Information Systems Frontiers (2024) 26:1109–1120
https://doi.org/10.1007/s10796-023-10404-7

Organizational Learning from Cybersecurity Performance: Effects on Cybersecurity Investment Decisions

Faheem Ahmed Shaikh[1] · **Mikko Siponen**[2]

Accepted: 15 May 2023 / Published online: 27 May 2023

Abstract
IS literature has identified various economic, performance, and environmental factors affecting cybersecurity investment decisions. However, economic modeling approaches dominate, and research on cybersecurity performance as an antecedent to investments has taken a backseat. Neglecting the role of performance indicators ignores real-world concerns driving actual cybersecurity investment decision-making. We investigate two critical aspects of cybersecurity performance: breach costs and breach identification source, as antecedents to cybersecurity investment decisions. We use organizational learning to theorize how performance feedback from these two aspects of cybersecurity breaches influences subsequent investment decisions. Using firm-level data on 722 firms in the UK, we find that higher breach costs are more likely to elicit increases in cybersecurity investments. This relationship is further strengthened if a third party identifies the breach instead of the focal firm. We contribute to the literature on cybersecurity investments and incident response. The findings stress the need for firms to analyze aspects of their cybersecurity performance and use them as feedback for investment decisions, making these decisions data-driven and based on firm-specific needs.

Keywords Cybersecurity investment · Cybersecurity breach · Cybersecurity performance · Breach identification · Breach cost · Organizational learning

1 Introduction

The importance of continual improvements to cybersecurity for ensuring business continuity is widely acknowledged. Towards this objective, academic literature and industry research emphasize the need for cybersecurity investments (Accenture, 2021; Fedele & Roner, 2022). Although there could be various antecedents to firms' security investments, they are ultimately targeted at improving the security posture. Firms channel these investments toward improving technological or human cybersecurity capabilities. The objective is to lower the risk of breach occurrence and enhance incident response capabilities.

✉ Faheem Ahmed Shaikh
faheem.a.shaikh@jyu.fi

Mikko Siponen
mikko.t.siponen@jyu.fi

[1] Faculty of Information Technology, University of Jyväskylä, Agora 521.3, P.O. Box 35, 40014 Jyväskylä, Finland

[2] Faculty of Information Technology, University of Jyväskylä, P.O. Box 35, 40014 Jyväskylä, Finland

Antecedents to cybersecurity investments can be broadly classified into external or internal. External antecedents include industry-specific requirements, regulations, market demands, and vendor or customer demands (Barton et al., 2016; Weishaupl et al., 2018; Xu et al., 2019). For instance, compliance with PCI DSS in the credit card industry or HIPAA in healthcare could drive security investments. Internal antecedents could include business process needs, internal audits, CXO recommendations, lowering insurance costs (Rowe & Gallaher, 2006; Zhao et al., 2009), internal cybersecurity human resource capabilities (Tatsumi & Goto, 2010), or commitment to cybersecurity (Nassimbeni et al., 2012; Tang & Liu, 2015). Due to the difficulty in quantifying these antecedents to security investment, most research in this area is qualitative; information security managers use some form of economic analysis based on cost–benefit, sometimes without quantifying the benefits (Bodin et al., 2018; Gordon et al., 2006). However, simulation and game-theoretic approaches based on cost–benefit analysis (Beresnevichiene et al., 2010), attacker motivation, attacker capabilities, assets, acceptable risk level, and asset importance (Cavusoglu et al., 2008; Fenz et al., 2011; Herath & Herath, 2008; Nagurney &

Shukla, 2017) have also been used widely to model security investment decisions. Regardless of the drivers, these security investments can be channeled through the purchase of security technology, the hiring of personnel, or training programs to improve cybersecurity capabilities. In summary, while research does acknowledge that a range of economic, performance, and environmental factors affect security investment decisions (Gordon et al., 2018), studies have focused mainly on economic issues through modeling approaches, leading to a neglect of research on performance outcomes' influence on security investment decisions.

Breach costs are an indicator of cybersecurity performance because they measure the impact of a breach, show the level of preparedness, and demonstrate the effectiveness of cybersecurity measures. While firms can choose to invest proactively, focusing on breach prevention (Kwon & Johnson, 2014; Safi et al., 2021), breaches, as an indicator of cybersecurity performance, can also trigger cybersecurity investments. Indeed, broader literature on strategic management contends that failures can often form the basis for investments to improve future performance (Haunschild & Sullivan, 2002). Despite this, there are no studies on breach costs motivating cybersecurity investments.

Accounting for breach costs is crucial because not all breaches elicit a strategic response; firms can choose to maintain the status quo (Bana et al., 2021; Gordon et al., 2018) or limit response to technical fixes that remedy the immediate vulnerability. For instance, firms frequently face incidents involving malware or lost devices that may have none or minimal impact; these may not always result in meaningful business impact. An organization-wide strategic cybersecurity response is not required in such cases. However, there may be singular incidents that elicit a broader reaction from stakeholders within and outside the firm, eventually serving as a trigger to increase cybersecurity investments. Ignoring the variation in breach costs as a motivation for investment decisions neglects real-world concerns and actual decision-making processes. Therefore, our study first investigates how breaches with varying costs to the firm influence cybersecurity investment decisions.

Secondly, the quality of incident response can lower or raise breach costs. Consequently, in addition to the type of breach, breach costs are also a function of the firm's incident response capabilities. Therefore, firm cybersecurity investment decisions in response to disruptive breaches can be expected to be more nuanced, based not only on breach severity but also on the firm's evaluation of the effectiveness of incident response. Again, research has not incorporated this critical aspect of cybersecurity performance into cybersecurity investment decisions. We use breach identification source, viz. whether the focal firm identified the breach or if it was identified by a third party, as one indicator of incident response efficiency and investigate how it influences cybersecurity investment decisions following a breach.

To answer our research questions, we use Organizational Learning Theory (Cyert & March, 1963) as a theoretical lens to hypothesize how breach costs and breach identification source affect cybersecurity investment decisions. We use firm-level data on actual breaches and cybersecurity investment decisions following these to test our hypotheses empirically.

