Computers & Security 124 (2022) 102974

Contents lists available at ScienceDirect

Computers & Security

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

Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity☆

Faheem Ahmed Shaikh*, Mikko Siponen

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

ARTICLE INFO

Article history:
Received 18 March 2022
Revised 5 October 2022
Accepted 19 October 2022
Available online 21 October 2022

Keywords:
Cybersecurity breach
Risk assessment
Top management team
Attention-based view
Post-breach management
Cybersecurity Governance

ABSTRACT

Information Systems (IS) research on managerial response to cybersecurity breaches has largely focused on externally oriented actions such as customer redressal and crisis response. Within the firm itself, a breach may be a symptom of systematic problems, and a narrow, siloed focus on only fixing immediate issues through technical fixes and controls might preclude other managerial actions to ensure future cybersecurity. Towards this end, Information Security Risk Assessments (ISRA) can help surface other vulnerabilities following a breach. While the role of governance in such exercises is emphasized in standards, it is undertheorized in IS research and lacks empirical evidence. We draw on the attention-based view to theorize that the principles of focus of attention, structural distribution of attention, and situated attention can lead to the top management team (TMT) according greater attention to cybersecurity following relatively high breach costs. Using firm level data, we find that high breach costs result in greater TMT attention to cybersecurity, while also making it more likely that firms will carry out an ISRA. Moreover, TMT attention to cybersecurity partially mediates the relation between breach costs and the decision to carry out an ISRA. We theorize that this is because the TMT is best positioned to oversee resource allocation, consider business implications, and centrally orchestrate an ISRA. Our findings stress the need for the cybersecurity function to work with the TMT in managing breach response.

1. Introduction

Cybersecurity breaches have implications for firms' market value, reputation, and competitive advantage (Goel and Shawky, 2009). The average cost to firms in the US due to breaches is witnessing an upward trend and was USD 133,000 in 2020 for firms with 250–999 employees (HISCOX, 2020). While cybersecurity standards such as the ISO/IEC 27000 (International Organization for Standardization/ International Electrotechnical Commission) recommend a range of technical and policy controls, these need to be customized to a firm's unique cybersecurity risk profile (Siponen and Willison, 2009). For this reason, firms need to actively engage in cybersecurity risk management.

Straub and Welke (1998) divide the cybersecurity risk planning and management process into four stages: deterrence, prevention, detection, and remediation. Deterrence, prevention, and detection are actions a firm takes before a breach is identified. Much along these lines, research has largely focused on cybersecurity management before breach identification. For instance, Cavusoglu et al. (2005) explore the role of intrusion detection systems while Kwon and Johnson (2013) emphasize how regulatory compliance can reduce the occurrence of data breaches. However, as we elaborate in the following, IS research on firm actions following a breach is lacking on several fronts.

Among the various kinds of breaches, data breaches have received overwhelming attention. However, outside of technical computer science and software engineering research, management-oriented research investigating data breaches mostly analyzes their market impact (Spanos and Angelis, 2016), while firm actions for security management following the breach take a backseat. Among the few studies that do investigate firm actions, the focus is largely on externally oriented actions. This includes customer redressal (Goode et al., 2017) and the role of corporate reputation and crisis response strategies to help protect firm market value (Gwebu et al., 2018; Knight and Nurse, 2020).

☆ This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

* Corresponding author.
E-mail addresses: faheem.a.shaikh@jyu.fi (F.A. Shaikh), mikko.t.siponen@jyu.fi (M. Siponen).

https://doi.org/10.1016/j.cose.2022.102974

This lack of focus in IS managerial-level research on internal firm actions is of concern because breaches could be a symptom of systemic issues, and the firm may continue to remain vulnerable (Say and Vasudeva, 2020). A narrow focus on fixing only the immediate issues through technical fixes or controls might preclude other managerial actions that are required to ensure long-term cybersecurity. Towards this end, Information Security Risk Assessments (ISRA), the first and most critical part of a risk management exercise can help surface other vulnerabilities (Shedden et al., 2009). Although the role of ISRA in ensuring cybersecurity is emphasized in industry standards, in actual practice firms tend to do it in a cursory manner, without reference to their actual situation, and on an intermittent basis (Webb et al., 2014). Small and medium enterprises with limited budgets and expertise are especially prone to such lapses (Ng et al., 2013). The ultimate responsibility for risk management initiatives and cybersecurity in organizations lies with the top management (IT Governance Institute, 2006, p. 21). This brings us to the second area of concern in the context of IS research on firm actions following a breach.

