CityU
香港城市大學
City University of Hong Kong
專業 創新 胸懷全球
Professional·Creative
For The World

CityU Scholars

Where is IT in Information Security? The Interrelationship among IT Investment, Security Awareness, and Data Breaches

Li, Wilson Weixun; Leung, Alvin Chung Man; Yue, Wei Thoo

Published in:
MIS Quarterly

Published: 01/03/2023

Document Version:
Final Published version, also known as Publisher's PDF, Publisher's Final version or Version of Record

License:
CC BY

Publication record in CityU Scholars:
Go to record

Published version (DOI):
10.25300/misq/2022/15713

Publication details:
Li, W. W., Leung, A. C. M., & Yue, W. T. (2023). Where is IT in Information Security? The Interrelationship among IT Investment, Security Awareness, and Data Breaches. *MIS Quarterly*, *47*(1), 317-342. https://doi.org/10.25300/misq/2022/15713

Citing this paper
Please note that where the full-text provided on CityU Scholars is the Post-print version (also known as Accepted Author Manuscript, Peer-reviewed or Author Final version), it may differ from the Final Published version. When citing, ensure that you check and use the publisher's definitive version for pagination and other details.

General rights
Copyright for the publications made accessible via the CityU Scholars portal is retained by the author(s) and/or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights. Users may not further distribute the material or use it for any profit-making activity or commercial gain.

Publisher permission
Permission for previously published items are in accordance with publisher's copyright policies sourced from the SHERPA RoMEO database. Links to full text versions (either Published or Post-print) are only available if corresponding publishers allow open access.

Take down policy
Contact lbscholars@cityu.edu.hk if you believe that this document breaches copyright and provide us with details. We will remove access to the work immediately and investigate your claim.

Download date: 01/03/2024

MIS Quarterly

RESEARCH NOTE

WHERE IS IT IN INFORMATION SECURITY? THE INTERRELATIONSHIP AMONG IT INVESTMENT, SECURITY AWARENESS, AND DATA BREACHES[1]

Wilson Weixun Li
Deakin Business School, Deakin University
Burwood, AUSTRALIA {wilson.li@deakin.edu.au}

Alvin Chung Man Leung
Department of Information Systems, College of Business, City University of Hong Kong
Kowloon, HONG KONG {acmleung@cityu.edu.hk}

Wei Thoo Yue
Department of Information Systems, College of Business, City University of Hong Kong
Kowloon, HONG KONG {Wei.T.Yue@cityu.edu.hk}

Data breaches can severely damage a firm's reputation and its customers' confidence. Firms must therefore continuously invest in security measures to prevent such breaches. However, the effectiveness of security investment has been questioned by both practitioners and academics. We illustrate the bidirectional dynamic relationship between information technology (IT) investment and data breaches moderated by threat and countermeasure security awareness using an eight-year panel of 311 U.S.-listed firms to provide empirical evidence that threat awareness broadens firms' scope for addressing data-breach issues by investing more in IT than in security. Countermeasure awareness equips firms with sufficient knowledge and experience to ensure effective implementation of IT, which provides more comprehensive protection than security investment alone. Our results suggest that firms should evolve beyond the reactive mindset of solely upgrading security and begin nurturing both threat awareness and countermeasure awareness to address the underlying IT system issues that are the cause of data breaches.

Keywords: Security investment, IT investment, security awareness, threat awareness, countermeasure awareness, data breach, panel vector autoregression model

Introduction

In recent years, firms have rapidly increased their security budgets. However, the effects of the added funds appear to be marginal and data breaches continue to proliferate. This casts doubt on the effectiveness of investments in security protection in general, which range from activities such as conducting information security training to implementing identity access management technologies. Many security experts caution that firms are not spending their security budgets effectively and some researchers have suggested that poorly integrated security solutions can lead to diminishing security investment returns (Angst et al., 2017; Sen & Borle, 2015).

IT investment is considered to play an increasingly critical role in security for addressing fundamental or root-cause issues that lead to poor security management[2] (Chen et al., 2011; Hsu, 2009; Pang & Tanriverdi, 2022; Sun et al., 2006). Security professionals have suggested that inefficiencies and flaws in the underlying IT environment are to blame and

[1] H. Raghav Rao was the accepting senior editor for this paper. Nirup Menon served as the associate editor. Wei Thoo Yue is the corresponding author.
[2] These may include, for example, human errors in manual processes, legacy, or incompatible systems.

©2023. The Authors. This work is licensed under a Creative Commons Attribution 4.0 International License.
(https://creativecommons.org/licenses/by/4.0/)

advise scrutinizing IT investments after breach incidents to enhance the effectiveness of integrating IT and security objectives (DiPietro, 2018; Glavach, 2017; Morgan, 2015). However, others have found that it is insufficient to rely on IT investment to address security issues due to the fact that some firms treat security investment and IT investment as independent decisions (Coltman et al., 2015; Pang & Tanriverdi, 2022; Van Niekerk & Von Solms, 2010). Accordingly, it has been suggested that *security awareness* is the missing link in integrating comprehensive security solutions (Boss et al., 2009; Spears & Barki, 2010; Straub & Welke, 1998). Hence, we posit that security awareness serves a moderating role between firms' IT and security resource allocations and their security outcomes.

Security awareness—broadly defined as a unified sense of awareness of security threats and proper countermeasures at the senior management level—is vital to maintaining a firm's security. With a better understanding of security threats and potential business impacts, firms' key stakeholders are more willing to cooperate with security policies and proactively protect the security environment by exchanging information and providing support (Johnson & Goetz, 2007; Ruighaver et al., 2007). In addition, comprehensive mindfulness of threats also enhances a firm's security mindset by assessing a wider range of investments (e.g., IT investments) related to data breaches, which promotes changes in both security and IT investment strategies (Loft et al., 2021; Soomro et al., 2016; Straub & Welke, 1998). Moreover, a holistic understanding of countermeasures can help a firm explore practical solutions to avoid conflicts between security and business (Herath et al., 2020; McEvilley, 2002).

Using panel data for 311 U.S.-listed firms from 2010 to 2017, we examine the bidirectional relationships between IT investment, security investment, and data breaches using the panel vector autoregression (PVAR) model. We follow the approach proposed by Gordon et al. (2010) to capture the effect of security awareness, in which a firm's voluntary disclosure of security activities indicates its security awareness. We suggest that such awareness—categorized into threat and countermeasure awareness—strengthens the communications and collaborations between security and business functions, which helps develop a clear view of the threat landscape and devise suitable and practical solutions through IT and security. Thus, security awareness moderates the relationship between IT and security investment and security performance; we measure the latter measure in terms of the number of data breaches.

We find that threat awareness stimulates firms to invest more in IT than in security after data breaches, possibly because threat awareness broadens the scope at which firms can assess security threats, which makes them more likely to identify root causes stemming from the underlying IT systems. As a result, firms allocate more resources to IT rather than upgrading specific security measures. We also find that with more IT investment and a higher level of countermeasure awareness, firms can curb data breaches more effectively. One explanation is that countermeasure awareness presents firms with a holistic view of their interconnected IT systems so that firms can consolidate different resources to support the effective implementation of IT and security. Furthermore, redesigning IT systems to align with business and security provides more comprehensive protection than solely upgrading security measures. Accordingly, we demonstrate that security awareness plays an essential moderating role in firms' decisions on IT resource allocation and security performance.

Our work makes several significant contributions to the growing body of literature on information security. First, we show that security performance is much more complex than previously acknowledged and identify the value of IT investment in terms of security performance. Second, we enrich the understanding of security awareness by breaking it down into the awareness of threats and countermeasures. We further demonstrate that these types of awareness play different but ongoing roles in firms' decisions on IT resource allocation. Finally, our finding that security awareness moderates IT investment but not security investment adds a novel insight to the literature.

Our study also has significant managerial implications. First, we show that IT should not be ignored when formulating information security solutions; indeed, our results suggest that information security should be considered as a factor in all IT-related decisions. Second, we demonstrate the importance of the different types of security awareness and offer insights into why some organizations have lower levels of security when they lack such awareness. Our findings demonstrate that threat awareness presents firms with a comprehensive view of the threat landscape and changes firms' mindset by adopting a wider scope of security solutions. More importantly, countermeasure awareness helps firms implement these solutions to address the fundamental issues of the underlying IT systems effectively.

The remainder of the paper is organized as follows. We present our hypothesis development in the next section. In the section that follows, we describe the data and model specifications in detail. Finally, we discuss our empirical findings and their implications. We present our literature review in Appendix A; the results of various robustness checks in Appendices B, C, D, and E; and examples of security awareness in Appendix F.

Hypothesis Development

Security Investment: Mindset Trap in Treating the Symptoms

Firms often invest in security solutions when facing cybersecurity threats; such actions may influence future security performance. Addressing cybersecurity risk, conceptually speaking, involves a dyadic interaction between firms' investments and their security performance. In this study, we use breach incidents as the trigger for investments in security and IT. These investments, in turn, may affect the outcome of future breach incidents.

Although data breaches or other security incidents should motivate firms to enhance their security practices, previous studies reveal that firms often manage security with symbolic gestures. One contributing factor is that, without the benefit of hindsight, firms tend to take a myopic view of security incidents (Angst et al., 2017; Kwon & Johnson, 2014). Moreover, firms are under constant pressure to fulfill requirements from external entities such as regulatory bodies and business partners, which leads them to neglect fundamental security issues (Herath et al., 2020; Kwon & Johnson, 2018; Nazareth & Choi, 2015). Hence, the ways in which firms manage security threats may not be consistent with their fundamental security objectives due to common mindset errors.

Even when firms understand the need to achieve specific security objectives, the extant literature shows that not all types of security investment lead to better security performance (Panel A of Table A1 in Appendix A). Several factors explain these failures to implement effective security measures: (1) the misallocation of security budgets (Sen & Borle, 2015), (2) the inability to integrate security measures into organizational systems and processes effectively (Li et al., 2021; Tanriverdi et al., 2020), and (3) the inability to align employees with organizational security objectives (Kwon & Johnson, 2014; Li et al., 2021). These failures demonstrate that there may be gaps in how firms leverage resources to develop workable security solutions.

In summary, incoherent objectives and actions may lead to discrepancies between perceived and actual effectiveness in security investment; that is to say, firms often fall into the trap of treating the symptoms but not the root causes of data breaches.

IT Investment: A Comprehensive Approach

Data breaches trigger firms to invest in security solutions, which may include not only security measures but also general IT investments. Previous studies have argued that incorporating IT into security solutions broadens firms' perspectives in dealing with security issues and hence serves as an essential component in effective security management (Chen et al., 2011; Hsu, 2009; Sun et al., 2006). Several facts further support this argument. First, IT aids firms in identifying and addressing vulnerabilities that arise from an inefficient and flawed IT design (Heidt et al., 2019; Herath et al., 2020; Hole & Netland, 2010; Kraemer et al., 2009; Loft et al., 2021). Second, creating strong IT infrastructures helps firms better integrate IT and security objectives (D'Arcy et al., 2009; Palanisamy et al., 2022; Silic et al., 2017). Third, various IT solutions can nurture a security culture among different business units when they are deployed to address security issues (Herath et al., 2020). In fact, security issues have often been found to be rooted in flawed IT implementation in practice (e.g., system glitches, misconfiguration, and human error/negligence). Nurturing a security culture can make employees more careful when planning, implementing, and using IT.

Previous studies (Kayworth & Whitten, 2010; Loft et al., 2021; Soomro et al., 2016) have highlighted the importance of aligning IT with security arrangements. Such studies note that information security is a process rather than a product, which requires constant alignment with the underlying environments (e.g., enterprise architecture) (Loft et al., 2021). Misalignment between IT and security objectives may weaken the deterrent effect of security measures (Li et al., 2020). Furthermore, some suggest that a security mindset in IT implementation is necessary to bridge the disconnect between IT and security initiatives.[3] Such a belief is consistent with previous research findings that an organizational-security mindset is a prerequisite for enhancing the effectiveness of security measures (Angst et al., 2017; Chang & Ho, 2006; Hsu et al., 2012).

