysis confirmed that high-risk firms outpaced low-risk ones in both security and IT investments ($t = 10{,}556.12$ and $t = 3956.97$ respectively, $p < 0.01$) than low-risk firms, underscoring that risk perception deeply influences firm responses to legal changes.

The results showed that high-risk firms do not see IT investment as a burden and thus refrain from curtailing their IT budgets. This suggests an understanding of IT's importance in embedding security measures, although not all such firms can seamlessly merge IT with security in their planning. Facing heightened phishing threats, high-risk firms seem to prefer maintaining their current IT investment while increasing security funding, taking a cautious "wait-and-see" strategy. This reflects an optimistic belief in IT's facilitation paired with practicality toward threats and regulatory changes.

Table A
The moderating effects of risk landscape, and IT capability.

Panel A				
Results	High-risk firms		Low-risk firms	
	(1)	(2)	(3)	(4)
	Security investment	IT investment	Security investment	IT investment
Antiph × *timeD*	0.2181**	−0.0046	0.0067*	−0.0631**
	(0.0100)	(0.0074)	(0.0034)	(0.0025)
N	76,570	76,570	399,870	399,870
R^2	0.1460	0.1907	0.1225	0.2672

Panel B						
Results			IT firms		Financial firms	
			(1)	(2)	(3)	(4)
			Security investment	IT investment	Security investment	IT investment
Antiph × *timeD*	0.2897**	0.0415**	0.0897**	−0.0346*		
	(0.0201)	(0.0089)	(0.0074)	(0.0101)		
N	23,158	23,158	53,412	53,412		
R^2			0.3157	0.3092	0.2958	0.1840

Note: Standard errors in parentheses: * denotes p < 0.05 and ** denotes $p < 0.01$. All analyses include control variables, year dummies, and firm dummies.

A.2. Firms with high IT capability increase investments in both security and IT

Firms with high IT capability are expected to identify and implement suitable solutions against escalating threats. Researchers have found that technology competence positively influences IT adoption [105,106]. Furthermore, increased IT human resources can provide better knowledge to support technology adoption [107,108], and greater technical knowledge can help firms understand how to implement and use IT more effectively in

the organizational context [109]. Therefore, we posit that firms with greater IT capability will proactively respond to anti-phishing laws with heightened security and IT investment.

To assess IT capability's moderating role, we compared IT firms and financial firms.[11] IT firms will likely have higher IT capability than financial firms. Despite a general increase in investment prompted by anti-phishing legislation, IT firms' inherent technological orientation may lead to a greater proclivity for adopting new IT measures. We used DID analysis, as with our primary analysis, to measure this effect among control groups from both sectors. Panel B of Table A reveals that post-law, IT firms' security investments rose ($\beta_1 = 0.2897, p < 0.01$), and while IT investments grew ($\beta_1 = 0.0415, p < 0.01$), financial firms saw a decline ($\beta_1 = -0.0346, p < 0.01$). Comparative tests show that IT firms enhanced their security ($t = 2007.18, p < 0.01$) and IT investments ($t = 991.75, p < 0.01$) significantly more than financial firms. This supports the notion that IT capability amplifies the positive influence of anti-phishing laws on both security and IT spending.

The differential impact of anti-phishing laws between IT and financial firms suggests that the former may not change general IT investments due to their lesser expertise in marrying IT and security strategies. Deloitte's findings corroborate this, indicating a talent gap in cybersecurity within financial firms, which hampers their ability to implement sophisticated cyber defenses [110]. On the other hand, IT-savvy firms might preemptively expand IT outlays to counteract phishing risks, acknowledging IT's integral role in ensuring security. Hence, the presence of IT capability—rather than the mere existence of a risk landscape—plays a pivotal role in utilizing IT resources to safeguard against phishing threats.

Appendix B. Comparisons of anti-phishing acts in michigan and oregon

Table B
Comparisons of anti-phishing acts in michigan and oregon.