Research on the role of the top management team (TMT) in IS literature is largely limited to governance issues around IT management. While managing cybersecurity is acknowledged as part of IT governance, the actual functioning has received relatively less attention (Liu et al., 2020); even less so in the context of firm actions following breaches. Managing cybersecurity is not just the responsibility of the IT function, but the TMT needs to get involved too (Nolan and McFarlan, 2005; Rothrock et al., 2018). While IT can fix technical vulnerabilities and immediate issues following a breach, managing systemic issues and risks requires intervention from the senior management. The neglect in IS research of the TMT's role in firm internal actions following a breach is concerning given that the TMT can be expected to be involved due to potential financial and reputational damage to the firm (Say and Vasudeva, 2020).

In summary, our understanding of firm response to breaches is incomplete because it does not incorporate ISRAs or the involvement of the TMT. To improve our understanding of these issues, we investigate the research question: How do cybersecurity breach costs and TMT attention to cybersecurity influence firm decision to carry out an ISRA?

We use the attention-based view (Ocasio, 1997) to develop theory explaining how TMT attention to cybersecurity mediates a firm's decision to carry out an ISRA in the context of relatively high breach costs. We use data from four waves of the UK Cybersecurity Survey and find that TMT attention to cybersecurity increases in response to high breach costs. Moreover, TMT attention to cybersecurity partially mediates the positive relationship between breach costs and the decision to carry out an ISRA. Our theorizing provides a more nuanced explanation of how firms respond to breaches. It also helps impress the role of the TMT in managing cybersecurity issues, particularly in the wake of relatively high breach costs. We contribute to the literature on cybersecurity governance and ISRA.

2. Theory development

2.1. Cybersecurity

Cybersecurity is defined as the activity or process, ability, or capability whereby information and communication systems and the information contained therein are protected against damage, unauthorised use or modification, or exploitation (Homeland Security, 2021). A cybersecurity breach is an event that compromises the confidentiality, integrity, or availability of an information system or security policies or procedures (NIST, 2021). Phishing, denial of service, zero-day-exploits, ransomware, and unauthorised access to information systems are a few examples. Each of these breach types has potential economic and reputational consequences for the affected firm. Depending on the type of breach, economic costs might include those for detection, regulatory notification, customer redressal and compensation, litigation, loss of market value or investments, regulatory fines, extortion payments, and cost of lost business.

Most research on breach consequences has focused on their market impact (Spanos and Angelis, 2016), impact of post-breach customer redressal actions on firm market value (Rasoulian et al., 2017), and the market impact of corporate communication following the breach (Knight and Nurse, 2020). However, in terms of managerial actions aimed directly at improving cybersecurity following breaches, research is scarce. Some of it has focused on risk models emphasizing the role of containment and recovery after a data breach (Khan et al., 2021), as well as on the importance of a business continuity plan to minimize disruption (Cerullo and Cerullo, 2004).

Since risks inherent in having organizational IT infrastructure connected to the internet cannot be completely eliminated, IS research acknowledges that firms need to manage these risks (Sen and Borle, 2015; Sutton et al., 2008). However, risk management in IS research is portrayed as an activity to be carried out before the occurrence of a breach, whether to lower breach probability, or to mitigate its consequences (Bojanc and Jerman-Blažič, 2008; Cavusoglu et al., 2008; Spears and Barki, 2010; Wang et al., 2015; Zhao et al., 2013). Breaches could indicate systemic weaknesses in firm cybersecurity (Say, 2020) or that the firm is lagging behind the ever-evolving threat landscape (Borrett et al., 2014; Wilshusen and Powner, 2009). In such a scenario, ISRAs might also be required following breaches with material consequences for the firm.