In summary, previous research reveals that IT and the effectiveness of security measures are closely connected. Hence, treating IT and security as separate processes may not be ideal. Instead, a holistic and diverse understanding of the interplay between IT and security issues can more effectively address the fundamental causes of security breaches.

[3] Practitioners coined this as "security by design" to reflect the importance of considering security even in the earliest stages of IT design (Lovejoy, 2020).

The Moderating Role of Security Awareness

Our literature review suggests that designing suitable security measures requires a diverse knowledge base to connect a firm's security environment with its business processes (Boss et al., 2009; Spears & Barki, 2010; Straub & Welke, 1998). Such a comprehensive understanding is often referred to as a state of security awareness, which assists firms in aligning their evolving security objectives in dynamic business landscapes (Olt et al., 2019; Straub & Welke, 1998). A notable mechanism is that having security awareness can facilitate communication and collaboration among internal and external stakeholders in the internal audit and governance processes (Gelbstein, 2016; Ruighaver et al., 2007). For instance, security awareness can help improve IT and security governance (AlGhamdi et al., 2020; Fazlida & Said, 2015; Johnston & Hale, 2009) and strengthen collaboration between internal audit functions (IAF) and other business units (Islam et al., 2018; Steinbart et al., 2018). Security awareness can also encourage firms to prepare for adversarial actions through better internal audit and governance implementations (Berkman et al., 2018; Kark et al., 2009; Kwon & Johnson, 2014), which is often achieved by integrating sound security policies and practices into business routines (Barton et al., 2016; Hsu et al., 2012).

Previous studies have generally treated security awareness as a one-dimensional construct (Hsu et al., 2012; Kwon et al., 2012), thus overlooking the extensive role of security awareness in moderating firms' reactions to breach incidents. Essentially, there is a lack of research on the relationship between security awareness and the dyadic interaction between firms' investments and their security. In view of this gap, we argue that effective investments to address breach incidents involve two different kinds of security awareness. The first is that the organization is aware of potential threats and vulnerabilities related to possible breach incidents (Hanus & Wu, 2016; Herath et al., 2020; Zhuang et al., 2020); the second is that firms possess a deep understanding of IT solutions to devise appropriate security solutions (Gopalakrishna-Remani et al., 2019; Ravichandran, 2005).

We borrow concepts from user-level studies that draw on protection motivation theory (PMT) (Hanus & Wu, 2016; Olt et al., 2019) to further classify security awareness into threat awareness (TA) and countermeasure awareness (CA). TA encompasses businesses' mindfulness of local threats in their processes; such attention enables firms to identify their valuable digital assets and to promote effective security measures to protect them (Fenz et al., 2014; Olt et al., 2019). CA is a thorough understanding of the solutions available to address security concerns effectively. This, in turn, helps firms deploy appropriate solutions to meet their business objectives (Straub & Welke, 1998) by infusing the most suitable technologies into their business activities (Claybaugh et al., 2017; Malhotra & Galletta, 2005; Purvis et al., 2001).

By differentiating the concepts of TA and CA, our study expands on the conventional understanding of how security awareness (or a security mindset) moderates the relationship between data breaches and IT (or security) investment. Figure 1 presents the conceptual model.

The Moderating Effect of Threat Awareness.

Data breaches (and their accompanying losses) may trigger firms to rethink their future investment strategies regarding IT and security (Lee & Larsen, 2009; Say & Vasudeva, 2020). As mentioned above, security awareness may affect senior management's evaluation of investments. Out of the two types of security awareness, TA is more directly associated with senior management's assessment of security-related threats (Olt et al., 2019). Therefore, different levels of TA may exert varying degrees of moderating effects on the relationship between data breaches and IT (or security) investment.

With strong TA, firms may adopt a more comprehensive approach to assessing their security threats (symptoms) and associated environment (Herath et al., 2020). Such an approach may extend the assessment beyond security measures adopted by the firm to the IT environment where security measures reside (Johnson et al., 2007). In fact, some security issues may not be easily addressed by fixing the symptoms (e.g., adopting the latest security measures) (Loft et al., 2021). The root causes of data breaches (e.g., human errors in manual processes; legacy or incompatible systems) may stem from the underlying IT environment (Cram et al., 2019; Kraemer et al., 2009). Therefore, strong TA may trigger firms to scrutinize the underlying IT systems to identify the root causes rather than examining the related security measures alone. This argument is supported by Straub and Welke (1998), who found that a comprehensive understanding of the threat landscape, which includes extensive examination of existing IT systems, is necessary to effectively address security problems. Thus, firms may devote more resources to improving the core IT systems with particular attention paid to the prevention or mitigation of future data breaches. This type of reaction differs from a narrow focus on allocating more security resources to specific security measures to solve particular security problems.

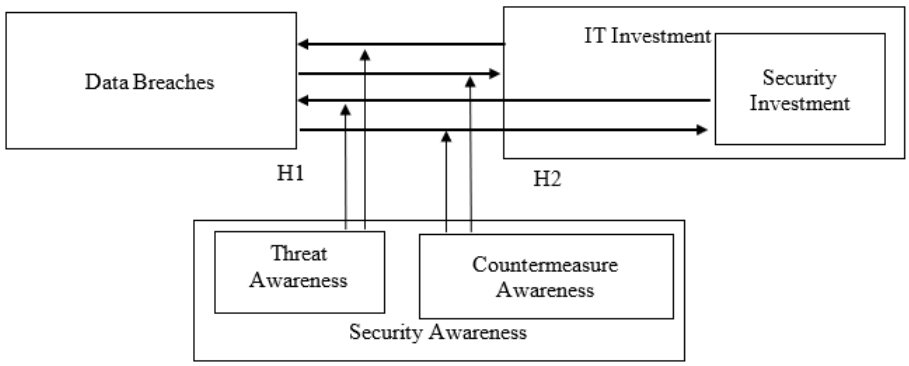

Figure 1. Conceptual Model

Differences in TA may trigger firms to adopt different IT investment strategies when facing significant security problems (e.g., data breaches) (Loft et al., 2021; Soomro et al., 2016). Hence, we posit that TA motivates firms to allocate more resources toward IT investment than security investment as mindful firms could be more inclined to consider an extensive range of solutions, including IT. To this effect, we propose the following hypothesis:

H1: *Threat awareness positively stimulates the positive effect of data breaches on IT investment more than security investment.*

The Moderating Effect of Countermeasure Awareness

Devoting more resources (IT or security) to deterring security-related threats may lead to a greater reduction in data breaches. However, the degree of effectiveness may hinge on senior management's awareness of appropriate resources or solutions to neutralize threats. This argument is supported by previous research, which shows that without awareness of the complexity and interdependency of these interconnected systems, firms may be unable to fully address security risks even if senior managers dedicate considerable resources to mitigating such risks (Li et al., 2021; Tanriverdi et al., 2020). In this case, CA may be the missing link that helps firms effectively leverage IT and security resources to devise practical solutions (Herath et al., 2020; McEvilley, 2002). We argue that CA equips firms with the necessary knowledge and experience to consolidate their resources (e.g., human resources, knowledge management), such that IT and security implementation is more effective in preventing security problems (Herath et al., 2020; Hirt & Swanson, 2001; Purvis et al., 2001; Somers & Nelson, 2004).

We also posit that IT investments made by countermeasure-aware firms deter more breaches than security investments for various reasons. First, IT revamped with embedded security features may provide more comprehensive protection than vulnerable systems with security patches (Baskerville, 2009; Herath et al., 2020). Furthermore, redesigning IT to align business and security is more likely to resolve the root causes of security issues, e.g., human errors or security violations, than solely upgrading security measures (Sarkar et al., 2020; Silic & Lowry, 2020; Tarafdar et al., 2015). Thus, we propose the following hypothesis:

H2: *Countermeasure awareness positively stimulates the negative effect of IT investment on data breaches more than the effect of security investment.*

Data and Methodology

Data Description

We collected three types of data—data breaches, security investment budgets, and IT investment budgets—from different sources, which are discussed below.

Source of Data Breach Information

We collected data on reported breaches from the Privacy Rights Clearinghouse (PRC) database,[4] which has been widely used in similar research (Angst et al., 2017), and aggregated all breach

[4] The PRC provides information on data breaches related to a range of organizations (businesses, educational institutions, governments, the military, medical providers, and nonprofit organizations) from the U.S., which are collected mainly from the list servers of the Open Security Foundation (DataLossDB.org), Databreaches.net, PHI Privacy and NAID, and the California Attorney General's list of data breaches.

incidents for each firm on an annual basis in our analysis. We also used the number of breached records[5] to better capture the seriousness and magnitude of the data breach events.

Source of Security and IT Investment Information

We obtained the data on IT investment budgets from the Computer Intelligence Technology Database (CiTDB) of Harte-Hanks Market Intelligence. This database contains detailed annual IT investment information, including that of Fortune 1,000 companies gathered through surveys and interviews. The database has been widely used in information systems (IS) studies (Arora & Forman, 2007; Forman, 2005), and we aggregated these site-level data to the firm level. We used the weighted average of IT budgets with the number of employees at the site level as a weight to characterize the overall IT investment made by a firm. In the same way, we used the weighted average of security budgets[6] with the number of employees at the site level as a weight to measure security investment.

Data and Measures of Firms' SA

To capture security awareness at the senior management level, we collected annual 10-K reports from firms listed by the Securities and Exchange Commission (SEC). For each firm with an annual 10-K report, we checked whether the firm had disclosed any security threats or identified any risk-related factors or security update activities in the corresponding fiscal year. The self-disclosure of information-security activities underscores the senior executives' level of attention to protecting information assets and positively affects firms' market value (Berkman et al., 2018; Chai et al., 2011; Gordon et al., 2010). Steelman et al. (2019) used a similar approach to capture firms' emphasis on or commitment to IT. Similarly, a firm's voluntary disclosure of security activities can serve as a proxy for its security awareness at the senior management level.

Following the methods used by Gordon (2010), we identified annual 10-K reports that contained at least one cybersecurity-related keyword.[7]+ Based on previous studies (Berkman et al., 2018; Steelman et al., 2019), we further constructed the level of awareness by counting the number of keywords in the reports. We regard the voluntary disclosure of security threats in the 10-K reports as a sign that the firm was aware of potential security threats, which we refer to as TA. The interaction term *Breach* × *TA* thus captures the moderating effects of TA on a firm's efforts. The voluntary disclosure of security activities in the 10-K reports also signals a firm's commitment to actively preventing security breaches, which we refer to as CA. Thus, the interaction term *IT (Security)* × *CA* captures the moderating effect of CA when firms implement IT (security) investment. Examples of security awareness as seen in the annual reports in terms of threats and countermeasures are provided in Appendix F.

We further collected data on exogenous variables, including firms' total assets and advertising expenditures from Compustat, search volume growth rate[8] from Google Trends, and the number of issued patents from Google Patent, which were used to control for firm size (Dewan et al., 1998) and performance (Aral & Weill, 2007), online popularity (Burtch et al., 2013),[9] and capability (Vandaie & Zaheer, 2014), respectively.

After matching the data from the various sources, we identified 160 U.S. firms (treated firms) that experienced breaches between 2010 and 2017 and for which data were available across all the datasets during the observed period. To control for selection bias and ensure a consistent model estimation, we used propensity score matching (PSM) to construct a control group of firms with no breaches from 2010 to 2017. PSM has been widely used in other IS research (Chang & Gurbaxani, 2012) to control for the selection bias issues caused by observed heterogeneity. For example, fundamental differences between treatment and control firms, such as online popularity and firm size, may affect the likelihood that firms will be breached and influence their investment budgets in both IT and security.

[5] Like other recent empirical studies on cybersecurity (Angst et al., 2017; Kwon & Johnson, 2014; Sen & Borle, 2015), our reliance on reported breaches is a limitation of our study. We have found no way to collect data on breaches that have not been discovered or disclosed and there is currently no empirical method that can be applied to address this issue appropriately (Angst et al., 2017). PRC is a reliable data source as it collects data from various sources and has been widely used in other studies, as previously mentioned. We also believe that there is little chance that firms would hide breach incidents, as breach notification laws have been enacted in 44 U.S. states as of 2010 (Greenberg, 2013).