	Michigan (Michigan Compiled Laws, Chapter 445. Trade and Commerce § 445.67 A)	Oregon (Oregon Revised Statutes Trade Regulations and Practices § 646 A.808)
Definition of Phishing	(a) Making electronic mail or other communication under false pretenses on behalf of a business without approval, to solicit personal identifying information. (b) Creating or operating a webpage that falsely represents itself as belonging to a business, to solicit personal identifying information. (c) Altering a user's computer settings to cause the user to view a false communication associated with a business, to solicit personal identifying information.	Using a website, electronic mail message, text message, or other electronic means to solicit, request, or induce another person to provide personal information by representing to the other person directly, indirectly, or by implication that the person is a third person, without the third person's knowledge, authorization, and consent.
Enforcement Mechanisms	Attorney General or Interactive Computer Service Provider: May bring a civil action against a person who has violated the Act. Attorney General: May investigate business transactions if there is reason to believe that a person has violated the section.	Prosecuting attorney may bring a suit to restrain unlawful practices, approve assurances of voluntary compliance, and seek civil penalties. Court may award attorney fees.
Penalties	Actual damages, reasonable attorney fees, or $5000 per violation or $250,000 for each day that a violation occurs.	Civil penalties up to $25,000 per violation for willful violations of injunctions, assurances of voluntary compliance, or willful use of unlawful methods. Court may award reasonable attorney fees and costs at trial and on appeal.

Remark: Our search in Thomson Reuters Westlaw database reveals that the Michigan anti-phishing act (MCL 445.67 A) has been cited on 45 occasions, while the Oregon anti-phishing act (ORS 646 A.808) has been referenced 4 times. These citations appear in various primary legal sources, encompassing Cases, Statutes & Court Rules, Appellate Court Documents, and Trial Court Documents, providing substantial evidence of the acts' significance and application within the legal landscape.
Sources: https://codes.findlaw.com/mi/chapter-445-trade-and-commerce/mi-comp-laws-445-67a/
https://codes.findlaw.com/or/title-50-trade-regulations-and-practices/or-rev-st-sect-646a-808.html

As shown in Table B, both states have taken legal measures to address phishing by defining and criminalizing the deceptive electronic practices aimed at obtaining personal information. Michigan's law details specific phishing methods, including false communication and fake webpages, and sets monetary penalties, whereas Oregon's law broadly focuses on false representation and categorizes phishing as an unlawful trade practice, subject to general trade regulations. The penalties in Michigan are explicitly monetary, whereas Oregon refers to general trade practice regulations.

Appendix C. A relative time model of pretreatment trends

To strengthen the validity of our analysis, we augmented our dataset with an additional pre-treatment period of IT investment data. This enabled us to employ a relative time model for a more rigorous examination of the parallel trend assumption. Following previous studies [111,112], the model is specified as follows,

$$\Upsilon_{i,t} = \sum_{\eta=-3}^{0} \beta_\eta Pre_\eta + \sum_{\eta=-3}^{0} Treat_i \times Pre_\eta + \varepsilon_{i,t},$$

where Pre_η is a dummy variable equals one if the current year is η years prior to the treatment. In our analysis, we designated the year preceding the treatment as the baseline period. We plotted the dynamic effects of the interaction terms with 95% confidence intervals. As shown in the Fig. C1, the coefficients of the variables are not significantly different from zero. That is, there is no evidence of significant differences in the pre-treatment trends between the treatment group and control group, thereby validating the parallel trend assumption for IT investments. Given the unavailability of additional pre-treatment security investment data, we drew inferences about security trends from the observed IT investment patterns. While this approach offers insights, we acknowledge this methodological limitation and advise caution in the interpretation of these inferred security trends.

[11] We acknowledge that the regulatory landscapes might be different between the financial and IT industries. Our research into nationwide regulation upon these two sectors suggests there are no other coinciding acts in the observed time period.