2.2. Information security risk assessment (ISRA)

A risk assessment evaluates what could go wrong, the probability of occurrence of such an incident, and the harm if the incident did occur (Santos, 2018, p. 127). An ISRA involves prioritized ranking of IT assets and relating them with varying levels of associated risks and potential damage (Volchkov, 2019, p. 154). The objective is to optimize IT resources for security controls through prioritization of potential breaches by the degree of harm (Wangen et al., 2018). It also helps firms benchmark their current security practices against industry standards. We focus on ISRAs for this study because activities that constitute risk assessment as a first step, including security audits, penetration testing, or cybersecurity awareness testing (Chopra and Chaudhary, 2020, p. 134; Landoll, 2016, p. 41) are largely common across firms, making comparison easier. Subsequent decisions including risk acceptance or mitigation, part of the larger risk management process, are, however, unique to each firm based on its unique risk appetite and available resources (Santos, 2018).

In the context of data breaches, Kwon and Johnson (2014) argue that firms can choose to increase security investments following a breach, referring to such investments as reactive security investments. They differentiate these from proactive security investments done before a data breach. However, reactive security investments represent only one high-level aspect of firm actions following a breach. Directly addressing firm security to identify threats and vulnerabilities to prevent future occurrences via risk assessments is an important first step that should precede financial allocations (Shedden et al., 2010; Wangen, 2017). Firms first need to assess the current state of security in light of the latest breach to identify problem areas. Subsequently, the need for technical, human, and financial resources to operationalize agreed-upon requirements is determined (ISO, 2018). We therefore argue that in the context of a breach, a firm may first need to carry out

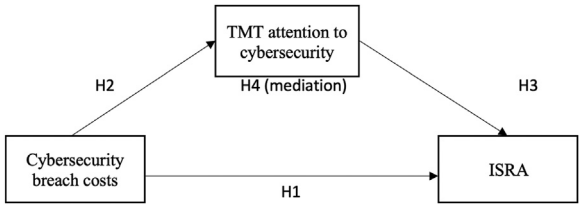

Fig. 1. Research model depicting hypotheses.

an ISRA. While ISRAs as part of preventive security measures represent the ideal scenario, those carried out in the context of high breach costs also do add value to a firm's cybersecurity posture in the following ways.

Firstly, ISRAs motivated by relatively high breach costs can use inputs from the breach to enhance the quality of the exercise and focus on vulnerable areas. Such actions promote corrective learning, leverage failure solutions to improve defense against future failures (Marcellus and Dada, 1991), and show agility (Yue and Cakanyildirim, 2007). In the field of manufacturing, learning associated with failure experiences has been shown to allow firms to cope better with future threats and failures (Haunschild and Sullivan, 2002).

Secondly, preventive security requires larger financial and time investments at the outset (Rowe and Gallaher 2006). However, it is difficult to quantify the return on cybersecurity investments because of intangible outcomes when 'nothing has happened' (Kwon and Johnson 2014). Because of this, many organizations might not even conduct risk management exercises until they have experienced negative breach consequences (Ng et al., 2013). Unlike preventive ISRAs, those motivated by high breach costs can avoid some of these issues, as they can target vulnerable areas identified in light of the latest breach. In such cases, firms can be more targeted and judicious in their choice of ISRA activities following breaches, with higher expected utility compared to an exercise that is wide-ranging and not based on actual breach experience.

Fig. 1. shows our conceptual model and we develop hypotheses describing these relationships in the following section.

2.3. Cybersecurity breach costs and ISRA

Firms may not always choose to carry out an ISRA following breaches. Their actions might not extend beyond the technical controls and corrective measures that suffice to remedy the exploited vulnerability. Therefore, while ISRAs are not a certainty following breaches, we now argue that the greater the breach costs, the more the likelihood of the firm carrying out an ISRA. This is for the following reasons.