Hui et al. (2016) identify security investments as one of the four major themes in IS research on securing digital assets. We contribute to the literature on cybersecurity investments (Gordon et al., 2018) by theorizing and providing empirical evidence for the role of cybersecurity performance, including breach costs and breach identification source as antecedents to cybersecurity investment decisions. We also contribute to the literature on incident response (Ahmad et al., 2022) by theorizing and providing empirical evidence for how breach identification source, an indicator of incident response efficiency, could be used by firms to calibrate cybersecurity investment decisions.

2 Background Literature

2.1 Cybersecurity breach costs

A cybersecurity breach is an event that results in unauthorized access to data, applications, services, networks, or devices by bypassing their underlying security mechanisms (ACSC, 2022). Some examples of incidents are data breaches, ransomware attacks, malware attacks, or phishing.

Incident costs can be divided into direct or short-term, recovery, and long-term costs (Fowler, 2016). Direct costs include direct loss or damage to assets, data, intellectual property, and loss of business continuity when staff cannot carry out normal activities, and customers cannot avail of services. Recovery costs include resources the IT function devotes to incident management, getting backups online, restoring business continuity, and costs of investigating the incident and communicating with stakeholders. Long-term costs include damage to reputation, lost business, market losses (Dong et al., 2023; Spanos & Angelis, 2016), loss of existing and potential customers, and customer redressal and compensation costs.

From the firm's perspective, high incident costs are undesirable as they add to business costs. Given that direct costs and the cost of recovery can vary based on firms' incident management capabilities, overall incident costs can be expected to vary among firms (Fowler, 2016). High incident costs can even threaten the survival of small and medium businesses (Paulsen, 2016; Ponemon, 2019). Therefore, it is in the firm's interest to avoid or keep these costs to a minimum (Hasan et al., 2021). Firms with mature security capabilities can identify incidents quicker and respond rapidly to reduce the incident impact and scope. Towards

this end, continuous improvement of cybersecurity capabilities is in the firm's business interests. Financial investments in cybersecurity contribute to building these capabilities toward improving incident avoidance and response capabilities (Anderson & Choobineh, 2008; Gordon et al., 2016). Indeed, industry surveys point out that with the number of incidents increasing annually, investments in cybersecurity are showing a rising trend (SANS, 2021).

Major cybersecurity failures can spur an organization to engage in problematic search and learn from its experience in dealing with the incident, making meaningful changes towards improving its cybersecurity capabilities. Organizational learning (Cyert & March, 1963) represents an appropriate theoretical lens to examine learning and action following such failures. Prior literature has used organizational learning as a framework to provide conceptual recommendations for improving security capabilities (e.g., Ahmad et al. (2020), Shedden et al. (2011)).

2.2 Organizational Learning Theory

The fundamental idea in organizational learning is that organizations learn from experience and effect improvements to their processes, strategies, and structures based on performance (Levitt & March, 1988). Organizations are characterized as history-dependent systems that evolve in response to past experience (Cyert & March, 1963). Learning can come through direct experience, through interpreting others' experiences via planned learning, information seeking through research, surveys, and experiments, or unsystematic learning (Huber, 1991). Learning is included into routines that serve as knowledge repositories, which are updated in response to experiences. Examples of routines are rules, strategies, technologies, practices, and capabilities. Effective learning organizations assimilate novel ideas and overcome inertia (Simon, 1991). This process involves learning as well as unlearning. Inter-firm collaboration, outsourcing, and rare events are a few examples of sources from where such experiences could originate (Haunschild & Sullivan, 2002). Broadly, success and failure are two types of experiences organizations learn from (Miner et al., 2008).

Organizations engage in problematic search to correct their behavior following failures and incorporate this learning into their routines. The objective is to reduce future failure rates (Kim & Miner, 2007; Madsen & Desai, 2010). Failures lead to learning by providing the motivation for learning and inputs in the form of experience from which to infer lessons. Major incidents trigger this search process (Haunschild & Sullivan, 2002; Madsen & Desai, 2010) as opposed to smaller failures that might only lead to minor adjustments in organizational routines. Crisis events like cybersecurity breaches provide opportunities to reevaluate current processes and motivate change (Miller & Chen, 1994).

Employing interviews with cybersecurity decision-makers, Weishaupl et al. (2018) find that cybersecurity incidents can serve as learning triggers. They also find that major breaches play an important role in decision-making regarding cybersecurity improvements; in the absence of incidents, firms prefer maintaining the status quo. Having experienced a major incident that resulted in material damage, a firm will want to avoid similar costs in the future. Financial investments in security are an essential first step toward improving security capabilities. This is especially true for resource-strapped firms; firms focusing on reducing expenses will likely limit themselves to responding to disruptive incidents rather than putting preventive measures in place (Kwon & Johnson, 2014). Using information from the most recent incident to put security measures in place is a cost-effective strategy for firms that can't implement preventive measures (Ozkaya, 2021). For instance, unlike larger organizations with adequate financial resources, resource-strapped organizations cannot afford a 24×7 Security Operations Center (SOC) for continuous monitoring. Since it is difficult for the management to calculate the return on security investments, this strategy provides a better estimation of costs based on attacks encountered rather than anticipated attacks that might never happen.

3 Hypothesis Development

3.1 Costs of breaches and cybersecurity investments

Firms can choose to maintain the status quo or improve their security capabilities after a breach. How firms react to cybersecurity incidents has implications for their future cybersecurity posture.

Organizational learning posits that organizations engage in single-loop learning in case of relatively minor failures, such as minor product defects. This involves identification, correction, and process changes to address the immediate issue and ensure it does not recur. Echoing this approach, Shedden et al. (2009) posit that in the wake of breaches, organizations typically focus on resolving the immediate technical issues, with limited attention to improving the overall incident response process and with hardly any long-term oriented consideration of improvements to security capabilities. For instance, firms can take corrective actions to plug security vulnerabilities. However, focusing on only correcting the vulnerability that led to the most recent breach will only protect the organization from attacks that exploit the specific vulnerability. Failures thus provide organizations with learning opportunities, but learning is not guaranteed. Organizations have leeway in interpreting failures and might choose to interpret them self-beneficially (Baumard & Starbuck, 2005).