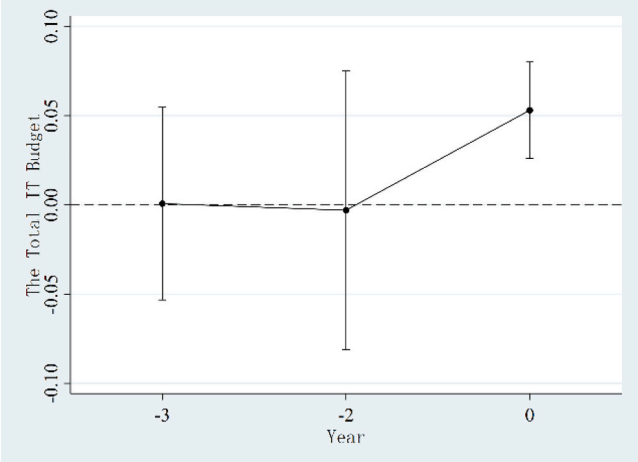


Fig. C1. Estimated coefficients of treatment effects on pre-treatment periods.

References

[1] C. Singleton, S. Carruthers, State of the Phish: IBM X-Force Reveals Current Phishing Attack Trends. https://securityintelligence.com/posts/state-of-the-phish-ibm-x-force-reveals-current-phishing-attack-trends/, 2020 (accessed May 4 2020).

[2] Statista, Volume of Successful Phishing Attacks on Businesses Worldwide in 2021. https://www.statista.com/statistics/1149241/share-organizations-worldwide-phishing-attack/, 2022 (accessed Nov 1st 2022).

[3] Ponemon, The Ponemon 2021 Cost of Phishing Study. https://www.proofpoint.com/us/resources/analyst-reports/ponemon-cost-of-phishing-study, 2021 (accessed Jun 21st 2022).

[4] X. Chen, I. Bose, A.C.M. Leung, C. Guo, Assessing the severity of phishing attacks: a hybrid data mining approach, Decis. Support. Syst. 50 (4) (2011) 662–672.

[5] M. Rothman, Email-Based Threat Intelligence: Industrial Phishing Tactics (New Series). https://securosis.com/blog/email-based-threat-intelligence-industrial-phishing-tactics, 2013 (accessed May 3, 2020).

[6] K. Sheridan, 85% of Data Breaches Involve Human Interaction: Verizon DBIR. https://www.darkreading.com/operations/85–of-data-breaches-involve-human-interaction-verizon-dbir/d/d-id/1341012, 2021 (accessed Jun 21st 2022).

[7] J. Vijayan, Phishing Attacks for Initial Access Surged 54% in Q1. https://www.darkreading.com/risk/phishing-attacks-for-initial-access-surged-q1, 2022 (accessed Jun 21st 2022).

[8] M. Sorensen, The New Face of Phishing. https://apwg.org/the-new-face-of-phishing, 2018 (accessed May 4 2020).

[9] D. Brecht, Phishing: Who is being targeted by phishers?. https://resources.infosecinstitute.com/topic/who-is-being-targeted-by-phishers, 2019 (accessed January 25 2021).

[10] A. Vishwanath, T. Herath, R. Chen, J. Wang, H.R. Rao, Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model, Decis. Support. Syst. 51 (3) (2011) 576–586.

[11] T. Zhang, T. Havakhor, D. Biros, Does cybersecurity slow down digitization? A quasi-experiment of security breach notification laws, in: Proceedings of the 40th International Conference on Information Systems, Munich, Germany, 2019.

[12] K. Maruri, Which States Have Cybersecurity Task Forces?. https://www.govtech.com/security/which-states-have-cybersecurity-task-forces, 2022 (accessed Oct 15 2023).

[13] S. Peltzman, The effects of automobile safety regulation, J. Polit. Econ. 83 (4) (1975) 677–725.

[14] S.P. Peterson, G.E. Hoffer, The impact of airbag adoption on relative personal injury and absolute collision insurance claims, J. Constr. Res. 20 (4) (1994) 657–662.

[15] N. De Silva, B. Torgler, Smoke Signals and Mixed Messages: Medical Marijuana & Drug Policy Signalling Effects. https://www.econstor.eu/handle/10419/214501, 2011.

[16] E. Bishop, The Art Of Impersonation: Can Your Employees Spot A Spear-Phishing Attack?. https://www.forbes.com/sites/forbestechcouncil/2022/04/08/the-art-of-impersonation-can-your-employees-spot-a-spear-phishing-attack/, 2022 (accessed Jun 21st 2022).