[6] As security budgets are not available in CiTDB, we calculate security budgets in the following way: $Security\ Budget_i = \sum_{j=1}^{K} \frac{Number\ of\ Employees_{i,j}}{Total\ Number\ of\ Employees_i} \times \left(\frac{Security\ Software\ Adopted_{i,j}}{Software\ Adopted_{i,j}} \times Software\ Budget_{i,j} + \frac{Security\ Services\ Adopted_{i,j}}{\text{IT-related Services Adopted}_{i,j}} \times \text{IT-related Services Budget}_{i,j} \right)$, where i refers to Firm *i* with *K* business sites and *j* refers to Site *j* of Firm *i*. For a robustness check, we followed previous security investment studies (Angst et al., 2017; Kwon & Johnson, 2014) and used the number of implemented security measures as the measure of security investment; the results were consistent (as shown in Appendix B).

[7] The keyword lists are shown in Table A2 of Appendix A. Over 80% of our original keywords are covered in widely used cybersecurity-related parlance (Ayala, 2016). We believe this result indicates a strong justification for our selected keywords.

[8] We calculate the Google Trends search volume growth rate for each firm by dividing the difference between a firm's Google Trends search volume in the current year added to its search volume in the previous year by the firm's search volume in the previous year. Thus, we can compare the variations in online popularity among all firms in our sample.

[9] With a larger internet presence, a firm can become a more obvious and attractive target for adversaries (Ransbotham & Mitra, 2009).

Following the standard PSM procedure (Chen et al., 2015; Kim et al., 2016), our control firms were selected from among firms having no data breaches during the observed time period (2010-2017). In the matching process, we used data for the year before the breach incident. We applied a probit model where the dependent variable (whether a firm has been breached from 2010 to 2017) is binary. We used variables such as total assets, advertising expenditures, and Google Patent and Google Trend ratios to control for firm size, firm capability, and online popularity, which may influence the likelihood of data breaches. To obtain more accurate estimation results of firms' reactions, we matched firms by industry (based on the Fama-French 10 industries). We then calculated the estimated propensity score based on the regression results of the probit model and used the nearest-neighbor method to match each treated firm with a counterpart that has never been breached. Meanwhile, we set the caliper (the maximum allowable difference between two participants) to equal to or less than 0.05. Over 90% of treatment firms were successfully matched, providing a total of 166 control firms and 145 treatment firms as the final sample.[10]

After implementing PSM, we ran a *t*-test to check the similarity of the matching results by comparing the means of each matching characteristic variable in the treatment and matched groups. As shown in Table 1, the PSM matching variables between the two groups are not significantly different from each other after matching, suggesting that they are statistically balanced.

We summarize the industry distribution of our whole sample based on the Fama-French 10 industries.[11] The top three industries are Services & Finance (41.5%), Business Equipment (22.5%), and Wholesale & Retail (15.8%). Utility firms and services and finances firms have the highest levels of TA and CA, respectively, while energy sector firms (oil, gas, and coal extraction and products) have the lowest levels of TA and CA. Over one third of the observations have an above-average level of TA, while 29% of the observations have an above-average level of CA. Table 2 provides the summary statistics and Table 3 shows the Pearson's correlation matrix.

Model

The Rationale for Using a Panel Vector Auto-regression Model.

A vector auto-regression (VAR) model can be used to test models with undefined or hard-to-define restrictions, such as causality (Backus, 1986). Each variable is expressed as a linear function of its own lagged values, the lagged values of other variables, and an uncorrelated error term. Panel VAR (PVAR) adds a cross-sectional dimension to the standard VAR model and can be used to examine the relationships in a system of interdependent variables without imposing ad hoc model restrictions (Dewan & Ramaprasad, 2014). Exogenous variables that influence endogenous variables can also be incorporated into the model, allowing us to address unobserved individual heterogeneity (Chen et al., 2015), thus complementing the PSM approach, which, as mentioned above, only considers observed heterogeneity issues.

Endogenous relationships (two-way causal relationships)—such as that between a firm's number of data breaches, its IT (or security) investment budget, and its level of security awareness—may exist between variables. For example, previous studies have documented that prior breach experience affects the likelihood of future breaches and investment decisions through the following competing mechanisms: (1) signaling a lower level of security control, thus attracting more adversaries and increasing the likelihood of a breach (Wang et al., 2015), and (2) revealing vulnerabilities, thus inducing firms to implement proper solutions and reducing the likelihood of a breach (Lankton et al., 2021). PVAR is an appropriate tool because it can model bidirectional and dynamic relationships and requires no restrictions or causal assumptions. This approach has been used to resolve endogeneity issues in prior IS research (Carlo et al., 2012). The model specification is as follows:

$$y_{i,t} = \begin{pmatrix} Breach_{i,t-s} \\ Investment_{i,t-s} \\ Security\ Awareness_{i,t-s} \\ Interaction\ Term_{i,t-s} \end{pmatrix} = \sum_{s=1}^{p} \Phi_s \cdot \begin{pmatrix} Breach_{i,t-s} \\ Investment_{i,t-s} \\ Security\ Awareness_{i,t-s} \\ Interaction\ Term_{i,t-s} \end{pmatrix} + \beta \cdot \begin{pmatrix} Revenue_{i,t} \\ Google\ Trend\ Ratio_{i,t} \\ Expenditure\ in\ Advertisement_{i,t} \\ Number\ of\ Patents\ Issued_{i,t} \end{pmatrix} + \varepsilon_{i,t}, \quad (1)$$

where $y_{i,t}$ = *(*$Breach_{i,t}$*,* $Investment_{i,t}$*,* *Voluntary Disclosure*$_{i,t}$*,* *Interaction Term*$_{i,t}$*)* is a four-element column vector for firm i at time t containing the log transformation of the dependent variables, *Investment* refers to security investment or IT investment, *Voluntary Disclosure* represents levels of security awareness of either threats or countermeasures, *Interaction* refers to either *Breach* × *TA* or *Investment* × *CA*, Φ_s and β are the matrices of the slope coefficients for the endogenous variables, and p is the number of lags.

[10] We have 2,411 firm-year observations and 10 variables in the regression, which satisfies the rule of thumb that ten times more observations than the number of variables is sufficient for multiple regression analysis, as noted in the extant literature (Sekaran & Bougie, 2003).

[11] The summary table is available upon request.

Table 1. Summary Statistics and Covariate Comparison Before and After Matching

Variable		Mean		*t*-stat (*p*-value)
		Treated	Control	
Total asset	Unmatched	9.115	6.898	13.20 (0.000)
	Matched	8.898	8.750	0.66 (0.508)
Advertising expenditure	Unmatched	2.544	0.850	13.67 (0.000)
	Matched	2.186	2.496	-1.05 (0.296)
Google patents	Unmatched	1.036	0.546	5.20 (0.000)
	Matched	0.884	0.810	0.49 (0.627)
Google trend ratio	Unmatched	-0.050	-0.068	0.71 (0.477)
	Matched	-0.045	-0.052	0.21 (0.835)
FF1	Unmatched	0.031	0.046	-0.87 (0.387)
	Matched	0.028	0.028	0.00 (1.000)
FF2	Unmatched	0.006	0.028	-1.66 (0.096)
	Matched	Nil	Nil	Nil
FF3	Unmatched	0.038	0.138	-3.67 (0.000)
	Matched	0.041	0.041	-0.00 (1.000)
FF4	Unmatched	0.013	0.047	-2.04 (0.041)
	Matched	0.014	0.014	0.00 (1.000)
FF5	Unmatched	0.206	0.153	1.85 (0.065)
	Matched	0.207	0.207	-0.00 (1.000)
FF6	Unmatched	0.044	0.019	2.25 (0.025)
	Matched	0.034	0.034	0.00 (1.000)
FF7	Unmatched	0.188	0.082	4.79 (0.000)
	Matched	0.186	0.186	-0.00 (1.000)
FF8	Unmatched	0.075	0.097	-0.93 (0.352)
	Matched	0.076	0.076	-0.00 (1.000)
FF9	Unmatched	0.019	0.049	-1.76 (0.079)
	Matched	0.021	0.021	0.00 (1.000)
FF10	Unmatched	0.381	0.342	1.05 (0.295)
	Matched	0.393	0.393	-0.00 (1.000)

Note: FF1~FF10 refers to 10 industry categories defined by Fama-French10. FF2 shows nil after matching because after matching, there are no firms in the industry of FF2.

Table 2. Summary Statistics

Variable	Obs	Mean	*SD*	Min	Max	Remark
Breach	2,411	1.643	62.075	0.000	3000.000	Total breaches (in million records)
IT	2,411	33.174	201.683	0.000	5882.421	Weighted average IT budget (in millions of dollars)
Security	2,411	0.126	1.039	0.000	25.423	Weighted average security budget (in millions of dollars)
Threat awareness (TA)	2,411	35.756	38.438	0.000	336.000	Firm's voluntary disclosure of security threats (total number of keywords)
Countermeasure awareness (CA)	2,411	17.937	35.943	0.000	336.000	Firm's voluntary disclosure of security countermeasures (total number of keywords)
Total assets	2,411	39279.14	171314.5	11.487	2261780.000	Firm's total assets (in millions of dollars)
Ad	2,411	126.532	427.433	0.000	6317.000	Advertising expenditure (in millions of dollars)
GTrGrt	2,411	-0.021	0.297	-0.731	5.579	Growth rate of Google Trend volume
Patents	2,411	22.068	105.4763	0.000	944.000	Number of patents issued

Table 3. Correlation Table

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
(1) Breach^	1.000										
(2) IT^	-0.031	1.000									
(3) Security^	-0.032	0.151	1.000								
(4) (Breach × TA)^	0.637	-0.025	-0.024	1.000							
(5) (IT × CA)^	-0.012	0.099	-0.002	-0.009	1.000						
(6) (Security × CA)^	-0.021	-0.042	0.121	-0.017	0.167	1.000					
(7) TA^	0.064	0.014	0.120	0.066	0.002	-0.003	1.000				
(8) CA^	0.019	-0.035	-0.035	0.002	-0.031	-0.050	0.264	1.000			
(9) Total assets	-0.035	0.039	0.013	-0.025	0.007	-0.010	-0.001	0.123	1.000		
(10) Ad	-0.030	0.011	-0.034	-0.007	-0.013	0.012	-0.057	0.045	0.134	1.000	
(11) GTrGrt	0.043	-0.043	0.016	0.026	-0.034	0.026	-0.008	0.032	0.035	-0.028	1.000
(12) Patents	-0.003	-0.058	-0.028	-0.004	0.032	-0.023	-0.036	-0.028	0.011	0.003	-0.005

Note: ^ indicates log transformed and Helmert transformed, as required by the PVAR model.

Following previous PVAR studies, we selected the optimal lag order based on information criteria such as Akaike's information criterion (AIC), the Bayesian information criterion (BIC), and the Hannan and Quinn information criterion (HQIC). The lowest AIC, BIC, and HQIC statistics across 1-4 year lags indicate that the one-year lag is the best lag order for model estimation, as shown in Table 4. The four-element column vector for firm i at time t ($AT_{i,t}$, *Google Trend Ratio*$_{i,t}$, *Expenditure in Advertisement*$_{i,t}$, *Number of Patents Issued*$_{i,t}$) controls for firm size, online popularity, advertising expenditure, and firm capability. To control for heteroskedasticity (Kim et al., 2016), we used robust standard errors clustered by industry.

To examine the stationarity of this panel dataset, we conducted the Phillips-Perron (1988) test and the augmented Dickey-Fuller (ADF) (1979) test. The null hypothesis is that all panels contain unit roots. The results in Table 5 show that the null hypothesis was rejected for each time-series variable; there is no unit root and all of the endogenous variables are stationary.

Following prior research using PVAR (Dewan & Ramaprasad, 2014), we also conducted the Granger (1969) causality test. The null hypothesis is that the excluded variable cannot Granger-cause the equation variable. As Table 6 shows, the interaction term *Breach* × *TA* can Granger-cause *IT* investment ($p < 0.10$), and the interaction term *IT* × *CA* can Granger-cause *Breach* ($p < 0.01$). The results show clear evidence of a bidirectional relationship among data breach, investment, and the interaction terms (*IT* × *CA*, *Breach* × *TA*), which supports the use of a dynamic model to address the endogeneity issues between the explanatory variables.