Firstly, resources required for ISRAs depend on various factors including firm size, complexity of the IT network, scope of the exercise, and expertise (Landoll, 2016, p. 37). ISRAs can therefore be wide-ranging in terms of complexity and expenses. This can deter firms, especially smaller enterprises and those with financial constraints, from proactively carrying out the exercise (Weishaupl et al., 2018). Indeed, due to the difficulty in justifying returns on security investments, Ng et al. (2013) find that SMEs especially favor a wait and watch approach to security; most firms only react to failures rather than carry out preventive security measures. SMEs may also see security as hampering business processes, and investments in core business activities take precedence over security (Ng et al., 2013). Thus, for resource-constrained firms or for firms that have never carried out an ISRA, relatively high breach costs could prompt them to carry out one.

Secondly, high breach costs result in pressure from multiple stakeholders. Depending on the size of the firm, this could include customers, stockholders, boards of directors, investors, as well as media (Goode et al., 2017). This can push the firm to ride over inertia and initiate an ISRA and subsequent risk management actions to show that cybersecurity remains a priority and that substantial improvements are being made. An ISRA, in addition to being the first step in helping to reduce the likelihood of a future breach, can also reduce the probability of fines and litigation from customers and regulators in case of a breach; it demonstrates that the firm is taking care of its responsibilities to safeguard critical infrastructure (Li et al., 2020).

Given the frequency of cybersecurity attacks, firms can't be completely immune to breaches. Moreover, considering the financial investments, expertise, and time required, it is not feasible to conduct a large-scale ISRA after every small breach. In such cases, it may be more prudent for the firm to directly patch the vulnerability or fix security loopholes using technical and policy solutions than to carry out an ISRA. However, in case of relatively high breach costs, it implies that valuable firm assets have been compromised or business continuity has been severely affected due to cybersecurity vulnerabilities. This could be in the form of large-scale loss of customer personal data, intellectual property, or disruptions to systems availability. Consequently, due to pressure from stakeholders or to make substantial security improvements, the firm will feel even more impelled to carry out an ISRA. Therefore,

Hypothesis 1. (H1): Higher cybersecurity breach costs have a positive effect on the decision to carry out an ISRA.

2.4. TMT and the attention-based view (ABV)

Top Management Team (TMT) refers to the small group of the most influential executives at the top of the organization (Hambrick and Mason, 1984). It does not indicate a formal committee, but a group of the top few management executives that could include the CEO, CFO, CIO, CISO (Enns et al., 2003; Geiger and North, 2006) or senior management executives (Angwin et al., 2009; Menz, 2012). Research on TMTs gained traction to focus on the senior leadership as driving firm decision-making. Characteristics and actions of the TMT, for instance, have been found to influence firm strategy (Peterson et al., 1999, pp. 49–69).

IS research on the role of TMT in the management of the IT function has largely focused on IT governance. For instance, Weill and Ross (2005) highlight business needs, IT-business alignment, IT investment decision-making, and communication of IT initiatives as the main TMT governance responsibilities. Sambamurthy and Zmud (1999) investigate factors influencing the choice of IT governance mode, while Tallon et al. (2013) study practices for governing information artifacts.

Cybersecurity governance is a key component of TMT IT governance responsibilities (IT Governance Institute, 2006). This entails the establishment and maintenance of the control environment to manage risks relating to the confidentiality, integrity and availability of information and its supporting processes and systems (Moulton and Coles, 2003). However, while the role of the TMT in relation to cybersecurity management is repeatedly emphasized in standards and IS research (Nolan and McFarlan, 2005; Rothrock et al., 2018), empirical research is lacking. Moreover, the mechanism through which this role is operationalized remains to be theorized.