[17] E. Chickowski, Why Security Awareness Training Should Be Backed by Security by Design. https://www.darkreading.com/threat-intelligence/why-security-awareness-training-should-be-backed-by-security-by-design/d/d-id/1339538, 2020 (accessed May 14th 2021).

[18] I.P. Png, C.-Y. Wang, Q.-H. Wang, The deterrent and displacement effects of information security enforcement: international evidence, J. Manag. Inf. Syst. 25 (2) (2008) 125–144.

[19] R. Duguay, M. Minnis, A. Sutherland, Regulatory spillovers in common audit markets, Manag. Sci. 66 (8) (2020) 3389–3411.

[20] L. Zhang, Regulatory spillover and workplace racial inequality, Adm. Sci. Q. 67 (3) (2022) 595–629.

[21] C. Peukert, S. Bechtold, M. Batikas, T. Kretschmer, Regulatory spillovers and data governance: evidence from the GDPR, Mark. Sci. 41 (4) (2022) 318–340.

[22] M. Ashraf, The role of peer events in corporate governance: evidence from data breaches, Account. Rev. 97 (2) (2022) 1–24.

[23] H. Li, S. Yoo, W.J. Kettinger, The roles of IT strategies and security investments in reducing organizational security breaches, J. Manag. Inf. Syst. 38 (1) (2021) 222–245.

[24] R. Murciano-Goroff, Do data breach disclosure laws increase firms' investment in securing their digital infrastructure?, in: Proceedings of 18th Annual Workshop on the Economics of Information Security Massachusetts, USA, Boston, 2019.

[25] F. Bisogni, H. Asghari, More than a suspect: an investigation into the connection between data breaches, identity theft, and data breach notification laws, J. Inf. Policy 10 (1) (2020) 45–82.

[26] J. Ju, D. Cho, J.K. Lee, J.H. Ahn, Can it clean up your inbox? Evidence from South Korean Anti-spam, Legislat. Prod. Operat. Manag. 30 (8) (2021) 2636–2652.

[27] S. Jackson, N. Vanteeva, C. Fearon, An investigation of the impact of data breach severity on the readability of mandatory data breach notification letters: Evidence from US firms, J. Assoc. Inf. Sci. Technol. 70 (11) (2019) 1277–1289.

[28] J. Tian, L. Xue, S. Cao, Y. Long, Transparency or perception manipulation? A study of it disclosure tone in the context of data breaches, in: Proceedings of the 14th China Summer Workshop on Information Management, Chongqing, China, 2021, pp. 183–194.

[29] M. Ashraf, J.X. Jiang, I.Y. Wang, Are there Trade-Offs with Mandating Timely Disclosure of Cybersecurity Incidents? Evidence from State-Level Data Breach Disclosure Laws, SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4068575, 2022.

[30] I. Obaydin, L. Xu, R. Zurbruegg, The unintended cost of data breach notification Laws: evidence from managerial bad news hoarding, SSRN (2021), https://doi.org/10.2139/ssrn.3926962.

[31] E. Karanja, J. Zaveri, Ramifications of the Sarbanes Oxley (SOX) act on IT governance, Int. J. Account. Inf. Manag. 22 (2) (2014) 134–145.

[32] W. He, T.W. Tong, M. Xu, How property rights matter to firm resource investment: evidence from china's property law enactment, Organ. Sci. 33 (1) (2022) 293–310.

[33] H. Sakaki, K. Thapar, Trade secrets protection and corporate tax avoidance, J. Acco. Fina. 18 (4) (2018) 114–132.

[34] K.A. Barton, G. Tejay, M. Lane, S. Terrell, Information system security commitment: a study of external influences on senior management, Comput. Secur. 100 (59) (2016) 9–25.

[35] C. Hsu, J.-N. Lee, D.W. Straub, Institutional influences on information systems security innovations, Inf. Syst. Res. 23 (3) (2012) 918–939.

[36] V. Viduto, C. Maple, W. Huang, D. López-Peréz, A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem, Decis. Support. Syst. 53 (3) (2012) 599–610.

[37] J.L. Spears, H. Barki, User participation in information systems security risk management, MIS Q. 34 (3) (2010) 503–522.