Results and Discussion

With Heightened Threat Awareness, Data Breaches Stimulate More IT Investment than Security Investment

We first examine the interrelationship among security investment, data breaches, and security awareness when controlling for firm size, advertising expenditure, online popularity, and capability. Table 7 shows the estimation results.

The lagged *Breach* × *TA* has a negative and nonsignificant effect (coefficient: -0.002) on security investment, as shown in Column 2 of Table 7.[12] Our explanation is that these firms may attempt to avoid complicating their systems and refrain from adding further unnecessary security measures. Alternatively, they may explore a wider range of solutions and identify more efficient approaches (Spears & Barki, 2010). Sen and Borle (2015) suggest that firms should rely on both technical solutions and administrative or physical controls to fully enhance their security capabilities, which are typically not covered by conventional security measures.

[12] Our subsample analysis of hi-tech firms shows that *Breach* × *TA* has a positive and significant effect on security investment. This finding corroborates with prior findings (e.g., Zhuang et al., 2020) that the security vulnerabilities or even the awareness of the vulnerabilities are prerequisites but not sufficient conditions of firms' incremental adoption of security measures. Firms need to be equipped with IT expertise and supporting resources such as IT infrastructure to identify proper security measures, which high-tech firms are more likely to do, as they have more experience in IT management.

Table 4. Panel VARX Lag Order Selection

Lag order	AIC	BIC	HQIC
1	12.162	17.998	14.317
2	12.018	18.962	14.607
3	13.064	21.603	16.284
4	13.199	24.236	17.422

Note: Model selection measures calculated using pvar2(option soc) for first to fourth-order panel VAR

Table 5. Unit Root Tests

Time series	Fisher-type test (PP)	Fisher-type test (ADF)
	Inverse logit *t* (*p*-value)	Inverse logit *t* (*p*-value)
Breach	-17.623(0.000)	-52.126(0.000)
IT	-16.452(0.000)	-28.877(0.000)
Security	-18.357(0.000)	-17.031(0.000)
Countermeasure awareness (CA)	-49.312(0.000)	-55.250(0.000)
Threat awareness (TA)	-16.352(0.000)	-20.304(0.000)
(Breach × TA)	-21.059(0.000)	-40.164(0.000)
(IT × CA)	-32.559(0.000)	-44.821(0.000)
(Security × CA)	-58.175(0.000)	-58.815(0.000)

Note: All variables are Log transformed and Helmert transformed as required by PVAR model

Table 6. Granger Causality Tests

Results	Caused by			
	Breach	IT	Breach × TA	IT × CA
Breach	-	0.038(0.845)	1.093(0.296)	25.027(0.000)
IT	1.107(0.293)	-	2.733(0.098)	0.090(0.765)

Note: The results reported are Wald-$\chi 2$ statistics with *p*-values in parentheses. Granger causality tests are performed with 1 lag for consistency with the PVAR models.

Table 7. The Interrelationship of Security (IT) Investment, Security Awareness, and Data Breaches

Independent variable	Dependent variable			
	(1)	(2)	(3)	(4)
	Breach	Security	Breach	IT
L.Breach	0.503**(0.223)	-0.004(0.011)	0.499*(0.277)	-0.512(0.487)
L.(Breach × TA)	-0.251(0.219)	-0.002(0.021)	-0.261(0.250)	1.121*(0.678)
L.Security	-0.010(0.279)	0.845***(0.234)		
L.(Security × CA)	-0.030(0.054)	0.084*(0.050)		
L.IT			0.023(0.119)	-0.143(1.960)
L.(IT × CA)			-0.043***(0.009)	0.128(0.427)
L.CA	-0.007(0.013)	0.022(0.019)	-0.167***(0.035)	0.481(2.746)
L.TA	-0.021*(0.012)	0.002(0.008)	-0.018(0.019)	-0.042(0.164)
N	1789	1789	1789	1789

Note: Standard errors are in parentheses; p-values are represented by * $p < 0.10$, ** $p < .05$, and *** $p < 0.01$; L indicates a lagged one-year term; Column 1 and Column 2 are from the same PVAR model, wherein security investment, breaches, security awareness, and the interaction terms are the endogenous variables; Column 3 and Column 4 are from the same PVAR model, wherein IT investment, breaches, security awareness, and the interaction terms are the endogenous variables; the estimation results for all control variables are omitted due to space limitations. *Google Trend Growth Rate* has a positive and significant effect (coefficient: 0.021; standard error: 0.006) on *Breach*; *Google Trend Growth Rate* has a negative and significant effect (coefficient: -0.035; standard error: 0. 011) on *Security investment.*

Next, we investigate the interrelationship among IT investment, data breaches, and security awareness. As shown in Column 4 of Table 7, the lagged *Breach* × *TA* has a positive and significant effect (coefficient: 1.121, $p < 0.10$) on IT investment, suggesting that firms with greater TA invest more in general IT after identifying security vulnerabilities. This result highlights the importance of using IT to address security incidents for threat-aware firms, which commonly occurs in practice. For example, after its high-profile breach in 2013, Target Corp. underwent a massive upgrade of its in-store payment infrastructure to support the use of the more-secure chip-and-PIN credit cards. A comparison test[13] of the corresponding coefficients between security investment and IT investment indicates a significant between-group difference (t = 70.02; p < 0.001). The coefficient of *Breach* × *TA* for IT investment is significantly larger than that for security investment, which supports H1 that threat-aware firms invest more in IT than in security measures after data breaches. Our findings are consistent with a recent Deloitte report, which suggests that security measures based on traditional network perimeters become less effective as information systems become more complex and the boundaries among employees, customers, and vendors become blurred. A vMware report found that more than 25% of breaches are caused by operating systems vulnerabilities and that 83% of respondents consider gaps in IT operations as security threats, thus indicating that firms are paying more attention to the root causes of security issues from the design and operational perspectives of IT.

With Heightened Countermeasure Awareness, IT Investment Deters More Data Breaches than Security Investment

We further investigate the impact of security and IT investment on breaches, and, as Column 1 of Table 7 indicates, the lagged *Security* × *CA* shows no significant effect on breaches (coefficient: -0.030). Thus, there is no evidence that security investment alone can effectively deter data breaches, even when firms are security aware. Although surprising, this result gives credence to doubts regarding the effectiveness of independent security spending as higher budgets do not necessarily lead to fewer data breaches (Sen & Borle, 2015). Our findings support the argument that security investment is only one factor, often a secondary factor, in an overall security solution strategy. As indicated in our main hypotheses, we further investigate whether general IT investment is the primary method of improving security performance.

In examining the impact of general IT investment on security performance, we found that CA has an important moderating role. The lagged *IT* × *CA* shows a significantly negative effect (coefficient: −0.043, $p < 0.01$) on *Breach*, as shown in Column 3 of Table 7. Thus, the importance of CA is demonstrated by the fact that firms with higher levels of CA outperform those with lower levels of CA in preventing data breaches. Their awareness means that they attempt to minimize the potential negative effects of data breaches through their IT solutions. This demonstrates not only the importance of IT solutions in combatting security incidents but also, more importantly, that security awareness plays a significant role in achieving this objective. We conducted a comparison test to compare the coefficients between the security and the IT models. The result indicates a significant between-group difference (t = -10.04; p < 0.001). The coefficient of the lagged *IT* × *CA* on breaches is significantly larger than that of the lagged *Security* × *CA*, which supports H2 that countermeasure-aware firms exploit IT, rather than security measures alone, to effectively combat data breaches. The 2020 EY Global Information Security Survey echoes our findings by suggesting that firms' security strategies should go beyond the defensive and reactive approach to proactively participate in digital transformation programs. A Deloitte report points out that such close alignment between security and IT functions could help firms stay ahead of adversaries and address security risks faster and more efficiently. However, the EY survey also found that very few executives understand the role of security as a business innovation enabler and that less than one third of firms consider cybersecurity in the early planning stages of new business initiatives. Therefore, it remains an urgent priority to nurture security awareness among senior managers, which in turn enhances the internal audit and security governance process. As a result, the firms can align overall IT strategies with security objectives and address the discrepancy between security and business.

Additional Analysis for Robustness Checks

We further conducted various robustness checks to confirm our results. First, we reestimated our model by using the alternative measurement of security investment. The results are consistent with our main findings, as shown in Appendix

[13] The comparison test was performed based on the formulae employed in Keil et al. (2000). Tan et al. (2014) also used the same approach to compare coefficient estimates of different models. The formulae are provided as follows: $S = \sqrt{\frac{N_1-1}{N_1+N_2-2} \times {SE_1}^2 + \frac{N_2-1}{N_1+N_2-2} \times {SE_2}^2}$, $t = \frac{PC_1-PC_2}{S \times \sqrt{\frac{1}{N_1}+\frac{1}{N_2}}}$, where S refers to the estimator for the variance, t refers to the t-statistic with $(N_1 + N_2 - 2)$ degrees of freedom, N_i is the sample size of dataset used in model i, SE_i is the standard error of coefficient estimate in model i, and PC_i is the coefficient in model i.

B. Second, we used alternative measurements of security awareness by using the number of distinct keywords to better capture the breadth of topics covered in the disclosure. The results are consistent with our main findings and are shown in Appendix C. Third, we conducted a subsample analysis with the generalized method of moments (GMM) model—widely used in previous IS research to address endogeneity issues in the panel data (Kim & Viswanathan, 2018) to corroborate our main results. These results are consistent with our main findings and are shown in Appendix D. Fourth, we include IT investment and security investment simultaneously in the same model to address the potential endogeneity issues between IT and security investments. The results are consistent with our main findings, as shown in Appendix E. Finally, following prior IS research (e.g., Cheng et al., 2016), we winsorized the breach data at 1% to control for potential outliers and found that our results are robust.

Conclusion

Data breaches have significantly negative impacts on firm value (Gwebu et al., 2018), thus prompting firms to carefully consider data protection and increase their security investment budgets. However, breaches persist, which reveals that there may be shortcomings in the mainstream security strategies. This study illustrates the dynamic relationship between IT (security) investment, security awareness, and data breaches: threat-aware firms react to security breaches by allocating more resources to IT than to security alone and countermeasure-aware firms use IT solutions more effectively to reduce data breaches.

Theoretical Contributions

Our findings have important implications for the information security literature. First, our results demonstrate that threat-aware firms scrutinize the impact of general IT strategies on security protection after data breaches. We enrich the existing information-security literature by offering empirical evidence to support the necessity of examining firms' security efforts beyond the scope of conventional security measures, which advances the recent discussions on the narrowness of the existing definition and measurement of security investment in empirical studies (Kwon & Johnson, 2014; Li et al., 2021). Our work contributes to the security management literature by identifying TA as the factor that alters firms' security mindsets so that they no longer consider security and IT to be mutually exclusive. This is a novel insight, as prior research has confined the reach of security awareness to the domain of security strategies (Hsu et al., 2012; Kwon et al., 2012; Olt et al., 2019). Notably, our study disrupts this inertial thinking by demonstrating that TA extends to IT strategies.

Second, we demonstrate that sufficient knowledge or experience of countermeasures enables effective implementation of IT investment, which provides more comprehensive security protection than security investment. This finding enriches our understanding of the effect of IT investment on security outcomes, which was highlighted as a burden in prior empirical studies (Li et al., 2021; Zhang et al., 2019). Our results highlight the importance of CA in devising practical solutions to align IT and security objectives. Our results also challenge the assumption that security performance is a direct consequence of security investment (Gordon & Loeb, 2002; Wang et al., 2008). The insignificant effect of security investment, regardless of CA, is already supported by some prior findings (Loft et al., 2021; Sen & Borle, 2015). We deepen the understanding of the ineffectiveness of conventional security measures by contrasting security investment with IT investment. Our results reveal that security measures likely treat only symptoms, whereas a thorough assessment and revamping of the underlying IT systems can address the root causes of security issues.