Minor failures also run the risk of going unnoticed or intentionally ignored. Managers tend to interpret minor failures as random events (Baumard & Starbuck, 2005). Small failures are less likely to challenge the IT security function or management's fundamental perceptions of the current security posture. Not all breaches are a cause for concern, and firms do not need to make major changes in response to every single breach. Due to budget constraints, firms must be judicious about how much and in which areas to invest. For instance, firms might be affected by different breaches that might not lead to data loss or loss of business continuity and have no business implications. In such cases, firms might perform technical fixes for low-cost breaches or choose to ignore them as one-off incidents. Other options include policy changes and training following breaches. Firms could also take other actions that do not necessarily demand investments, such as changing tool configurations and access controls, modifying backup and contingency plans, and standard operating procedures, taking disciplinary action, updating software, or updating passwords (Fowler, 2016).

On the other hand, organizational learning contends that major failures are more likely to elicit a meaningful response from an organization. Compared to minor failures, major failures can evoke surprise and greater recognition and lead to meaningful changes through a double-loop learning process (Argyris, 1977). Double-loop learning leads to the organization examining fundamental routines in an area of concern in greater depth to advance long-term improvements. It is more likely to occur in crises due to major events. Along these lines, major breaches give the firm a visible measure of the impact breaches can have on business. High breach costs increase the visibility of the cybersecurity function and make it easier to justify and gain support for cybersecurity investments. This is because breaches with higher costs can lead to extensive problematic search and major improvements to security to improve the overall security posture substantially (Ahmad et al., 2020; Van Niekerk & von Solms, 2004). After a costly breach, firms might invest more in cybersecurity to prevent repeat breaches and rebuild trust in key stakeholders. Firms can see such events as an opportunity to improve firm security capabilities to prevent, identify, and manage the response to future breaches.

In summary, compared to breaches with less material impact, breaches resulting in higher costs are more likely to gain wider visibility in the organization and provide greater motivation to effect improvements to cybersecurity routines. The organization would be more likely to reassess its security strategy and effect increased security investments rather than undertake only a limited tactical response. Therefore,

H1: Compared to breaches associated with lower costs, those with higher costs will be more likely to result in increased cybersecurity investments.

3.2 Organization Learning Theory and incident response

In learning from incidents, organizational learning theory emphasizes the importance of postmortems, which are systematic measures to diagnose problems (Basten & Haamann, 2018). This involves reflecting on positive and negative aspects of events to derive actionable items. Learning from careful analyses like postmortems is preferred over haphazard evaluations. In case of cybersecurity breaches, postmortems come in the form of post-breach reviews. They involve reflecting on and reviewing the preparedness, identification, and management of a breach to reduce the probability of a repeat incident and improve future incident identification and management capabilities (Fowler, 2016). This happens through a formal review, reports, and presentations to management. Changes to procedures are documented to serve as repositories for organizational routines in dealing with future breaches. We now hypothesize how breach identification, an essential component of incident response, can moderate the relationship proposed in H1.

Incident response (IR) is the formal process through which organizations engage personnel to analyze, identify, and respond to an incident (Ozkaya, 2021). Incident response aims to protect the organization from the negative consequences following a breach and enable timely business recovery (Grispos et al., 2015; Menges & Pernul, 2018). Effective incident response capabilities are critical in ensuring that a breach does not escalate. As such, incident response is one area where firm cybersecurity investments are directed. Due to its business impact, the process is a top priority for the management and security functions, and a dedicated team may be tasked to do it. Security Operations Centers in large organizations carry out incident response. In contrast, in small and medium-sized businesses, a smaller team from the IT function or the IT manager might carry out this activity (Ahmad et al., 2012).

Multiple standards propose linear incident response frameworks that move from one phase to another (CREST, 2021; IEC, 2016). The typical phases of incident response are preparation, identification, containment, eradication, recovery, and post-incident review (Ozkaya, 2021). Preparation involves having the relevant technology, processes, and governance mechanisms in place. Identification consists in ascertaining that an incident has actually taken place. The objective of containment is to stop further damage to the firm's information systems. Eradication consists in removing the root causes of the breach, e.g., by removing the malware. Recovery involves restoring business continuity and routine operations. Finally, post-incident review consists in reflecting on incident handling to improve processes for managing future incidents.

3.3 Breach identification source

Early identification is vital to the incident response process, with consequences for breach costs. Industry research shows that attacks are increasingly sophisticated, with attackers increasing their dwell time to access critical information. Consequently, the time to identify breaches has increased annually (IBM Security, 2019). According to FireEye (2021), the mean dwell time globally is 146 days before breach identification. Given the wide variation in dwell time, the quicker an organization can identify a breach, the better it will be able to limit the damage. Activities such as containment and recovery can only be carried out after breach identification, making breach identification capabilities of critical importance.

Breaches could be identified by several sources, broadly classified as internal or self-identified and external or third-party identified. Third parties include regulators, law enforcement, independent security professionals, or customers after they have experienced repercussions due to the breach (Clearinghouse, 2009). For instance, breaches could come to light after users report suspicious activity on their bank accounts or payment methods.

On the other hand, self-identification of breaches could originate from the IT security function or employees in the wider organization who notice suspicious activity. Self-identification, where firms identify breaches instead of being notified by third parties, signals effective firm cybersecurity capabilities and can help reduce negative media scrutiny that can unduly influence response. Well-managed incident response is of utmost importance to limit financial and reputational damage by ensuring the organization is effectively in control.

3.4 Breach identification source and performance feedback

Breach self-identification by the focal firm indicates that multiple facets of its security operations work effectively. For instance, effectively trained employees can be an essential means of early breach identification (McIlwraith, 2021) through activities such as reporting suspicious files, directories, or emails. Although they may not have the technical expertise to ascertain that the organization is under attack, cyber security-aware employees can signal their suspicion to the cybersecurity function for follow-up (Kemper, 2019). Efficient communication channels with the security function, an essential part of firm security capabilities, can facilitate this.

Another source of self-identification is security software, where firms have a choice of multiple security technologies and ways of configuring these according to their specific network. A one size fits all approach is not recommended for cybersecurity, and organizations need to be cognizant of their business needs and adapt cybersecurity to their specific environment. Deriving meaningful output and making sense of firewall notifications, malware and intrusion detection systems, and host-based and network-based tool logs (Gupta & Srinivasagopalan, 2020) involves optimal configuration and is a firm-specific capability.

In summary, self-identification of breaches reflects the firm's security capabilities, including how well employees are trained and security-aware, how well the SOC functions, and how well the security tools are configured and leveraged. While breaches may not be entirely avoidable, breach identification is part of a firm's cybersecurity capabilities. If the breach is identified by a third party instead of the focal firm, it is more likely that the firm evaluates its security capabilities negatively during post-incident reviews.