[38] D. Straub, R. Welke, Coping with systems risk: security planning models for management decision making, MIS Q. 22 (4) (1998) 441–469.

[39] A. Ahmad, K.C. Desouza, S.B. Maynard, H. Naseer, R.L. Baskerville, How integration of cyber security management and incident response enables organizational learning, J. Assoc. Inf. Sci. Technol. 71 (8) (2020) 939–953.
[40] R. Baskerville, P. Spagnoletti, J. Kim, Incident-centered information security: managing a strategic balance between prevention and response, Inf. Manag. 51 (1) (2014) 138–151.
[41] H.R. Yen, W. Wang, C.-P. Wei, S.H.-Y. Hsu, H.-C. Chiu, Service innovation readiness: dimensions and performance outcome, Decis. Support. Syst. 53 (4) (2012) 813–824.
[42] M.S. Islam, T. Wang, N. Farah, T. Stafford, The spillover effect of focal firms' cybersecurity breaches on rivals and the role of the CIO: evidence from stock trading volume, J. Account. Public Policy 41 (2) (2021).
[43] A.S. Kelton, R.R. Pennington, Do voluntary disclosures mitigate the cybersecurity breach contagion effect? J. Inf. Syst. 34 (3) (2020) 133–157.
[44] H. Li, S. Yoo, W. Kettinger, The changing tides of investments and strategies and their impacts on security breaches, in: Proceedings of the 40th International Conference on Information Systems, Munich, Germany, 2019.
[45] C.Y. Jeong, S.-Y.T. Lee, J.-H. Lim, Information security breaches and IT security investments: impacts on competitors, Inf. Manag. 56 (5) (2019) 681–695.
[46] P. Garg, Cybersecurity breaches and cash holdings: spillover effect, Financ. Manag. 49 (2) (2020) 503–519.
[47] S. Kashmiri, C.D. Nicol, L. Hsu, Birds of a feather: intra-industry spillover of the target customer data breach and the shielding role of IT, marketing, and CSR, J. Acad. Mark. Sci. 45 (2) (2017) 208–228.
[48] N.J. Freeman, J.C. Sandler, The Adam Walsh Act: a false sense of security or an effective public policy initiative? Crim. Justice Policy Rev. 21 (1) (2010) 31–49.
[49] C. Rydenfält, Å. Ek, P.A. Larsson, Safety checklist compliance and a false sense of safety: new directions for research, BMJ Qual. Saf. 23 (3) (2014) 183–186.
[50] H. Grant, H. Crowther, How effective are fines in enforcing privacy?, enforcing privacy: regulatory, Legal Technol. Approach. (2016) 287–305.
[51] J. Wolff, N. Atallah, Early GDPR penalties: analysis of implementation and fines through may 2020, J. Inf. Policy 11 (2021) 63–103.
[52] S. Chai, M. Kim, H.R. Rao, Firms' information security investment decisions: stock market evidence of investors' behavior, Decis. Support. Syst. 50 (4) (2011) 651–661.
[53] L. Khansa, D. Liginlal, The influence of regulations on innovation in information security, in: Proceedings of the 13th America Conference on Information Systems, Keystone, Colorado, USA, 2007, pp. 180–191.
[54] D.J. Houston, L.E. Richardson, Risk compensation or risk reduction? Seatbelts, state laws, and traffic fatalities, Soc. Sci. Q. 88 (4) (2007) 913–936.
[55] M.G. Aboelmaged, Predicting e-readiness at firm-level: an analysis of technological, organizational and environmental (TOE) effects on e-maintenance readiness in manufacturing firms, Int. J. Inf. Manag. 34 (5) (2014) 639–651.
[56] S.E. Chang, C.B. Ho, Organizational factors to the effectiveness of implementing information security management, Ind. Manag. Data Syst. 106 (3) (2006) 345–361.
[57] P.-Y. Chen, G. Kataria, R. Krishnan, Correlated failures, diversification, and information security risk management, MIS Q. 35 (2) (2011) 387–422.
[58] C.W. Hsu, Frame misalignment: interpreting the implementation of information systems security certification in an organization, Eur. J. Inf. Syst. 18 (2) (2009) 140–150.
[59] L. Sun, R.P. Srivastava, T.J. Mock, An information systems security risk assessment model under the Dempster-Shafer theory of belief functions, J. Manag. Inf. Syst. 22 (4) (2006) 109–142.
[60] M. Heidt, J.P. Gerlach, P. Buxmann, Investigating the security divide between SME and large companies: how SME characteristics influence organizational IT security investments, Inf. Syst. Front. 21 (6) (2019) 1285–1305.
[61] P. Loft, Y. He, H. Janicke, I. Wagner, Dying of a hundred good symptoms: why good security can still fail-a literature review and analysis, Enterprise Inform. Syst. 15 (4) (2021) 448–473.
[62] J. D'Arcy, A. Hovav, D. Galletta, User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach, Inf. Syst. Res. 20 (1) (2009) 79–98.
[63] R. Palanisamy, A.A. Norman, M.L. Mat Kiah, BYOD policy compliance: risks and strategies in organizations, J. Comput. Inf. Syst. (2020) 1–12.
[64] H. Li, W.G. No, J.E. Boritz, Are external auditors concerned about cyber incidents? Evidence from audit fees, Auditing: J. Pract. Theory 39 (1) (2020) 151–171.
[65] T.C. Herath, H.S. Herath, J. D'Arcy, Organizational adoption of information security solutions: an integrative lens based on innovation adoption and the technology-organization-environment framework, ACM SIGMIS Database: DATABASE Adv. Inform. Syst. 51 (2) (2020) 12–35.
[66] C.M. Angst, E.S. Block, J. D'Arcy, K. Kelley, When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches, MIS Q. 41 (3) (2017) 893–916.
[67] W.W. Li, A.C.M. Leung, W.T. Yue, Where is IT in information security? The interrelationship among IT investment, security awareness, and data breaches, MIS Q. 47 (1) (2023) 317–342.
[68] L. Argote, B. McEvily, R. Reagans, Managing knowledge in organizations: an integrative framework and review of emerging themes, Manag. Sci. 49 (4) (2003) 571–582.
[69] N.T. Brewer, N.D. Weinstein, C.L. Cuite, J.E. Herrington, Risk perceptions and their relation to risk behavior, Ann. Behav. Med. 27 (2) (2004) 125–130.