Third, our findings show that security awareness leads to firms' emphasizing IT strategies as the foundation of addressing security issues. Hence, the "security-by-antiquity" approach[14] may not be the best strategy—firms should instead focus on IT modernization (Pang & Tanriverdi, 2022). This insight echoes observations that security awareness can enhance the internal auditing and security governance process (Gelbstein, 2017; Hartmann & Carmenate, 2021; Ruighaver et al., 2007). Thus, security awareness facilitates better protection through IT and security investments that are responsive to the threat and protection environment.

Altogether, our work closes the loop between investment decisions and security performance and sheds light on the mechanisms underlying the role of security awareness in improving firms' security performance. Unlike recent studies that focus on other types of static or non-security-centric moderating factors (Angst et al., 2017; Kwon & Johnson, 2018), we demonstrate the importance of TA and CA in firms' ongoing attempts to address the root causes of security issues with the comprehensive assessment of the threat landscape and the effective implementation and integration of IT solutions.

[14] A "security-by-antiquity" mindset means that firms consider legacy IT systems to be more stable and believe that upgrading to modernized systems is risky and insecure. Such a mindset leads to the trap of ignorance of the vulnerabilities caused by legacy systems. Pang and Tanriverdi (2022) found that spending in IT modernization addresses legacy issues effectively; however, it is unclear how to motivate firms to recognize this.

Managerial Contributions

From the managerial perspective, our findings on the importance of IT solutions for security performance have been echoed by many security practitioners. According to a recent survey, many frontline security-related duties are conducted by organizations' IT personnel, implying that IT teams can fundamentally influence security performance. The business value of IT investment has increasingly been linked to security performance through the enforcement of cybersecurity requirements for IT service and product providers, including cybersecurity in due-diligence considerations in M&A transactions. Our empirical results extend these arguments by demonstrating the importance of instilling security awareness among IT personnel to effectively curb data breaches.

Our results also demonstrate that security awareness has a two-way effect on the identification of appropriate IT resources as well as the proper implementation of IT solutions to remediate breaches. Although most senior managers realize the importance of paying attention to security threats, lacking the awareness of proper solutions (e.g., IT resources, security policies) or failing to deliver the message to middle-level managers often results in a narrow scope of security strategies and the unsuccessful remediation of data breaches (Ruighaver et al., 2007). To bridge these gaps, we suggest that firms take initial steps to reduce collaboration hurdles among different business units by improving security governance (Gelbstein, 2016) and expanding internal audit capabilities (Kahyaoglu & Caliyurt, 2018). By so doing, security solutions can be better designed and delivered with greater stakeholder participation (Fazlida & Said, 2015). This would also encourage employees to gain a better grasp of the changing threat landscape so that they can devise suitable solutions (Ruighaver et al., 2007). Furthermore, we suggest that policy makers take proactive approaches to provide relevant knowledge and monetary incentives to foster the adoption of updated IT solutions and security practices, especially for small- and medium-sized enterprises (SMEs).

Limitations and Future Directions

We conclude by identifying some limitations of our study and directions for future research. To the best of our knowledge, ours is the first study to connect IT investment with security performance. In future studies, scholars could investigate the antecedents of the disconnect between IT and security. One limitation is that our dataset is relatively small and restricted to U.S. listed firms, as it is constrained by the data sources. Our findings could be verified in future research using SMEs or firms outside the U.S. In terms of the business value of IT investment for security performance, identifying the specific IT investments that can reduce particular types of security incidents would be beneficial.[15] We also acknowledge that measuring security awareness based on firms' disclosure of security activities may not be a perfect method. Future studies might consider developing a more comprehensive representation of firms' security awareness.

[15] For example, an efficient human resources system may help reduce insider threats by enabling better oversight of employees' rights to access and control.

Acknowledgments

The authors thank the senior editor, H. R. Rao, the associate editor, and three anonymous reviewers for their constructive feedback throughout the review process. We are indebted to Eric Zheng, Sean Xin Xu, and the participants of the Workshop of e-Business (WeB), CityU IS Summer Workshop, the International Conference on Information Systems (ICIS) Doctoral Consortium, and the Pacific Asia Conference on Information Systems (PACIS) Doctoral Consortium for their valuable advice on the earlier version of the paper. The work described in this paper was partially supported by a grant from the Research Grants Council of the Hong Kong Special Administrative Region (SAR), China (Project No. CityU 11505015), the Innovation and Technology Fund from the Innovation and Technology Commission (Project No. GHP/142/18GD), the University Grants Committee's Special Grant for Strategic Development of Virtual Teaching and Learning (Project No. 6430900), and the Digital Innovation Laboratory of the Department of Information Systems, City University of Hong Kong.

References

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & Security*, *99*, Article 102030. https://doi.org/10.1016/j.cose.2020.102030

Angst, C. M., Block, E. S., ''Arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly*, *41*(3), 893-916. https://doi.org/10.25300/MISQ/2017/41.3.10

Aral, S., & Weill, P. (2007). IT assets, organizational capabilities, and firm performance: How resource allocations and organizational differences explain performance variation. *Organization Science*, *18*(5), 763-780. https://doi.org/10.1287/orsc.1070.0306

Arellano, M., & Bond, S. (1991). Some tests of specification for panel data: Monte Carlo evidence and an application to employment equations. *Review of Economic Studies*, *58*(2), 277-297. https://doi.org/10.2307/2297968

Arora, A., & Forman, C. (2007). Proximity and information technology outsourcing: How local are IT services markets?

Journal of Management Information Systems, *24*(2), 73-102. https://doi.org/10.2753/MIS0742-1222240204

Ayala, L. (2016). *Cybersecurity lexicon*. Springer. https://doi.org/10.1007/978-1-4842-2068-9_1

Backus, D. (1986). The Canadian-US exchange rate: Evidence from a vector autoregression. *The Review of Economics and Statistics*, *68*(4), 628-637. https://doi.org/10.2307/1924522

Barton, K. A., Tejay, G., Lane, M., & Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. *Computers & Security*, *100*(59), 9-25. https://doi.org/10.1016/j.cose.2016.02.007

Baskerville, R. (2009). Information security control decision theory: Management reasoning in threes. In *Proceedings of IFIP TC 8 International Workshop on Information Systems Security Research*.

Barton, K. A., Tejay, G., Lane, M., & Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. *Computers & Security*, *100*(59), 9-25. https://doi.org/10.1016/j.cose.2016.02.007

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, *37*(6), 508-526. https://doi.org/10.1016/j.jaccpubpol.2018.10.003

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, ''ll do what ''m asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, *18*(2), 151-164. https://doi.org/10.1057/ejis.2009.8

Burtch, G., Ghose, A., & Wattal, S. (2013). An empirical examination of the antecedents and consequences of contribution patterns in crowd-funded markets. *Information Systems Research*, *24*(3), 499-519. https://doi.org/10.1287/isre.1120.0468

Carlo, J. L., Lyytinen, K., & Rose, G. (2012). A knowledge-based model of radical innovation in small software firms. *MIS Quarterly*, *36*(3), 865-895. https://doi.org/10.2307/41703484

Chai, S., Kim, M., & Rao, H. R. (2011). Firms' information security investment decisions: Stock market evidence of investor'' behavior. *Decision Support Systems*, *50*(4), 651-661. https://doi.org/10.1016/j.dss.2010.08.017

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, *106*(3), 345-361. https://doi.org/10.1108/02635570610653498

Chang, Y. B., & Gurbaxani, V. (2012). Information technology outsourcing, knowledge transfer, and firm productivity: An empirical analysis. *MIS Quarterly*, *36*(4), 1043-1063. https://doi.org/10.2307/41703497

Chen, H., De, P., & Hu, Y. J. (2015). IT-enabled broadcasting in social media: An empirical study of artists' activities and music sales. *Information Systems Research*, *26*(3), 513-531. https://doi.org/10.1287/isre.2015.0582

Chen, P.-y., Kataria, G., & Krishnan, R. (2011). Correlated failures, diversification, and information security risk management. *MIS Quarterly*, *35*(2), 387-422. https://doi.org/10.2307/23044049

Cheng, H. K., Li, Z., & Naranjo, A. (2016). Cloud computing spot pricing dynamics: Latency and limits to arbitrage. *Information Systems Research*, *27*(1), 145-165. https://doi.org/10.1287/isre.2015.0608

Claybaugh, C. C., Ramamurthy, K., & Haseman, W. D. (2017). Assimilation of enterprise technology upgrades: A factor-based study. *Enterprise Information Systems*, *11*(2), 250-283. https://doi.org/10.1080/17517575.2015.1041060

Coltman, T., Tallon, P., Sharma, R., & Queiroz, M. (2015). Strategic IT alignment: Twenty-five years on. *Journal of Information Technology*, *30*, 91-100. https://doi.org/10.1057/jit.2014.35

Cram, W. A., Proudfoot, J. G., & ''Arcy, J. (2019). When enough is enough: Investigating the antecedents and consequences of information security fatigue. *Information Systems Journal*, *31*(4), 521-549. https://doi.org/10.1111/isj.12319

''Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79-98. http://dx.doi.org/10.1287/isre.1070.0160

Dewan, S., Michael, S. C., & Min, C.-K. (1998). Firm characteristics and investments in information technology: Scale and scope effects. *Information Systems Research*, *9*(3), 219-232. http://dx.doi.org/10.1287/isre.9.3.219

Dewan, S., & Ramaprasad, J. (2014). Social media, traditional media, and music sales. *MIS Quarterly*, *38*(1), 101-121. https://doi.org/10.25300/MISQ/2014/38.1.05

Dickey, D. A., & Fuller, W. A. (1979). Distribution of the estimators for autoregressive time series with a unit root. *Journal of the American Statistical Association*, *74*(366a), 427-431. https://doi.org/10.1080/01621459.1979.10482531

DiPietro, B. (2018). Speed of tech change a threat to cybersecurity. *The Wall Street Journal.* https://blogs.wsj.com/riskandcompliance/2015/03/17/speed-of-technological-change-is-a-threat-to-cybersecurity/

Fazlida, M. R., & Said, J. (2015). Information security: Risk, governance and implementation setback. *Procedia Economics and Finance*, *28*, 243-248. https://doi.org/10.1016/S2212-5671(15)01106-5

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. *Information Management & Computer Security*, *22*(5), 410-430. https://doi.org/10.1108/IMCS-07-2013-0053

Forman, C. (2005). The corporate digital divide: Determinants of internet adoption. *Management Science*, *51*(4), 641-654. https://doi.org/10.1287/mnsc.1040.0343

Gelbstein, E. (2016). IS audit basics: Auditing IS/IT risk management, Part 1. *ISACA Journal*, *2*, 1-3. https://www.isaca.org/resources/isaca-journal/issues/2016/volume-2/is-audit-basics-auditing-isit-risk-management-part-1

Gelbstein, E. (2017). IS Audit basics: Preparing for auditing new risk. *ISACA Journal*, *1*, 8-11. https://www.isaca.org/resources/isaca-journal/issues/2017/volume-1/is-audit-basics-preparing-for-auditing-new-risk-part-2

Glavach, D. (2017). *In IT Ops, separate security teams should be a thing of the past*. TechBeacon. https://techbeacon.com/it-ops-separate-security-teams-should-be-thing-past

Gopalakrishna-Remani, V., Jones, R. P., & Camp, K. M. (2019). Levels of EMR adoption in US hospitals: An empirical examination of absorptive capacity, institutional pressures, top management beliefs, and participation. *Information Systems Frontiers*, *21*(6), 1325-1344. https://doi.org/10.1007/s10796-018-9836-9

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, *5*(4), 438-457. https://doi.org/10.1145/581271.581274

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Sohail, T. (2006). The impact of the sarbanes-Oxley Act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy*, *25*(5), 503-530. https://doi.org/10.1016/j.jaccpubpol.2006.07.005

Gordon, L., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly*, *34*(3), 567-594. https://doi.org/10.2307/25750692

Granger, C. W. (1969). Investigating causal relations by econometric models and cross-spectral methods. *Econometrica: Journal of the Econometric Society*, *3*(3), 424-438. https://doi.org/10.2307/1912791