The incident response process is improved iteratively by incorporating feedback and insights gained from experience dealing with breaches (Ahmad et al., 2020). Learning from incidents will provide feedback to security routines when the team identifies what technical and procedural aspects worked and which did not and need rectification. Indeed, the security function is responsible not only for managing the technical response in the immediate aftermath of the incident, but also for providing inputs to validate and improve the incident response process (Fowler, 2016; West-Brown et al., 2003). This consists in documenting the experience and learning from incidents, communicating these to the management, and making a persuasive case for process changes if required (Grance et al., 2004; Shedden et al., 2011). Compared to self-identification, in case of breaches identified by third parties, the security function is more likely to recommend substantial changes toward improving security capabilities. This raises the likelihood of increased cybersecurity investments. Therefore,

> **H2:** Breach identification source will moderate the positive relationship between breach cost and cybersecurity investments such that third party-identified breaches will be more likely to result in cybersecurity investments.

4 Method

4.1 Sample

We used data from the UK Cyber Security Breaches Survey to test our hypotheses. The survey is carried out annually by the Department for Digital, Culture, Media, and Sport of the Government of the UK (UKCS, 2020). The objective of the survey is to provide input to cybersecurity policy through understanding various aspects of cybersecurity threats. The survey targets small, medium, and large firms and charities spanning multiple industries in the UK. Data is collected through a telephone survey using random probability sampling to avoid selection bias. The data is anonymized, and

firms are not tracked longitudinally. We used data collected in survey iterations from 2018 to 2020 as these iterations had uniform survey instruments directly applicable to our research questions; relevant questions were dropped in later iterations. The data had 267, 252, and 203 observations for 2018, 2019, and 2020 respectively. The specific section of the questionnaire asked the respondents to answer the questions in the context of the one cybersecurity breach or related series of breaches or attacks that caused the most disruption to their organization in the last 12 months.

4.2 Measures

Dependent variable Our dependent variable is cybersecurity investment. Firms were asked: "What, if anything, have you done since this breach or attack to prevent or protect your organization from further breaches like this?" Firms were provided with multiple options related to possible actions. For our dependent variable, we focused on the specific response option " Increased spending on cybersecurity." The dependent variable was coded as 1 if firms responded yes to this option, 0 otherwise.

Independent variable Our independent variable is breach cost. Firms were asked: "In total, approximately how much, if anything, do you think this single most disruptive breach or attack has cost your organization financially?" Responses were collected on a scale ranging from 1 to 12 (1: Less than £100; 2: £100 to less than £500; 3: £500 to less than £1,000; 4: £1,000 to less than £5,000; 5: £5,000 to less than £10,000; 6: £10,000 to less than £20,000; 7: £20,000 to less than £50,000; 8: £50,000 to less than £100,000; 9: £100,000 to less than £500,000; 10: £500,000 to less than £1 million; 11: £1million to less than £5million; 12: £5 million or more).

Moderator Our moderator is breach identification source. This was coded as 1 if the firm self-identified the breach and 0 if a third party identified it. Firms were asked, "Thinking about your most disruptive breach or attack, how was this identified?" Respondents were provided with an extensive list of options from which they chose the source of breach identification. We classified this list of sources into self-identified and third-party identified. Specifically, breaches were coded as self-identified if the source was more likely to be the firm and included the following: by antivirus/ anti-malware software, routine internal security monitoring, other internal control activities not done routinely (e.g., reconciliations, audits, etc.), unusual email/ file activity, typos/ poor grammar/ use of English, pop-ups, website/ computer crashed, previous experience/ it was obvious, loss of data/ money, unusual phone calls, inappropriate requests for information/ money, by accident, reported/ noticed by staff/ contractors.

We coded breaches as third-party identified if the source was likely to be outside the firm and includes the following: from warning by government/ law enforcement, breach/ attack reported by the media, similar incidents reported in the media, reported/ noticed by customer(s)/ customer complaints, by the bank/ credit card company, external IT service provider, disruption to business/ staff/ users/ service provision, reported/ noticed by an external third-party.

Controls We included control variables to account for other factors that might influence our hypothesized relationships. We controlled for firm size using the number of employees. The survey classified firms based on the number of employees as micro (1–9), small (10–49), medium (50–249), or large (250+). We controlled for all 12 industries captured in the survey using dummy variables coded 1 for a specific industry and 0 otherwise. We also controlled for firms' online presence as those with a greater online presence could be more attentive to cybersecurity. We created a composite variable to account for online presence based on responses to multiple questions under the "Online presence" section in the survey. This included whether the firm had a social media presence, if customers could pay for services online, an online bank account for customers to pay into, an industrial control system if customer's personal information was held electronically, if people could donate online, or if beneficiaries could access services online. We also controlled for the type of breach (ransomware, malware, denial of service, bank account hacking, impersonation, phishing, unauthorized file/ network access by insiders, unauthorized file/ network access by outsiders, other security incident). Finally, we controlled for year fixed effects. The equation below shows the model tested:

$$\begin{aligned} &CybersecurityInvestment \\ &= (\beta_1 \times BreachCost) \\ &+ (\beta_2 \times BreachCost \times BreachIdentificationSource) \\ &+ (\gamma \times Controls) \\ &+ \eta_t + \mu \end{aligned}$$

In the model indicated above, β_1 and β_2 are coefficients indicating the impact of breach cost and breach identification source on the decision to increase cybersecurity investment. The term γ indicates the effect of each of the controls described above. Finally, the term η_t represents time-fixed effects, while μ is the error term.

We used logistic regression with robust standard errors in Stata to test our hypotheses. Four control variables (dummies for entertainment or services, health or social care, utilities or production industries, and ," unauthorized use of computers, networks or servers by staff even if accidental")

were found to predict failure perfectly and dropped by Stata in the regression analysis. This led to a total of 496 firm-year observations in the model. Table 1 shows the correlations among variables incorporated in the final regression analysis.