[70] E. Gelbstein, IS audit basics: auditing IS/IT risk management, Part 1, in, ISACA J. (2016) 1–3.
[71] V.Z. Chen, J. Li, D.M. Shapiro, International reverse spillover effects on parent firms: evidences from emerging-market MNEs in developed markets, Eur. Manag. J. 30 (3) (2012) 204–218.
[72] D. Liu, Y. Ji, V. Mookerjee, Knowledge sharing and investment decisions in information security, Decis. Support. Syst. 52 (1) (2011) 95–107.
[73] Y. Chen, L. Che, D. Zheng, H. You, Corruption culture and accounting quality, J. Account. Public Policy 39 (2) (2020) 106698.
[74] T. Homonoff, B. Willage, A. Willén, Rebates as incentives: the effects of a gym membership reimbursement program, J. Health Econ. 70 (2020) 102285.
[75] R. Santhanam, D. Liu, W.-C.M. Shen, Research note—gamification of technology-mediated training: not all competitions are the same, Inf. Syst. Res. 27 (2) (2016) 453–465.
[76] S. Purkait, Examining the effectiveness of phishing filters against DNS based phishing attacks, Inform. Comp. Security 23 (3) (2015) 333–346.
[77] K. Xie, Y.-J. Lee, Social media and brand purchase: quantifying the effects of exposures to earned and owned social media activities in a two-stage decision making model, J. Manag. Inf. Syst. 32 (2) (2015) 204–238.
[78] M. Lemmon, M.R. Roberts, The response of corporate financing and investment to changes in the supply of credit, J. Financ. Quant. Anal. 45 (3) (2010) 555–587.
[79] Y. Zhang, C. Zhang, Y. Xu, Effect of data privacy and security investment on the value of big data firms, Decis. Support. Syst. 146 (2021) 113543.
[80] N. Nohria, S. Ghoshal, Differentiated fit and shared values: alternatives for managing headquarters-subsidiary relations, Strateg. Manag. J. 15 (6) (1994) 491–502.
[81] T.C. Ambos, J. Birkinshaw, Headquarters' attention and its effect on subsidiary performance, Manag. Int. Rev. 50 (4) (2010) 449–469.
[82] P.R. Rosenbaum, D.B. Rubin, Constructing a control group using multivariate matched sampling methods that incorporate the propensity score, Am. Stat. 39 (1) (1985) 33–38.
[83] H.-L. Chang, Y.-C. Chou, D.-Y. Wu, S.-C. Wu, Will firm's marketing efforts on owned social media payoff? A quasi-experimental analysis of tourism products, Decis. Support. Syst. 107 (2018) 13–25.
[84] J. Schreyögg, M.M. Grabka, Copayments for ambulatory care in Germany: a natural experiment using a difference-in-difference approach, Eur. J. Health Econ. 11 (3) (2010) 331–341.
[85] D.H. Autor, Outsourcing at will: the contribution of unjust dismissal doctrine to the growth of employment outsourcing, J. Labor Econ. 21 (1) (2003) 1–42.
[86] S. He, J. Peng, J. Li, L. Xu, Impact of platform owner's entry on third-party stores, Inf. Syst. Res. 31 (4) (2020) 1467–1484.
[87] M. Keil, B.C. Tan, K.-K. Wei, T. Saarinen, V. Tuunainen, A. Wassenaar, A cross-cultural study on escalation of commitment behavior in software projects, MIS Q. 24 (2) (2000) 299–325.
[88] C.-H. Tan, J. Sutanto, C.W. Phang, A. Gasimov, Using personal communication technologies for commercial communications: a cross-country investigation of email and SMS, Inf. Syst. Res. 25 (2) (2014) 307–327.
[89] P.-F. Hsu, S. Ray, Y.-Y. Li-Hsieh, Examining cloud computing adoption intention, pricing mechanism, and deployment model, Int. J. Inf. Manag. 34 (4) (2014) 474–488.
[90] B. Ramdani, D. Chevers, D.A. Williams, SMEs' adoption of enterprise applications: a technology-organisation-environment model, J. Small Bus. Enterp. Dev. 20 (4) (2013) 735–753.
[91] Y. Alshamaila, S. Papagiannidis, F. Li, Cloud computing adoption by SMEs in the north east of England: a multi-perspective framework, J. Enterp. Inf. Manag. 26 (3) (2013) 250–275.
[92] B.S. Neo, Factors facilitating the use of information technology for competitive advantage: an exploratory study, Inf. Manag. 15 (4) (1988) 191–201.
[93] S. Dewan, F. Ren, Information technology and firm boundaries: impact on firm risk and return performance, Inf. Syst. Res. 22 (2) (2011) 369–388.
[94] IC3, Internet Crime Complaint Center. https://www.ic3.gov/Home/AnnualReports, 2023 (accessed Aug 1st 2023).
[95] G. Aaron, R. Rasmussen, Global Phishing Survey. https://apwg.org/globalphishingsurvey, 2017 (accessed Jun 1st 2022).
[96] I. Bose, A.C.M. Leung, Do phishing alerts impact global corporations? A firm value analysis, Decis. Support. Syst. 64 (2014) 67–78.
[97] J. Kwon, M.E. Johnson, Proactive versus reactive security investments in the healthcare sector, MIS Q. 38 (2) (2014) 451–471.
[98] B. Bulgurcu, H. Cavusoglu, I. Benbasat, Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness, MIS Q. 34 (3) (2010) 523–548.
[99] M. Siponen, A. Vance, Neutralization: new insights into the problem of employee information systems security policy violations, MIS Q. 34 (3) (2010) 487–502.
[100] K.-L. Hui, S.H. Kim, Q.-H. Wang, Cybercrime deterrence and international legislation: evidence from distributed denial of service attacks, MIS Q. 41 (2) (2017) 497–523.
[101] V.A. Kini, Anti-Phishing Legislation: Catch Me if You Can?. https://www.theglobaltreasurer.com/2005/10/03/anti-phishing-legislation-catch-me-if-you-can, 2005 (accessed May 5 2020).
[102] K.A. Salleh, L. Janczewski, Security considerations in big data solutions adoption: lessons from a case study on a banking institution, Proc. Comp. Sci. 164 (2019) 168–176.
[103] L.-C. Chen, D. Farkas, An investigation of decision-making and the tradeoffs involving computer security risk, in: Proceedings of the 15th America Conference on Information Systems, California, USA, San Francisco, 2009, pp. 610–617.
[104] M. Vergelis, N. Demidova, T. Shcherbakova, Spam and phishing in Q2. https://securelist.com/spam-and-phishing-in-q2-2021/103548/, 2018 (accessed Jun 21st 2022).