Greenberg, P. (2013). Right to know: December 2008. *State Legislatures Magazine*. https://www.ncsl.org/research/telecommunications-and-information-technology/sl-magazine-right-to-know.aspx

Gwebu, K. L., Wang, J., & Wang, L. (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems*, *35*(2), 683-714. https://doi.org/10.1080/07421222.2018.1451962

Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, *33*(1), 2-16. https://doi.org/10.1080/10580530.2015.1117842

Hartmann, C., & Carmenate, J. (2021). Academic research on the role of corporate governance and IT expertise in addressing cybersecurity breaches: Implications for practice, policy and research. *Current Issues in Auditing*, *15*(2), A9-A23. https://doi.org/10.2308/CIIA-2020-034

Heidt, M., Gerlach, J. P., & Buxmann, P. (2019). Investigating the security divide between SME and large companies: How SME characteristics influence organizational IT security investments. *Information Systems Frontiers*, *21*(6), 1285-1305. https://doi.org/10.1007/s10796-019-09959-1

Herath, T. C., Herath, H. S., & ''Arcy, J. (2020). Organizational adoption of information security solutions: An integrative lens based on innovation adoption and the technology-organization-environment framework. *The Data Base for Advances in Information Systems*, *51*(2), 12-35. https://doi.org/10.1145/3400043.3400046

Hirt, S. G., & Swanson, E. B. (2001). Emergent maintenance of ERP: new roles and relationships. *Journal of Software Maintenance and Evolution: Research and Practice*, *13*(6), 373-387. https://doi.org/10.1002/smr.238

Hole, K., & Netland, L.-H. (2010). Toward risk assessment of large-impact and rare events. *IEEE Security & Privacy*, *8*(3), 21-27. https://doi.org/10.1109/MSP.2010.55

Hsu, C., Lee, J.-N., & Straub, D. W. (2012). Institutional influences on information systems security innovations. *Information Systems Research*, *23*(3), 918-939. https://doi.org/10.1287/isre.1110.0393

Hsu, C. W. (2009). Frame misalignment: Interpreting the implementation of information systems security certification in an organization. *European Journal of Information Systems*, *18*(2), 140-150. https://doi.org/10.1057/ejis.2009.7

Islam, M. S., Farah, N., & Stafford, T. F. (2018). Factors associated with security/cybersecurity audit by internal audit function. *Managerial Auditing Journal*, *33*(4), 377-409. https://doi.org/10.1108/MAJ-07-2017-1595

Jeong, C. Y., Lee, S.-Y. T., & Lim, J.-H. (2019). Information security breaches and it security investments: Impacts on competitors. *Information & Management*, *56*(5), 681-695. https://doi.org/10.1016/j.im.2018.11.003

Johnson, M. E., & Goetz, E. (2007). Embedding information security into the organization. *IEEE Security & Privacy*, *5*(3), 16-24. https://doi.org/10.1109/MSP.2007.59

Johnson, P., Lagerström, R., Närman, P., & Simonsson, M. (2007). Enterprise architecture analysis with extended influence diagrams. *Information Systems Frontiers*, *9*(2), 163-180. https://doi.org/10.1007/s10796-007-9030-y

Johnston, A. C., & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM*, *52*(1), 126-129. http://doi.acm.org/10.1145/1435417.1435446

Kahyaoglu, S. B., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*, *33*(4), 360-376. https://doi.org/10.1108/MAJ-02-2018-1804

Kark, K., Penn, J., & Dill, A. (2009). *2008 CISO priorities: The right objectives but the wrong focus*. Forrester Research. http://www.mag-securs.com/mag/IMG/pdf/Forrester_2008_CISO_Priorities_The_right_Objectives_But_The_Wrong_Focus.pdf

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly Executive*, *9*(3), 163-175. https://aisel.aisnet.org/misqe/vol9/iss3/5/

Keil, M., Tan, B. C., Wei, K.-K., Saarinen, T., Tuunainen, V., & Wassenaar, A. (2000). A cross-cultural study on escalation of commitment behavior in software projects. *MIS Quarterly*, *24*(2), 299-325. https://doi.org/10.2307/3250940

Khansa, L., Ma, X., Liginlal, D., & Kim, S. S. (2015). Understanding members' active participation in online question-and-answer communities: A theory and empirical analysis. *Journal of Management Information Systems*, *32*(2), 162-203. https://doi.org/10.1080/07421222.2015.1063293

Kim, K., & Viswanathan, S. (2018). The "experts" in the crowd: The role of experienced investors in a crowdfunding market. *MIS Quarterly*, *43*(2), 347-372. https://doi.org/10.25300/MISQ/2019/13758

Kim, S. H., Mukhopadhyay, T., & Kraut, R. E. (2016). When does repository kms use lift performance? The role of alternative knowledge sources and task environments. *MIS Quarterly*, *40*(1), 133-156. https://doi.org/10.25300/MISQ/2016/40.1.06

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: pathways to vulnerabilities. *Computers & Security*, *28*(7), 509-520. https://doi.org/10.1016/j.cose.2009.04.006

Kwon, J., & Johnson, M. E. (2014). Proactive versus reactive security investments in the healthcare sector. *MIS Quarterly*, *38*(2), 451-471. https://doi.org/10.25300/MISQ/2014/38.2.06

Kwon, J., & Johnson, M. E. (2018). Meaningful healthcare security: Does meaningful-use attestation improve information security performance? *MIS Quarterly*, *42*(4), 1043-1067. https://doi.org/10.25300/MISQ/2018/13580

Kwon, J., Ulmer, J. R., & Wang, T. (2012). The association between top management involvement and compensation and information security breaches. *Journal of Information Systems*, *27*(1), 219-236. https://doi.org/10.2308/isys-50339

Lankton, N., Price, J. B., & Karim, M. (2021). Cybersecurity breaches and the role of information technology governance in

audit committee charters. *Journal of Information Systems*, *35*(1), 101-119. https://doi.org/10.2308/isys-18-071

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 177-187. https://doi.org/10.1057/ejis.2009.11

Li, H., No, W. G., & Boritz, J. E. (2020). Are external auditors concerned about cyber incidents? Evidence from audit fees. *Auditing: A Journal of Practice and Theory*, *39*(1), 151-171. https://doi.org/10.2308/ajpt-52593

Li, H., Yoo, S., & Kettinger, W. J. (2021). The roles of IT strategies and security investments in reducing organizational security breaches. *Journal of Management Information Systems*, *38*(1), 222-245. https://doi.org/10.1080/07421222.2021.1870390

Loft, P., He, Y., Janicke, H., & Wagner, I. (2021). Dying of a hundred good symptoms: Why good security can still fail-a literature review and analysis. *Enterprise Information Systems*, *15*(4), 448-473. https://doi.org/10.1080/17517575.2019.1605000

Lovejoy, K. (2020). *How to manage cyber risk with a security by design approach*. EY Global. https://www.ey.com/en_gl/consulting/how-to-manage-cyber-risk-with-a-security-by-design-approach

Malhotra, Y., & Galletta, D. (2005). A multidimensional commitment model of volitional systems adoption and usage behavior. *Journal of Management Information Systems*, *22*(1), 117-151. https://doi.org/10.1080/07421222.2003.11045840

McEvilley, M. (2002). The essence of information assurance and its implications for the ADA community. *ACM SIGADA ADA Letters*, *23*(1), 35-39. https://doi.org/10.1145/1066404.589459

Moqri, M., Mei, X., Qiu, L., & Bandyopadhyay, S. (2018). Effect of "following" on contributions to open source communities. *Journal of Management Information Systems*, *35*(4), 1188-1217. https://doi.org/10.1080/07421222.2018.1523605

Morgan, S. (2015). Is poor software development the biggest cyber threat? *CSO Online.* https://www.csoonline.com/article/2978858/application-security/is-poor-software-development-the-biggest-cyber-threat.html

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information & Management*, *52*(1), 123-134. https://doi.org/10.1016/j.im.2014.10.009

Olt, C., Gerlach, J., Sonnenschein, R., & Buxmann, P. (2019). On the benefits of senior executives' information security awareness. In *Proceedings of Proceedings of the 4^{0t}h International Conference on Information Systems*.

Palanisamy, R., Norman, A. A., & Mat Kiah, M. L. (2022). BYOD policy compliance: Risks and strategies in organizations. *Journal of Computer Information Systems*, *62*(1), 61-72. https://doi.org/10.1080/08874417.2019.1703225

Pang, M.-S., & Tanriverdi, H. (2022). Strategic roles of IT modernization and cloud migration in reducing cybersecurity risks of organizations: The case of U.S. federal government. *The Journal of Strategic Information Systems*, *31*(1), Article 101707. https://doi.org/10.1016/j.jsis.2022.101707

Phillips, P. C., & Perron, P. (1988). Testing for a unit root in time series regression. *Biometrika*, *75*(2), 335-346. https://doi.org/10.1093/biomet/75.2.335

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management*, *51*(5), 551-567. https://doi.org/10.1016/j.im.2014.03.009

Purvis, R. L., Sambamurthy, V., & Zmud, R. W. (2001). The assimilation of knowledge platforms in organizations: an empirical investigation. *Organization Science*, *12*(2), 117-135. https://doi.org/10.1287/orsc.12.2.117.10115

Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research*, *20*(1), 121-139. https://doi.org/10.1287/isre.1080.0174

Ravichandran, T. (2005). Organizational assimilation of complex technologies: An empirical study of component-based software development. *IEEE Transactions on Engineering Management*, *52*(2), 249-268. https://doi.org/10.1109/TEM.2005.844925

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: extending the end-user perspective. *Computers & Security*, *26*(1), 56-62. https://doi.org/10.1016/j.cose.2006.10.008

Sarkar, S., Vance, A., Ramesh, B., Demestihas, M., & Wu, D. T. (2020). The influence of professional subculture on information security policy violations: A field study in a healthcare context. *Information Systems Research, 31*(4), 1240-1259. https://doi.org/10.1287/isre.2020.0941

Say, G., & Vasudeva, G. (2020). Learning from digital failures? The effectiveness of firms' divestiture and management turnover responses to data breaches. *Strategy Science*, *5*(2), 117-142. https://doi.org/10.1287/stsc.2020.0106

Sekaran, U., & Bougie, R. (2003). *Research methods for business: A skill building approach*. Wiley.

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: an empirical approach. *Journal of Management Information Systems*, *32*(2), 314-341. https://doi.org/10.1080/07421222.2015.1063315

Silic, M., Barlow, J. B., & Back, A. (2017). A new perspective on neutralization and deterrence: predicting shadow IT usage. *Information & Management*, *54*(8), 1023-1037. https://doi.org/10.1016/j.im.2017.02.007

Silic, M., & Lowry, P. B. (2020). Using design-science based gamification to improve organizational security training and compliance. *Journal of Management Information Systems, 37*(1), 129-161. https://doi.org/10.1080/07421222.2019.1705512

Somers, T. M., & Nelson, K. G. (2004). A taxonomy of players and activities across the ERP project life cycle. *Information & Management*, *41*(3), 257-278. https://doi.org/10.1016/S0378-7206(03)00023-5

Sonnenschein, R., Loske, A., & Buxmann, P. (2017). The role of top managers' it security awareness in organizational IT security management. In *Proceedings of Proceedings of the 38th International Conference on Information Systems*.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215-225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, *34*(3), 503-522. https://doi.org/10.2307/25750689

Steelman, Z. R., Havakhor, T., Sabherwal, R., & Sabherwal, S. (2019). Performance consequences of information technology investments: Implications of emphasizing new or current

information technologies. *Information Systems Research*, *30*(1), 204-218. https://doi.org/10.1287/isre.2018.0798

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society*, *71*(C), 15-29. https://doi.org/10.1016/j.aos.2018.04.005

Straub, D., & Welke, R. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, *22*(4), 441-469. https://doi.org/10.2307/249551

Sun, L., Srivastava, R. P., & Mock, T. J. (2006). An information systems security risk assessment model under the Dempster-Shafer theory of belief functions. *Journal of Management Information Systems*, *22*(4), 109-142. https://doi.org/10.2753/MIS0742-1222220405

Tan, C.-H., Sutanto, J., Phang, C. W., & Gasimov, A. (2014). Using personal communication technologies for commercial communications: A cross-country investigation of email and SMS. *Information Systems Research*, *25*(2), 307-327. https://doi.org/10.1287/isre.2014.0519

Tanriverdi, H., Kwon, J., & Im, G. (2020). Data breaches in multihospital systems: antecedents and mitigation mechanisms. In *Proceedings of the 41st International Conference on Information Systems*.