Due to limited attention resources, the TMT attends to the most critical stimuli internal or external to the firm, that are of potential consequence to firm performance (Rerup, 2009). The attention-based view theorizes that firm behavior is the outcome of how firms channel the attention of their decision-makers. It takes into account limited human rationality (March and Simon, 1958; Simon, 1991) to build its arguments. Essentially, decision-maker's

actions depend on what problems and solutions they focus on (Ocasio, 1997). Senior managers need to deliberately target and selectively attend to issues because they cannot effectively attend to all possible issues. This selective attention then dictates the kinds of actions decision-makers take. Attention in this perspective is defined as the 'noticing, encoding, interpreting, and focusing of time and effort by organizational decision-makers on specific issues - the range of problems, threats and opportunities, and solutions - the range of actions including routines, programs, and procedures' (Ocasio, 1997). This helps them reduce attention load and speed up decision-making. The attention-based view has been used in the past to study, for instance, opportunity seeking and monitoring (Hillman and Dalziel, 2003) and merger and acquisition (Yu et al., 2005). The attention-based view moves beyond the Upper Echelons Theory (Hambrick and Mason, 1984) by considering issues that the senior management actually attends to and acts upon, instead of only relying on TMT characteristics.

In the following, we use the principles of focus of attention, structural distribution of attention, and situated attention that make up the core attention-based view arguments, to theorize how high breach costs can lead to greater TMT attention to security.

2.5. Cybersecurity breach costs and TMT attention to security

The principle of focus of attention states that due to limited attention capacity, individuals decipher the relative importance of issues and solutions in a context (Ocasio et al., 2020, p. 15). They allocate attention based on issue salience and relevance (Rerup, 2009). Negative events can become salient and require TMT attention for action (Tuggle et al., 2010). In the present case, high breach costs point to below expectation performance in ensuring security. It represents a failure that may lead the TMT to allocate more attention to cybersecurity to prevent future breaches and to ensure that adequate preventive measures are undertaken.

The principle of structural distribution of attention contends that the position of organizational actors in hierarchy shapes their attention distribution (Ocasio, 1997). The TMT has a fiduciary responsibility to its stakeholders to monitor and assess firm performance (Hillman and Dalziel, 2003). By virtue of its ultimate decision-making position in firm hierarchy, it is responsible for oversight and needs to protect firm reputation. Regulations such as the Sarbanes-Oxley Act hold the TMT legally responsible for risk management and reporting, including information technology risks (Deloitte, 2004). Failure to perform these duties can expose the firm and TMT to liability and litigation (Andrus et al., 2019). This is evidenced in the Target data breach where the President and CEO resigned in the wake of a massive data breach (Douglas, 2014). This is also evidenced in the GDPR (General Data Protection Regulation) where directors can be held accountable for breaches of security standards, privacy regulations, and data management procedures (GDPR, 2018). Therefore, from a regulatory perspective, the final responsibility for breaches lies with the TMT, and by virtue of their position in the organizational structure, the TMT can be expected to accord greater attention to security issues, when faced with higher breach costs.

Finally, the principle of situated attention states that an individual's attention is a product of the situation (Fiske and Taylor, 2013, p. 201; Ocasio, 1997). Specifically, immediate situations confronting the TMT such as issue severity and task urgency (Seshadri and Shapira, 2001; Sullivan, 2010) draw the focus of attention to such issues. In the case of cybersecurity, it is expected that firms will be regularly subject to cyber-attacks. Cyber-attacks that translate into low-impact breaches may be frequent and not every minor breach needs to be brought to TMT attention. IT and cybersecurity personnel are responsible for remediating such minor breaches. However, breaches that result in relatively greater material damage to the firm represent urgent issues that require managerial attention and follow-up. For these reasons, the higher the breach costs, the more the TMT can be expected to accord attention to cybersecurity issues. Therefore,

Hypothesis 2. (H2): Higher cybersecurity breach costs have a positive effect on TMT attention to cybersecurity.

2.6. TMT attention to cybersecurity and ISRA

Even when customer personal data is not implicated, visible breaches could lead to stakeholders questioning firm's management of cybersecurity risks. With firm operations increasingly relying on digital infrastructure connected to the internet, the overall operational risk for a firm, in addition to many other risks, will also be a function of cybersecurity risks. The TMT is responsible for issues related to risk and compliance. This may be in the form of senior executives like a Chief Risk Officer or Chief Compliance Officer with designated responsibilities for risk management, or the senior management in case there is no designated individual (Li et al., 2010; Miller, 2014). IS research identifies individuals such as the CIO, CISO, CFO and CEO as C-suite executives responsible for managing various forms of cybersecurity risk (Banker et al., 2011; Benaroch and Chernobai, 2017; Feng and Wang, 2019; Vincent et al., 2015).