Table 2 shows the results of hypothesis testing with logistic regression. In Model 1 we included only the control variables. In Model 2, we added breach costs and found that its effect on cybersecurity pending (H1) was significant ($\beta = 0.237$; $p = 0.008$; S.E. = 0.099). Although we did not hypothesize for the direct effect of the breach identification source, we added it as a control in Model 3. We found no significant effect ($\beta = -0.453$; $p = 0.186$; S.E. = 0.507).

Model 4, the final model, includes all control variables, direct effects of the independent variable and moderator, and moderating effect. The positive effect of breach costs on increased spending on cybersecurity stays significant ($\beta = 0.522$; $p = 0.006$; S.E. = 0.192). H2, which argues for a moderating effect of the breach identification source, is confirmed ($\beta = -0.409$; $p = 0.044$; S.E. = 0.240).

5 Discussion

Organizational learning posits that firms learn when they experience problems (March, 1996). Learning occurs nonlinearly, with crisis events as triggers (March et al., 1991). Empirical analysis of firm-level data confirms the hypothesis that breaches resulting in higher financial costs are positively associated with the decision to increase cybersecurity investments. Furthermore, the likelihood of such an increase in cybersecurity spending is increased in case of weaker incident response capabilities represented by third-party reported breaches. That the moderator is not independently significant shows that firms are not likely to base their cybersecurity investment decisions solely on whether a breach was identified internally or by a third party. Information about the breach identification source will only be used to further calibrate cybersecurity investment decisions in the broader context of breach costs.

Firms cannot be expected to make strategic cybersecurity decisions in reaction to every breach; breaches with relatively greater financial costs will significantly affect their cybersecurity investment decisions. When faced with frequent low-impact breaches, firms might choose to maintain the status quo and focus on successes instead of minor failures (Madsen & Desai, 2010). This is because minor failures provide weak cues about firm performance (Eggers, 2012). On the other hand, major incidents are more likely to elicit support from the management for organizational learning and acting for sustained change. This translates to broadening the focus to identify the assets compromised, identifying more areas of weakness, investing more in securing assets, and improving incident response capabilities.

Even while reacting to high-cost breaches, firms need to be aware that they do not have unlimited resources and will need to consider their current state of incident response capabilities before deciding to invest. Self-identification of breaches is one such indicator of incident response capabilities; it is a culmination of many aspects of cybersecurity working efficiently. For instance, it reflects how well the employees are trained, how well security tools are configured, and how well the SOC correlates alerts to identify breaches. Therefore, the learning that firms derive following breaches will be different as third-party identified breaches might indicate greater room for improvement in cybersecurity.

Given that both higher breach costs and third-party identified breaches tend to signal relatively greater security shortcomings and might require increased cybersecurity spending, organizations must prioritize efforts to minimize breach costs and enhance their internal breach identification capabilities. Several practical recommendations can be considered to achieve these objectives.

Firstly, organizations can leverage tools, knowledge and training towards achieving these objectives. Examples of tools include Security Information and Event Management (SIEM) systems to swiftly identify potential breaches. In addition to security tools, regular monitoring of updates from global security expert groups such as Computer Emergency Response Teams (CERT) can help organizations stay abreast of emerging vulnerabilities so that response to zero-day attacks can be expedited. Implementing comprehensive Security Education, Training, and Awareness (SETA) programs (Hu et al., 2022) can empower employees to play an active role in detecting and reporting breaches in a timely manner; this could also lead to reduced breach dwell times, consequently lowering costs. These measures can help improve organizations' internal breach identification capabilities.

Secondly, organizations need to focus on expediting incident response phases following breach identification, including containment, eradication, and recovery, to restore operations quickly and minimize business disruption (Fowler, 2016, pp. 12–13). This can help minimize overall breach costs.

Thirdly, the findings encourage firms to review their security budgets based on post-incident review findings. Analysis of the incident management experience can lead to organizational learning, allowing a more efficient allocation of resources into relatively weaker areas to strengthen the overall cybersecurity posture.

Table 1 Descriptive Statistics

Variables	Mean	S.D	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1. Firm size	2.481	1.119	1													
2. Online presence	2.939	1.250	0.257**	1												
3. Breach costs	3.855	1.863	0.241**	0.021	1											
4. Cybersecurity investment	0.042	0.202	0.025	-0.033	0.112**	1										
5. Breach identification source	0.778	0.415	-0.041	-0.002	-0.079*	-0.035	1									
6. Ransomware	0.134	0.341	0.037	-0.036	0.155**	0.057	0.054	1								
7. Malware	0.150	0.358	-0.043	-0.082*	-0.094*	-0.032	0.076*	-0.166**	1							
8. Denial of service	0.078	0.269	-0.034	0.121**	-0.021	0.065	-0.103**	-0.115**	-0.123**	1						
9. Bank account hacking	0.034	0.182	-0.115**	-0.076*	-0.050	-0.003	-0.045	-0.075*	-0.080*	-0.055	1					
10. Impersonation	0.156	0.363	0.094*	0.052	0.125**	0.040	-0.101**	-0.170**	-0.182**	-0.126**	-0.082*	1				
11. Phishing	0.313	0.464	0.027	0.028	-0.185**	-0.114**	0.101**	-0.266**	-0.285**	-0.198**	-0.128**	-0.291**	1			
12. Unauthorized file/ network access (Insider)	0.016	0.127	0.031	0.041	0.039	-0.028	0.043	-0.051	-0.055	-0.038	-0.025	-0.056	-0.088*	1		
13. Unauthorized file/ network access (Outsider)	0.072	0.258	-0.034	-0.029	0.128**	0.047	-0.071	-0.110**	-0.117**	-0.082*	-0.053	-0.120**	-0.188**	-0.036	1	
14. Other security incident	0.042	0.202	-0.042	-0.033	-0.009	0.023	-0.035	-0.083*	-0.089*	-0.062	-0.040	-0.091*	-0.143**	-0.028	-0.059	1