Tarafdar, M., D'Arcy, J., Turel, O., & Gupta, A. (2015). The dark side of information technology. *MIT Sloan Management Review*. *56*(2), https://sloanreview.mit.edu/article/the-dark-side-of-information-technology/

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awareness on information technology professionals' behavior. *Computers & Security*, *79*, 68-79. https://doi.org/10.1016/j.cose.2018.08.007

van Niekerk, J., & von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, *29*(4), 476-486. https://doi.org/10.1016/j.cose.2009.10.005

Vandaie, R., & Zaheer, A. (2014). Surviving bear hugs: Firm capability, large partner alliances, and growth. *Strategic Management Journal*, *35*(4), 566-577. https://doi.org/10.1002/smj.2115

Wang, J., Chaudhury, A., & Rao, H. R. (2008). A value-at-risk approach to information security investment. *Information Systems Research*, *19*(1), 106-120. https://doi.org/10.1287/isre.1070.0143

Wang, J., Gupta, M., & Rao, H. R. (2015). Insider Threats in a financial institution: Analysis of attack-proneness of information systems applications. *MIS Quarterly*, *39*(1), 91-112. https://doi.org/10.25300/MISQ/2015/39.1.05

Wang, T., Kannan, K. N., & Ulmer, J. R. (2013). The association between the disclosure and the realization of information security risk factors. *Information Systems Research*, *24*(2), 201-218. https://doi.org/10.1287/isre.1120.0437

Zhang, T., Havakhor, T., & Biros, D. (2019). Does cybersecurity slow down digitization? A quasi-experiment of security breach notification laws. In *Proceedings of Proceedings of the 40th International Conference on Information Systems*.

Zhuang, Y., Choi, Y., He, S., Leung, A. C. M., Lee, G. M., & Whinston, A. (2020). Understanding security vulnerability awareness, firm incentives, and ICT development in Pan-Asia. *Journal of Management Information Systems*, *37*(3), 668-693. https://doi.org/10.1080/07421222.2020.1790185

About the Authors

Wilson Weixun Li is a lecturer in the Department of Information Systems and Business Analytics at the Deakin Business School, Deakin University, Australia. He conducts research on cybersecurity investment, data protection, cybersecurity regulation, and information systems governance. Wilson completed his Ph.D. at the City University of Hong Kong in 2022.

Alvin Chung Man 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 the 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.

Appendix

Appendix A Literature Review

Our work is closely related to the following three main areas: the impact of security investment, the importance of security awareness, and the measurement and classification of firms' security awareness. We looked for the relevant empirical IS papers from 2010 onward on Google Scholar, using keywords like "security investment," "security awareness," "information security management," "top management support," and "voluntary disclosure." We summarize and discuss the related concepts of each stream of research below, followed by a detailed summary of the main findings of each study (as shown in Table A1).

Concerning the impact of security investment, not all types of security investment have been found to improve firm performance. In previous studies, researchers criticize the effectiveness of security investment for three main reasons: (1) security management may be inefficient when the security budget is not spent on data-breach control technologies (Sen & Borle, 2015), (2) increased complexity in existing information systems makes it difficult for security investment to fundamentally address the core security issues (Straub & Welke, 1998), and (3) public disclosure of implemented security measures may attract more adversaries (Angst et al., 2017).

In prior studies, it has been found that proactive security investment (Kwon & Johnson, 2014), substantial IT adoption (Angst et al., 2017), and meaningful IT (Kwon & Johnson, 2018) can effectively deter security breaches. Awareness of evolving threats and solutions has also been noted as one of the critical success factors (Jeong et al., 2019). These findings also indicate that the prime factor in security investments' failure to protect firms is a lack of understanding of the relevant security risks and security measures (Straub & Welke, 1998).

Concerning previous research on security awareness, both the senior management's degree of commitment to security and the security awareness of top managers have been found to play important moderating roles in the effectiveness of security management (Hsu et al., 2012). Moreover, heightened security awareness can help facilitate the assimilation of security policies and practices (Barton et al., 2016) and lead to more effective IT security management (Sonnenschein et al., 2017). Previous research also highlights the importance of addressing security issues with a broader perspective (e.g., with a view toward general IT resources and IT planning processes), not only with investment in security tools.

Security awareness has usually been measured by firms' voluntary disclosure of security-related activities in corporate reporting (e.g., 10-K reports) in prior literature. Gordon et al. (2006) classify security-related activities in 10-K reports into three categories: proactive solutions, security vulnerabilities, and security breaches. Using a text mining approach, Wang et al. (2013) classified the activities into four categories: actions toward threats, external threats, internal challenges such as limited resources, and intentions to mitigate detected threats. Previous studies have shown that the more security-related activities a firm exhibits, the higher the firm's security awareness (Hanus & Wu, 2016; Olt et al., 2019; Posey et al., 2014; Torten et al., 2018). Based on the voluntary disclosure of security-related activities in firms' annual reports, we can infer their underlying corporate security awareness in two dimensions, namely, threat awareness and countermeasure awareness.

Building on previous research, we seek to develop a conceptual model to explain the interrelationship between IT (and security) investment and security performance (measured by breach incidents) in the current study. We highlight the importance of the moderating role played by firms' security awareness from the perspectives of threat and countermeasure. Our empirical findings show that the critical success factor in effective security performance is the integration of relevant security mindsets to formulate holistic security protection strategies and address the fundamental security issues in the underlying IT systems.

Table A1. Literature Summary Table

Panel A: Evaluation of different types of security investment

Authors	Main findings	Theory / methodology / data source
Kwon & Johnson (2014)	Proactive security implementations (security investment occurred before any breach incidents) are effective in controlling security failures, while reactive security measures (security investment happened after a breach incident) increase security risks.	Organizational learning; Cox proportional-hazard model; secondary U.S. hospital data
Sen and Borle (2015)	Security investment increases security risks at both the state and industry levels, possibly due to inefficient security management or security budget being allocated to the wrong technologies.	Opportunity theory of crime, institutional anomie theory, and institutional theory; negative binomial distribution model; secondary U.S. state-level and industry-level data

Angst et al. (2017)	Symbolic (substantive) IT adoption refers to practices that are loosely (tightly) coupled with organizational activities. Security investment in symbolic IT adopters contributes to the increasing trend of data breaches, while substantive IT adopters hinder the increasing trend. However, substantive adopters' security investment cannot reduce data breaches directly.	Institutional theory; latent class growth mixture models; secondary U.S. hospital data
Kwon and Johnson (2018)	Implementation of security mechanisms certified by "meaningful use" attestation effectively reduces internal accidental breaches attributed to human error, but not enough to deter external breaches caused by rapidly evolving technologies. The certified mechanisms motivate hospitals to meet certain requirements regarding the use of electronic health record (EHR) systems for patient care as well as privacy and security provisions.	Signaling theory and organizational learning theory; propensity-score matching and difference-in-difference model; secondary U.S. hospital data
Panel B: Importance of security awareness		
Authors	**Main findings**	**Theory / methodology / data source**
Straub and Welke (1998)	Lack of knowledge about security risks and security controls is the major cause of ineffective security investment and management. Security management can help firms improve their awareness of potential risks and produce proper solutions using security-risk planning models and security-awareness training.	General deterrence theory; comparative qualitative studies, action research; 2 U.S Fortune 500 firms
Hsu et al. (2012)	Information-security management is an administrative innovation, not a technological innovation. Security awareness among senior managers (or top management support) plays a moderating role in the assimilation (security policies and practices become embedded into organizational activities) of information security management.	Institutional theory; field study; two-stage survey data of Korean organizations
Barton et al. (2016)	Security awareness among senior managers affects their security-related participation (e.g., security governance, nurturing security culture, etc.), further influencing the assimilation of security policies and practices.	Neo-institutional theory; survey; small- and medium-sized enterprises (SMEs) in the south-central U.S.
Berkman et al. (2018)	Markets react positively to firms with heightened cybersecurity awareness because they are more proactive in adopting security measures and policies that would appropriately control security risks.	Ohlson model; Russell 3,000 firms
Panel C: Measurement and classification of security awareness (or disclosure of security threat and countermeasure activities)		
Authors	**Main findings**	**Theory / methodology / data source**
Gordon et al. (2006)	The Sarbanes-Oxley Act of 2002 encourages firms to voluntarily disclose cybersecurity activities, reflecting senior management's cybersecurity valuation and serving as a signal to differentiate superior performers from inferior performers. Firm-year observations related to disclosures of security-related activities are identified based on security-related keywords. Disclosures are further classified into proactive solutions, security vulnerabilities, or security breaches.	Distribution analysis and factor analysis; secondary U.S. firm-level data
Wang et al. (2013)	Firms disclosing risk-mitigating actions are less likely to be breached in the future, compared with those that only disclose risk factors. Firms' disclosure of security activities is measured by the number of information security risk factors disclosed in annual reports. Contents of risk factors are grouped into different clusters based on text mining and are further classified into security risk mitigation or risk acceptance activities by the decision tree model.	Decision tree classification model; secondary U.S. firm-level data
Hanus and Wu (2016)	Users perceive and cope with threats following the security behaviors recommended by firms. Threat awareness and countermeasure awareness are developed based on "threat appraisal" and "coping appraisal" processes in protection motivation theory and measured by the familiarity of the interviewees with related terms (e.g., virus, worm, antivirus software, etc.).	Protection motivation theory; surveys; U.S. undergraduate students
Olt et al. (2019)	Security awareness strengthens senior executives' intention to improve security. The concepts of threats awareness and countermeasure awareness are formulated using Straub and Welke's (1998) model. Senior executives' knowledge of cybersecurity risks and countermeasures is measured using the survey approach.	Surveys; senior executives from Germany

Table A2. List of Keywords Used in 10-K Report Search

Threat-related keywords
Computer Breach*, Computer Security, Computer System Security, Computer Virus*, Cyber Attack*, Cyber Security, Cybersecurity, Data Security, Denial of Service (Denial-of-Service), Hacker*, Identity Theft*, Information Security, Infosec, Intrusion, Malware*, Network Security, Phishing*, Security Breach*, Security Control*, Security Expenditure*, Security Incident*, Security Management, Security Measure*, Security Procedure*, Security System*, Security tech*, Social Engineering, Unauthorized Access*, Unauthorized Participate*, Unauthorized Release*
Countermeasure-related keywords
Access Control, Authentication*, Automatic Update*, Background Check*, Backup Server*, Business Continuity, Contingency Plan*, Data Center Resiliency*, Data Protection*, Disaster Recovery*, Encrypt*, Encryption*, Entry Book-keeping, Firewall*, Intrusion Detection*, Password*, Penetration Test*, Recovery Process*, Redundancy Process*, Safeguard*, Secure Transmission*, Security Monitoring

Note: * represents wild-card searches

Appendix B

Alternative Measures of Security Investment

Following previous security investment studies (Angst et al., 2017; Kwon & Johnson, 2014), we used the number of implemented security measures as the measurement of security investment for robustness checks. To make it comparable with IT investment, we performed a weighted average transformation of the alternative measurement based on the number of employees, as done in the main analysis.

We reestimated the main model by using this alternative measurement of security investment and contrast the results of IT investment. As shown in Table B1, the results are in general consistent with our main findings. The coefficient of L.(Breach × TA) for IT investment is significantly larger than that for security investment. The comparison test of the corresponding coefficients between security investment and IT investment indicates a significant between-group difference (t = -70.24; $p < 0.001$), which supports H1 that the interaction effect of data breaches and threats awareness stimulates more IT investment than security investment. Regarding H2, we conducted a comparison test to compare the coefficients of the lagged interaction terms with CA between the security model and the IT model. The results indicate a significant between-group difference (t = 35.46; $p < 0.01$). That is, the lagged interaction effect of IT investment and countermeasures awareness reduces more data breaches, compared with the lagged interaction effect of security investment and countermeasures awareness.