The attention-based view argues that the TMT will choose solutions that it focuses more on. In the present context, given the risk management responsibilities of the TMT, an ISRA can be expected to be a very likely solution following a breach. Indeed, ISRA is characterized as primarily a governance issue (Nolan et al., 2019) and active engagement of the board in IT risk management has been shown to reduce the likelihood of occurrence of breaches and consequent costs (Smith et al., 2018), making it a favorable solution.

In summary, if TMT attention to security is not high, it will be less likely that an ISRA will be carried out. IT security personnel may take technical measures to eliminate the vulnerabilities and may or may not carry out an ISRA without TMT involvement. On the other hand, as we have argued above, if the TMT pays more attention to security, an ISRA is a solution that the TMT will be highly likely to undertake. Therefore,

Hypothesis 3. (H3): TMT attention to cybersecurity has a positive effect on the decision to carry out an ISRA.

2.7. Cybersecurity breach costs and ISRA: mediation by TMT attention to cybersecurity

While the level of complexity and resource-intensity of ISRAs vary depending on a firm's unique context, Sun et al. (2006) characterize it as a complex decision requiring significant resources; carrying out one needs to be viewed as a business decision, and not just an IT decision. For instance, the firm needs to decide if its scope is limited to a technical assessment or whether it needs to be extended to cover employees' security awareness testing, whether a security audit is required, and whether the audit needs to be done internally, or by an independent auditor (Wangen, 2016). Moreover, the benefits of directing resources towards an ISRA against lower short-term performance in other areas like innovation need to be weighed (Raza et al., 2018). While cybersecurity personnel may be primarily concerned about the tactical aspects of an ISRA, the TMT is in a better position to evaluate the impact of the exercise vis-à-vis the overall strategic position of the firm. Approaches solely driven by compliance goals might lack alignment with the firm's business objectives (Overby, 2012). Understanding cybersecurity requirements requires assessing unique firm risks due to multiple aspects including processes, goals, risk tolerance, and culture. A standalone response from the IT function

might not account for strategic business or regulatory considerations. TMT intervention ensures that an ISRA as a response to high breach costs is aligned with business objectives. Therefore, TMT attention to cybersecurity can be expected to mediate firm response to high breach costs with an ISRA.

Although breaches target firm IT infrastructure, they have business implications (Spanos and Angelis, 2016). This implies the need for a strategic response that involves multiple departments (Ahmad et al., 2015). The TMT is in the best position to identify the most critical business assets that need to be protected and has a unified view of assets, operating divisions, culture, cybersecurity awareness, and training (Volchkov, 2019, p. 113). As an example, activities such as mergers and acquisitions have a major impact on IT infrastructure and can be expected to change the firm's IT security risk profile and ISRA requirements (Chang and Cho, 2017). The TMT is best positioned to direct an ISRA in the context of the ecosystem in which the firm is operating, the kind of visibility an IT department may not possess. An ISRA could suffer from inadequacies due to a fragmented approach if the TMT is not involved. For these reasons, an ISRA needs a centralized approach and high-level attention that the TMT can offer.

To summarize the foregoing arguments, the TMT is in the best position to oversee resource allocation, consider business implications, and carry out centralized orchestration of ISRA. Combined with H2 and H3, arguing for higher cost breaches attracting greater TMT attention, and greater TMT attention leading to an ISRA, we argue that TMT attention is the conduit through which high breach costs are likely to result in the decision to carry out an ISRA. The more attention the TMT allocates to cybersecurity following high breach costs, the more likely it will be that an ISRA will be carried out. Therefore,

Hypothesis 4. (H4): TMT attention to cybersecurity mediates the positive effect of cybersecurity breach costs on the decision to carry out an ISRA.