[105] T. Oliveira, M.F. Martins, Understanding e-business adoption across industries in European countries, Ind. Manag. Data Syst. 110 (9) (2010) 1337–1354.
[106] K. Zhu, K.L. Kraemer, J. Dedrick, Information technology payoff in e-business environments: an international perspective on value creation of e-business in the financial services industry, J. Manag. Inf. Syst. 21 (1) (2004) 17–54.
[107] H.-S. Kim, Y.-G. Kim, C.-W. Park, Integration of firm's resource and capability to implement enterprise CRM: a case study of a retail bank in Korea, Decis. Support. Syst. 48 (2) (2010) 313–322.
[108] K. Zhu, K.L. Kraemer, Post-adoption variations in usage and value of e-business by organizations: cross-country evidence from the retail industry, Inf. Syst. Res. 16 (1) (2005) 61–84.
[109] S.K. Lippert, C. Govindarajulu, Technological, organizational, and environmental antecedents to web services adoption, Commun. IIMA 6 (1) (2006) 14.
[110] S. Friedman, Taking Cyber Risk Management to the Next Level. https://www2.deloitte.com/us/en/insights/topics/cyber-risk/cyber-risk-management-financial-services-industry.html, 2016 (accessed Jun 21st 2022).
[111] Z. Li, Y. Hong, Z. Zhang, The empowering and competition effects of the platform-based sharing economy on the supply and demand sides of the labor market, J. Manag. Inf. Syst. 38 (1) (2021) 140–165.
[112] Z. Li, C. Liang, Y. Hong, Z. Zhang, How do on-demand ridesharing services affect traffic congestion? The moderating role of urban compactness, Prod. Oper. Manag. 31 (1) (2022) 239–258.
[113] H. Cavusoglu, B. Mishra, S. Raghunathan, The value of intrusion detection systems in information technology security architecture, Inf. Syst. Res. 16 (1) (2005) 28–46.