Table B1. The Interrelationship of IT (Security) Investment, Security Awareness, and Data Breaches

Independent variables	Dependent variables			
	(1) Breach	(2) Security	(3) Breach	(4) IT
L.(Breach × TA)	-0.253(0.230)	-0.005(0.004)	-0.261(0.250)	1.121*(0.678)
L.(Security × CA)	0.017(0.071)	-0.027*(0.015)		
L.(IT × CA)			-0.043***(0.009)	0.128(0.427)
N	1789	1789	1789	1789

Note: Standard errors in parentheses; *p*-values are represented by * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$; L indicates lagged one year. Control variables are omitted in the table due to space limitations. Column 1 and Column 2 are from the same PVAR model, whereby security investment, breaches, security awareness, and the interaction terms are the endogenous variables. Column 3 and Column 4 are from the same PVAR model, whereby IT investment, breaches, security awareness, and the interaction terms are the endogenous variables.

Appendix C

Alternative Measures of Security Awareness

We used an alternative measure of security awareness to better capture the breadth of topics covered in the disclosure. We measured threat awareness and countermeasure awareness by counting the number of distinct keywords shown in 10-K reports (see Table A2 in Appendix A for details). More distinct keywords imply that the firms have a higher awareness of various threats and consider more options for possible countermeasures. Using the number of distinct keywords as a robustness test instead of the total number of keywords can also avoid repetitive use of the same security-related keywords in long reports.

We reran both IT and security investment models using an alternative measure of security awareness. Columns 1-4 of Table C1 show the regression results. In general, the results are similar to our main findings. Threat awareness positively moderates the effects of breaches on IT investment but not security investment; countermeasure awareness negatively moderates the effect of IT investment on data breaches while the effect of security investment is not significant.

Table C1. The Interrelationship of IT (Security) Investment, Security Awareness, and Data Breaches

Independent variables	Dependent variables			
	(1) Breach	(2) Security	(3) Breach	(4) IT
L.(Breach × TA)	-0.187(0.387)	0.012(0.031)	-0.172(0.452)	1.320**(0.655)
L.(Security × CA)	-0.035(0.057)	0.117(0.082)		
L.(IT × CA)			-0.055***(0.013)	0.216(0.412)
N	1789	1789	1789	1789

Note: Standard errors in parentheses; *p*-values are represented by * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$; L indicates lagged one year. Control variables are omitted in the table due to space limitations. Column 1 and Column 2 are from the same PVAR model, whereby security investment, breaches, security awareness, and the interaction terms are the endogenous variables. Column 3 and Column 4 are from the same PVAR model, whereby IT investment, breaches, security awareness, and the interaction terms are the endogenous variables.

Appendix D

Robustness Tests Based on a Two-Step GMM Model

To address the concerns that security (IT) investment and security awareness are significantly different between treatment and control firms in the pre-treatment period, we constructed a subsample by conducting PSM on security (IT) investment, security awareness as well as other control variables. The PSM matching variables between the two groups are not significantly different after matching, as shown in Table D1, suggesting that they are statistically balanced.

Table D1. Summary Statistics and Covariate Comparison Before and After Matching

Variable		Mean		*t*-stat (*p*-value)
		Treated	Control	
IT investment	Unmatched	1.132	1.073	0.46 (0.643)
	Matched	1.122	0.904	1.58 (0.116)
Security investment	Unmatched	0.044	0.061	-0.57 (0.569)
	Matched	0.048	0.044	0.14 (0.891)
Threat awareness	Unmatched	2.910	2.354	3.16 (0.002)
	Matched	2.856	2.821	0.19 (0.847)
Countermeasure awareness	Unmatched	1.324	0.874	2.39 (0.017)
	Matched	1.291	1.119	0.79 (0.428)

To verify our main findings, we reestimated our proposed conceptual framework by using the generalized method of moments (GMM) as follows.

$$Breach_{i,t} = \alpha_0 + \alpha_1 Breach_{i,t-1} + \alpha_2 Investment_{i,t-1} + \alpha_3 Countermeasures\ Awareness_{i,t-1} + \alpha_4 (Countermeasures\ Awareness_{i,t-1} \times Investment_{i,t-1}) + \alpha_5 Control_{i,t} + \varepsilon_{i,t} \quad \text{(D1)}$$

$$Investment_{i,t} = \beta_0 + \beta_1 Investment_{i,t-1} + \beta_2 Breach_{i,t-1} + \beta_3 Threats\ Awareness_{i,t-1} + \beta_4 (Threats\ Awareness_{i,t-1} \times Breach_{i,t-1}) + \beta_5 Control_{i,t} + \varepsilon_{i,t} \quad \text{(D2)}$$

$Investment_{i,t}$ refers to investment either in security measures or general IT. $Control_{i,t}$ refers to the same set of variables to control for firm size, online popularity, advertising expenditure, and firm capability used in the main analysis.

Given that a bidirectional relationship exists between dependent variables ($Breach$ and $Investment$) in Equation (D1) and Equation (D2) and other potential endogeneity issues (e.g., serial correlation between lagged dependent variables and error terms) in dynamic models raised by prior literature (Arellano & Bond, 1991; Khansa et al., 2015), OLS estimator may generate biased results and is not suitable to estimate the model. Following previous studies (Khansa et al., 2015; Moqri et al., 2018), we adopted the two-step GMM estimator, which uses the lagged terms of dependent variables as well as explanatory variables as instruments. This approach has been widely applied in datasets with large panels but short time periods (Moqri et al., 2018). We specified the models (e.g., number of lags used as instruments) to satisfy the diagnostic tests for autocorrelation (Arellano and Bond's serial correlation tests[16]) and exogeneity (Hansen *J* test[17]). As shown in Table D2, the null hypotheses of the Hansen *J* tests are not rejected in all four models, indicating that the overidentifying restrictions are valid for all variables. Moreover, the second-order (AR(2) test) serial correlations for the differenced error terms are all not significant, indicating that second-order serially correlated measurement errors are not exhibited. These results suggest that the system GMM estimation is suitable for our panel dataset. Table D2 presents the estimation results, which are qualitatively similar to those from the PVAR model.

[16] The null hypothesis of Arellano and Bond's serial autocorrelation test is that the errors in the first-difference regression do not exhibit first or second-order serial correlation.

[17] The null hypothesis of the Hansen *J* test is that the instruments are not correlated with the residuals.

Table D2. System GMM Dynamic Panel Data Estimates of Security (IT) Investment, Security Awareness, and Data Breaches

	Dependent variables			
Independent variables	**(1) Breach**	**(2) Security**	**(3) Breach**	**(4) IT**
L.(Breach × TA)		0.094(0.077)		0.751(0.321)**
L.(Security × CA)	0.013(0.018)			
L.(IT × CA)			-0.013(0.008)*	
AR(1) [p-values]	-1.52 [0.129]	-3.01[0.003]	-1.65 [0.099]	-8.51 [0.000]
AR(2) [p-values]	-1.17 [0.241]	-0.62[0.535]	-1.17 [0.241]	-1.34[0.182]
Hansen Test [*p*-values]	2.11[0.909]	9.96 [0.354]	5.39 [0.494]	9.77 [0.369]
N	1481	1481	1481	1481

Note: Standard errors in parentheses; p-values are represented by * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$; L indicates lagged one-year term; All GMM models were estimated using the system GMM estimator implemented via the Stata command xtabond2; Control Variables are omitted in the table due to space limitations.

Appendix E

Robustness Tests by including IT Investment and Security Investment Simultaneously

As an endogenous relationship might exist between security investment and IT investment, we use an alternative model, as specified in Equation (E1), to include security investment and IT investment simultaneously. The model specifications:

$$\mathrm{y}_{i,t} = \begin{pmatrix} Breach_{i,t} \\ IT\ Investment_{i,t} \\ Security\ Investment_{i,t} \\ CA_{i,t} \\ TA_{i,t} \\ (Breach \times CA)_{i,t} \\ (IT\ Investment \times TA)_{i,t} \\ (Security\ Investment \times CA)_{i,t} \end{pmatrix} = \sum_{s=1}^{p} \Phi_s \cdot \begin{pmatrix} Breach_{i,t-1} \\ IT\ Investment_{i,t-1} \\ Security\ Investment_{i,t-1} \\ CA_{i,t-1} \\ TA_{i,t-1} \\ (Breach \times CA)_{i,t-1} \\ (IT\ Investment \times TA)_{i,t-1} \\ (Security\ Investment \times CA)_{i,t-1} \end{pmatrix} + \beta \cdot \begin{pmatrix} Revenue_{i,t} \\ Google\ Trend\ Ratio_{i,t} \\ Expenditure\ in\ Advertisement_{i,t} \\ Number\ of\ Patents\ Issued_{i,t} \end{pmatrix} + \varepsilon_{i,t}, \qquad \text{(E1)}$$

As shown in Table E1, the results are consistent with our main findings. That is, the lagged interaction term of data breaches and threat awareness stimulates more IT investment than security investment. Regarding the effect on deterring data breaches, the lagged interaction term of IT investment and countermeasure awareness has a negative and significant effect on breaches, and the effect is significantly greater than that of the lagged interaction term between security investment and countermeasure awareness.

Table E1. The Interrelationship of Security (IT) Investment, Security Awareness, and Data Breaches

	Dependent variables		
Independent variables	**(1) Breach**	**(2) Security**	**(3) IT**
L.(Breach × TA)	-0.288(0.199)	-0.009(0.020)	0.865*(0.501)
L.(Security × CA)	0.085(0.118)	0.116(0.074)	-0.100(0.994)
L.(IT × CA)	-0.055***(0.015)	-0.016(0.016)	0.064(0.611)
N	1789	1789	1789

Note: Standard errors in parentheses; p-values are represented by * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$; L indicates lagged one-year term; Control variables are omitted due to space limitations. Columns (1), (2), and (3) are from the same PVAR model, whereby IT investment, security investment, breaches, security awareness, and the interaction terms are the endogenous variables.

Appendix F

Examples of Firms' Voluntary Disclosure Related to Security Awareness in 10-K Forms

Table F1. Examples of Firms' Voluntary Disclosures Related to Security Awareness in 10-K Forms
Panel A: Examples of threat awareness
"These **disruptions** may be caused by failures during routine operations such as system upgrades or user errors, as well as network or hardware failures**, malicious or disruptive software, computer hackers**, ... In addition, such events could result in unauthorized disclosure of material confidential information." – The Coca-Cola Company, 2012[18]
"**Information security risks** to companies that use digital technologies continue to increase due in part to the **increased adoption of and reliance** upon these technologies by companies and consumers. Our **risk and exposure** to these matters remain heightened due to a variety of factors including, among other things, the **evolving nature of these threats and related regulation**, the **increased sophistication of organized crime, cyber criminals and hackers**, the prominence of our brand, our and our franchisees' **extensive office footprint**, our plans to **continue to implement our DIY and mobile channel strategies**, and our use of **third party vendors**." – H&R Block, Inc, 2015[19]
Panel B: Examples of countermeasure awareness
"We seek to detect and investigate all security incidents and to prevent their occurrence or recurrence. We continue to **invest in and improve our threat protection, detection and mitigation policies, procedures and controls**. In addition, we work with other companies in the industry and government participants on **increased awareness and enhanced protections** against cybersecurity threats." – Science Applications International Corporation, 2013[20]
"**Training and awareness programs** to educate employees on information security are on-going and include multiple approaches such as mandatory computer-based training, **phishing simulations**, and the designation of individuals as **Information Security and Privacy Champions** within the businesses." – Northern Trust Corporation, 2017[21]

[18] https://www.sec.gov/Archives/edgar/data/21344/000002134413000007/a2012123110-k.htm
[19] https://www.sec.gov/Archives/edgar/data/12659/000157484215000011/hrb2015043010k.htm
[20] https://www.sec.gov/Archives/edgar/data/353394/000119312513127240/d451558d10k.htm
[21] https://www.sec.gov/Archives/edgar/data/73124/000007312418000141/a201710-k.htm

Copyright of MIS Quarterly is the property of MIS Quarterly and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.