$n = 722$

** $p < 0.01$, * $p < 0.05$.

Table 2 Hypothesis testing results

Variables	Hypothesis	Model 1		Model 2		Model 3		Model 4	
DV: Cybersecurity investment		B	S.E	B	S.E	B	S.E	B	S.E
Firm size		0.095	0.120	0.197	0.182	0.198	0.189	0.204	0.191
Online presence		0.195	0.141	-0.142	0.191	-0.228	0.189	-0.236	0.190
Ransomware		0.408	0.815	-0.545	0.913	-0.615	0.936	-0.542	0.919
Malware		-0.648	0.893	-1.171	1.051	-1.207	1.060	-1.278	1.088
Denial of service		0.629	0.826	0.687	0.884	0.606	0.884	0.728	0.895
Bank account hacking		-0.019	1.041	-0.433	1.298	-0.531	1.320	-0.463	1.297
Impersonation		-0.340	0.790	-0.422	0.901	-0.539	0.931	-0.593	0.938
Phishing		-1.133	0.778	-1.899**	1.027	-2.643**	1.202	-2.762**	1.234
Unauthorized file/ network access (Insider)		0.830	1.029	0.000	0.000	0.000	0.000	0.000	0.000
Unauthorized file/ network access (Outsider)		0.456	0.884	-0.785	1.102	-0.980	1.120	-1.060	1.179
Breach costs	H1(+)			0.237***	0.099	0.228**	0.106	0.522***	0.192
Breach identification source						-0.453	0.507	1.665	1.328
Breach costs x Breach identification source	H2(+)							-0.409**	0.240
Constant		-3.706***	0.951	-3.521***	1.239	-3.109**	1.388	-4.672***	1.496

*** $p<0.01$, ** $p<0.05$, * $p<0.1$

Controls for Year and Industry included

We contribute to the literature on cybersecurity investments (Gordon et al., 2016) by theorizing and providing empirical evidence for the role of cybersecurity performance. Past literature has overlooked the role of cybersecurity performance in cybersecurity investment decisions. It has mainly examined the market impact of a particular kind of breach, viz. data breaches (Spanos & Angelis, 2016), while ignoring their impact on internal functioning and investments. This is concerning because feedback from performance drives strategic decision-making. Our study moves the conversation from focusing on simulation approaches and game-theoretic models to actual firm experiences in the form of failures driving decision-making. We contribute to theory by explaining the cybersecurity investment decision process using the organizational learning perspective. This perspective leverages arguments from the actual functioning of organizations and provides practitioners with actionable insights. Wolff and Lehr (2017) indicate that empirical evidence lags far behind modeling and simulation approaches. We fill this research gap by examining the financial costs of actual breaches and cybersecurity investment decisions following these.

While incident response is understudied (Ahmad et al., 2022), the postmortem phase of incident response has received even less research attention (Shedden et al., 2011). Literature on incident response has focused mainly on technical aspects involving identification, recovery, and investigation for legal follow-up (Mitropoulos et al., 2006; Shedden et al., 2011) while implications for strategic security posture have been ignored. This is concerning because postmortems are critical phases that shape future cybersecurity posture. Despite this, past research has focused on the immediate response rather than organizational learning toward improving security capabilities. We theorize how firms could use postmortem analysis in the form of evaluation of the breach identification source to calibrate cybersecurity investment decisions.

6 Limitations

Our research focuses on cybersecurity investment decisions made by firms in response to the most disruptive breaches. We contend that not all cybersecurity breaches will necessarily trigger security investments, which is why it is more useful to examine security investment decisions as a function of breach costs rather than the mere occurrence of a breach. It is possible that organizations experience minor breaches from which they derive valuable insights and subsequently make improvements to their security measures. However, due to practical constraints, such minor breaches and the corresponding firm reactions cannot be feasibly included in a comprehensive survey spanning hundreds of organizations. Despite this limitation, our empirical analysis, which encompasses a diverse range of organizations and controls for breach type, offers robust evidence in support of our arguments.

To gain further insight into firm reactions to minor breaches that do not result in high costs but still highlight security gaps, qualitative case studies conducted within a limited number of organizations may present a suitable

methodology. By complementing our current findings with case studies, a more comprehensive understanding of how organizations respond to different types and severities of breaches can be achieved.

7 Conclusion

Firms need to be concerned with cybersecurity investments and reactions to breaches as both have implications for their cybersecurity posture and downstream effects on overall business performance. Our study combines these two important areas of practical concern to examine the relationship between cybersecurity performance and cybersecurity investment decisions. Empirical results confirm the hypothesis that higher breach costs result in more security investment. Moreover, this relationship is strengthened if the breach is identified by a third-party instead of internally by the focal firm.

Our findings and theory are especially important to security decision-makers who can look at multiple aspects of their operational security performance to make cybersecurity investment decisions. It can help firms make their cybersecurity investment decisions data-driven. This presents a better alternative to other motivations for cybersecurity investments, including spontaneous reactions following breaches, adopting the latest security tools in fashion without examining firm-specific needs, or making fear appeals to the management.

Future research can extend this focus on cybersecurity performance to examine how other aspects of actual cybersecurity performance including failures, influence organizational learning and decision-making.

Funding Open Access funding provided by University of Jyväskylä (JYU).

Data Availability The data used in the current study is publicly accessible at the following URL:http://doi.org/10.5255/UKDA-SN-8480-1

Declarations

Financial Interests The authors have no relevant financial or non-financial interests to disclose.

References

Accenture. (2021). *State of cybersecurity*. https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf. Accessed 24 May 2023

ACSC. (2022). *Australian cyber security centre: Glossary*. https://www.cyber.gov.au/learn-basics/view-resources/glossary. Accessed 24 May 2023

Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams – challenges in supporting the organisational security function. *Computers & Security, 31*(5), 643–652. https://doi.org/10.1016/j.cose.2012.04.001

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology, 71*(8), 939–953. https://doi.org/10.1002/asi.24311

Ahmad, A., Maynard, S., & Baskerville, R. (2022). Editorial. *Computers & Security, 112*, 102530. https://doi.org/10.1016/j.cose.2021.102530

Anderson, E. E., & Choobineh, J. (2008). Enterprise information security strategies. *Computers & Security, 27*(1), 22–29. https://doi.org/10.1016/j.cose.2008.03.002

Argyris, C. (1977). Double loop learning in organizations. *Harvard Business Review, 55*(5), 115–125.