Xiaoxiao Wang received her Ph.D. from Department of Information Systems in City University of Hong Kong. Her research interests focus on information security, innovation, and firm investment strategy. Her research works were published in the proceedings of PACIS 2019 and presented in BIGS 2019.

Wilson Li is a Lecturer in Department of Information Systems and Business Analytics, Deakin Business School, Deakin University. He received his Ph.D. in Management Information Systems from City University of Hong Kong. His current research focuses on information security, data protection and cybersecurity regulation and information systems governance. His research works were published in MIS Quarterly and Internet Research, and presented in academic conferences such as INFORMS, PACIS, WeB and BIGS.

Alvin Leung is an Associate Professor in the Department of Information Systems, City University of Hong Kong. He received his Ph.D. in Information Management from McCombs School of Business, the University of Texas at Austin. His research interests include IT business value, financial technology, technology-mediated learning, and information security. His work has appeared in MIS Quarterly, Information Systems Research, Journal of Management Information Systems, Management Science, Decision Support Systems and other journals.

Wei Thoo Yue is a Professor of Management Information Systems in the Department of Information Systems at City University of Hong Kong. He received his Ph.D. in Management Information Systems from Purdue University. Prior to joining City University of Hong Kong, he was a faculty member at the University of Texas, Dallas. His research interests focus on the economic and operational aspects of information security and information systems. His work has appeared in Management Science, Information Systems Research, MIS Quarterly, Journal of Management Information Systems, Decision Support Systems, and other journals.