Bana, S., Brynjolfsson, E., Jin, W., Steffen, S., & Wang, X. (2021). Cybersecurity hiring in response to data breaches. *SSRN*. https://doi.org/10.2139/ssrn.3806060

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

Basten, D., & Haamann, T. (2018). Approaches for organizational learning: A literature review. *Sage Open, 8*(3). https://doi.org/10.1177/2F2158244018794224

Baumard, P., & Starbuck, W. H. (2005). Learning from failures: Why it may not happen. *Long Range Planning, 38*(3), 281–298. https://doi.org/10.1016/j.lrp.2005.03.004

Beresnevichiene, Y., Pym, D., & Shiu, S. (2010). Decision support for systems security investment. *IEEE/IFIP Network Operations and Management Symposium Workshops, 2010*, 118–125. https://doi.org/10.1109/NOMSW.2010.5486590

Bodin, L. D., Gordon, L. A., Loeb, M. P., & Wang, A. (2018). Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy, 37*(6), 527–544. https://doi.org/10.1016/j.jaccpubpol.2018.10.004

Cavusoglu, H., Raghunathan, S., & Yue, W. T. (2008). Decision-theoretic and game-theoretic approaches to IT security investment. *Journal of Management Information Systems, 25*(2), 281–304. https://doi.org/10.2753/Mis0742-1222250211

Clearinghouse, P. R. (2009). *A chronology of data breaches*. https://privacyrights.org/data-breaches. Accessed 24 May 2023

CREST. (2021). *Cyber security incident response maturity assessment*. https://www.crest-approved.org/approved-services/cyber-security-incident-response-maturity-assessment/. Accessed 24 May 2023

Cyert, R. M., & March, J. G. (1963). *A behavioral theory of the firm*. Englewood Cliffs, NJ, 2(4), 169–187.

Dong, T., Zhu, S., Oliveira, M., & Luo, X. (2023). Making better IS security investment decisions: Discovering the cost of data breach announcements during the covid-19 pandemic. *Industrial Management & Data Systems, 123*(2), 630–652. https://doi.org/10.1108/IMDS-06-2022-0376

Eggers, J. P. (2012). All experience is not created equal: Learning, adapting, and focusing in product portfolio management. *Strategic Management Journal, 33*(3), 315–335. https://doi.org/10.1002/smj.956

Fedele, A., & Roner, C. (2022). Dangerous games: A literature review on cybersecurity investments. *Journal of Economic Surveys, 36*(1), 157–187. https://doi.org/10.1111/joes.12456

Fenz, S., Ekelhart, A., & Neubauer, T. (2011). Information security risk management: In which security solutions is it worth investing? *Communications of the Association for Information Systems, 28*(1), 22.

FireEye. (2021). *M-trends 2021*. https://www.mandiant.com/sites/default/files/2021-09/rpt-mtrends-2021-3.pdf. Accessed 24 May 2023

Fowler, K. (2016). *Data breach preparation and response: Breaches are certain, impact is not*. Syngress, Cambridge, MA, 20-23

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. A., Loeb, M. P., & Zhou, L. (2016). Investing in cybersecurity: Insights from the Gordon-Loeb model. *Journal of Information Security*, *7*(2), 11. https://doi.org/10.4236/jis.2016.72004

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2018). Empirical evidence on the determinants of cybersecurity investments in private sector firms. *Journal of Information Security*, *9*(2), 21. https://doi.org/10.4236/jis.2018.92010

Grance, T., Kent, K., & Kim, B. (2004). *Computer security incident handling guide*. NIST. http://www.eprivacy.com/lectures/IV-2_denialofservice/incident_prevention_and_response.pdf. Accessed 24 May

Grispos, G., Glisson, W. B., & Storer, T. (2015). Security incident response criteria: A practitioner's perspective. *The 21st Americas Conference on Information Systems*, Puerto Rico, USA, 35

Gupta, B. B., & Srinivasagopalan, S. (Eds.). (2020). *Handbook of research on intrusion detection systems*. IGI Global. https://doi.org/10.4018/978-1-7998-2242-4.

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications, 58*, 102726. https://doi.org/10.1016/j.jisa.2020.102726

Haunschild, P. R., & Sullivan, B. N. (2002). Learning from complexity: Effects of prior accidents and incidents on airlines' learning. *Administrative Science Quarterly, 47*(4), 609–643. https://doi.org/10.2307/3094911

Herath, H. S. B., & Herath, T. C. (2008). Investments in information security: A real options perspective with bayesian postaudit. *Journal of Management Information Systems, 25*(3), 337–375. https://doi.org/10.2753/Mis0742-1222250310

Hu, S., Hsu, C., & Zhou, Z. (2022). Security education, training, and awareness programs: Literature review. *Journal of Computer Information Systems, 62*(4), 752–764. https://doi.org/10.1080/08874417.2021.1913671

Huber, G. P. (1991). Organizational learning: The contributing processes and the literatures. *Organization Science, 2*(1), 88–115. https://doi.org/10.1287/orsc.2.1.88

Hui, K. L., Vance, A., & Zhdanov, D. (2016). *In MIS Quarterly research curations,* Ashley Bush and Arun Rai, (Eds.). https://www.misqresearchcurations.org/blog/2017/5/10/securing-digital-assets-1. Accessed 24 May 2023

IBM Security. (2019). *IBM ponemon institute 2019 cost of data breach report*. https://www.ibm.com/security/data-breach. Accessed 10 June 2022

IEC. (2016). *ISO/ IEC 27035:2016 - Information security incident management*. https://www.iso27001security.com/html/27035.html. Accessed 24 May 2023

Kemper, G. (2019). Improving employees' cyber security awareness. *Computer Fraud & Security, 2019*(8), 11–14. https://doi.org/10.1016/s1361-3723(19)30085-5

Kim, J. Y., & Miner, A. S. (2007). Vicarious learning from the failures and near-failures of others: Evidence from the U.S. Commercial banking industry. *Academy of Management Journal, 50*(3), 687–714.

Kwon, J., & Johnson, M. E. (2014). Proactive versus reactive security investments in the healthcare sector. *MIS Quarterly, 38*(2), 451.

Levitt, B., & March, J. G. (1988). Organizational learning. *Annual Review of Sociology, 14*(1), 319–338.

Madsen, P. M., & Desai, V. (2010). Failing to learn? The effects of failure and success on organizational learning in the global orbital launch vehicle industry. *Academy of Management Journal, 53*(3), 451–476. https://doi.org/10.5465/Amj.2010.51467631

March, J. G. (1996). Continuity and change in theories of organizational action. *Administrative Science Quarterly, 41*(2), 278–287. https://doi.org/10.2307/2393720

March, J. G., Sproull, L. S., & Tamuz, M. (1991). Learning from samples of one or fewer. *Organization Science, 2*(1), 1–13. https://doi.org/10.1287/orsc.2.1.1

McIlwraith, A. (2021). *Information security and employee behaviour: How to reduce risk through employee education, training and awareness*. Routledge.

Menges, F., & Pernul, G. (2018). A comparative analysis of incident reporting formats. *Computers & Security, 73*, 87–101. https://doi.org/10.1016/j.cose.2017.10.009

Miller, D., & Chen, M. J. (1994). Sources and consequences of competitive inertia - a study of the United States airline industry. *Administrative Science Quarterly, 39*(1), 1–23. https://doi.org/10.2307/2393492

Miner, A. S., Ciuchta, M. P., & Gong, Y. (2008). Organizational routines and organizational learning. In M. C. Becker (Ed.), *Handbook of organizational routines (pp. 152-186)*. Edward Elgar Publishing, Inc

Mitropoulos, S., Patsos, D., & Douligeris, C. (2006). On incident handling and response: A state-of-the-art approach. *Computers & Security, 25*(5), 351–370. https://doi.org/10.1016/j.cose.2005.09.006

Nagurney, A., & Shukla, S. (2017). Multifirm models of cybersecurity investment competition vs. Cooperation and network vulnerability. *European Journal of Operational Research, 260*(2), 588–600. https://doi.org/10.1016/j.ejor.2016.12.034

Nassimbeni, G., Sartor, M., & Dus, D. (2012). Security risks in service offshoring and outsourcing. *Industrial Management & Data Systems, 112*(3), 405–440. https://doi.org/10.1108/02635571211210059

Van Niekerk, J., & von Solms, R. (2004). Organisational learning models for information security education. *The ISSA 2004 Enabling Tomorrow Conference*, Midrand, South Africa. 1-11

Ozkaya, E. (2021). *Incident response in the age of cloud: Techniques and best practices to effectively respond to cybersecurity incidents (pp. 19-25)*. Packt Publishing.

Paulsen, C. (2016). Cybersecuring small businesses. *Computer, 49*(8), 92–97. https://doi.org/10.1109/mc.2016.223

Ponemon, I. (2019). *2019 global state of cybersecurity in small and medium-sized businesses*. https://www.cisco.com/c/dam/en/us/products/collateral/security/ponemon-report-smb.pdf. Accessed 24 May 2023

Rowe, B. R., & Gallaher, M. P. (2006). Private sector cyber security investment strategies: An empirical analysis. *The Fifth Workshop on The Economics of Information Security (WEIS06)*, Pittsburgh, PA. https://econinfosec.org/archive/weis2006/prog.html. Accessed 23 May 2023

Safi, R., Browne, G. J., & Naini, A. J. (2021). Mis-spending on information security measures: Theory and experimental evidence. *International Journal of Information Management*, *57*, 14. https://doi.org/10.1016/j.ijinfomgt.2020.102291

SANS. (2021). *Spends and trends: SANS 2020 IT cybersecurity spending survey*. https://sansorg.egnyte.com/dl/BH0WcC9VHj. Accessed 23 May 2023

Shedden, P., Smith, W., Scheepers, R., & Ahmad, A. (2009). Towards a knowledge perspective in information security risk assessments – an illustrative case study. *Australasian Conference on Information Systems (ACIS 2009) Proceedings,* 96

Shedden, P., Ahmad, A., & Ruighaver, A.B. (2011). Informal Learning in Security Incident Response Teams. *Australasian Conference on Information Systems (ACIS 2011) Proceedings,* 37

Simon, H. A. (1991). Bounded rationality and organizational learning. *Organization Science, 2*(1), 125–134. https://doi.org/10.1287/orsc.2.1.125

Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security, 58*, 216–229. https://doi.org/10.1016/j.cose.2015.12.006

Tang, C., & Liu, J. (2015). Selecting a trusted cloud service provider for your saas program. *Computers & Security, 50*, 60–73. https://doi.org/10.1016/j.cose.2015.02.001

Tatsumi, K.-i., & Goto, M. (2010). Optimal timing of information security investment: A real options approach. In *Economics of information security and privacy* (pp. 211–228). Springer. https://doi.org/10.1007/978-1-4419-6967-5_11

UKCS. (2020). *Cybersecurity breaches survey*. https://www.gov.uk/government/collections/cyber-security-breaches-survey. Accessed 24 May 2023

Weishaupl, E., Yasasin, E., & Schryen, G. (2018). Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. *Computers & Security, 77*, 807–823. https://doi.org/10.1016/j.cose.2018.02.001

West-Brown, M. J., Stikvoort, D., Kossakowski, K.-P., Killcrece, G., & Ruefle, R. (2003). *Handbook for computer security incident response teams (CSIRTs)* (pp. 9-21). Carnegie-Mellon University Pittsburgh PA, Software Engineering Institute

Wolff, J., & Lehr, W. (2017). Degrees of ignorance about the costs of data breaches: What policymakers can and can't do about the lack of good empirical data. *SSRN*. https://doi.org/10.2139/ssrn.2943867

Xu, F., Luo, X., Zhang, H., Liu, S., & Huang, W. (2019). Do strategy and timing in IT security investments matter? An empirical investigation of the alignment effect. *Information Systems Frontiers, 21*(5), 1069–1083. https://doi.org/10.1007/s10796-017-9807-6

Zhao, X., Xue, L., & Whinston, A. B. (2009). Managing interdependent information security risks: A study of cyberinsurance, managed security service and risk pooling. *ICIS 2009 Proceedings, 49*

Dr. Faheem Ahmed Shaikh obtained his Ph.D. in Management Information Systems from Nanyang Business School, Singapore. He works in the Cybersecurity group at the Faculty of Information Technology, University of Jyväskylä. Prior to his Ph.D., he worked for several years in security and telecommunications companies.

Dr. Mikko Siponen is Professor of Information Systems at the University of Jyväskylä. He holds a Ph.D. in Information Systems from the University of Oulu, Finland, and a Ph.D. in Philosophy from the University of Joensuu, Finland. His research interests include Cybersecurity, Computer ethics, and philosophical aspects of IS. He has published more than 150 research articles in journals including MIS Quarterly, Journal of the Association for Information Systems, Computers & Security, Information & Management, European Journal of Information Systems, Communications of the ACM, and others.