3. Method

3.1. Data

To test our hypotheses, we obtained data from the UK Cyber Security Breaches Survey conducted by the Department for Digital, Culture, Media, and Sport of the Government of the UK (DCMS, 2021). The survey is aimed at shaping future cybersecurity policy through understanding the types of cyber-threats faced by firms. The data is collected through a random probability telephone survey of UK businesses and charities. The survey specifically targeted small, medium, and large businesses across industries, as well as charities for balanced statistical representation. Random probability sampling was used to avoid selection bias. The data is collected annually; we use all four iterations of the survey, from 2018 to 2021. Firms were surveyed anonymously and were not tracked longitudinally. We use the entire survey population containing 8352 unique firm-year observations.

3.2. Measures

3.2.1. Dependent variable

Our dependent variable is ISRA. Firms were asked if they conducted an ISRA during the previous year. We coded a dummy variable as 1 if they did, and 0 otherwise.

3.2.2. Independent variable

Our independent variable is breach costs. We measured this as the total cost of all breaches experienced during the past year for the focal firm. The survey divided this variable into nine intervals, with cost in British Pounds Sterling ranging from 0 to 500,000 GBP. We used the same nine ordered intervals as specified in the survey. Specifically, the intervals in GBP were: 0, 1–500, 500–999, 1000–4999, 5000–9999, 10,000–19,999, 20,000–49,999, 50,000–99,999, and 100,000–499,999.

3.2.3. Mediator

Our mediator is TMT attention to cybersecurity. We measured this as the frequency with which a firm's directors or senior management were updated on cybersecurity issues during the past year. The survey measured this on a scale of 1 to 7, ranging from never to daily. Specifically, the scale values were: never, less than once a year, annually, quarterly, monthly, weekly, daily.

3.2.4. Controls

We include several control variables to rule out alternative explanations for why a firm might carry out ISRA more or less frequently. We controlled for firm size measured as the number of employees in 4 intervals, with the survey classifying firms as micro (1–9), small (10–49), medium (50–249), or large (250+). We controlled for the industrial sector. The data contained firms belonging to 12 industrial sectors in all; we created dummy variables for each industrial sector and used it as a control variable. Values were coded as 1 if the firm belonged to that specific industrial sector dummy, otherwise 0. We controlled for the type of organization, viz. whether a firm is for-profit, a charity or an educational institution. We controlled for a firm's online presence. Firms with greater online presence might be more circumspect with security, which could influence the frequency with which they do an ISRA. This variable was created as a composite measure based on responses to several questions indicated in appendix A. We also controlled for year fixed effects.

4. Results

We used structural equation modeling with the "medsem" package in Stata to test our hypotheses (Mehmetoglu, 2018). The package employs the Baron and Kenny method (Baron and Kenny, 1986) modified by Iacobucci et al. (2007) with the Sobel test (Sobel, 1987) to examine mediation.

We found no multicollinearity issues among tested variables as all variance inflation factors were well below 4. Table 1 shows the correlations among variables while Table 2 shows the coefficients for relationships among variables using the Baron and Kenny method (Baron and Kenny, 1986). The coefficients show that larger firms are more likely to carry out ISRA (β=0.077; p = 0.000; S.E.=0.012), and that TMTs in larger firms accord more attention to cybersecurity (β=0.083; p = 0.041; S.E.=0.040). Firms with greater online presence are more likely to carry out an ISRA (β=0.041; p = 0.002; S.E.=0.013), and TMTs in firms with greater online presence are more likely to attend to cybersecurity (β=0.137; p = 0.002; S.E.=0.043).

The direct positive effect of cybersecurity breach costs on ISRA in H1 is significant (β=0.028; p = 0.000; S.E.=0.008). The results confirm H2 stating that breach costs are positively associated with TMT attention to cybersecurity (β=0.104; p = 0.000; S.E.=0.027). H3 states that TMT attention to cybersecurity is positively associated with ISRA and is confirmed (β=0.077; p = 0.000; S.E.=0.008).

To test mediation in H4, upon addition of TMT attention to cybersecurity to the model, the direct effect remains significant (β=0.019; p = 0.018; S.E.=0.008). The Sobel test is significant and indicates partial mediation (Z = 3.495; p = 0.000). The ratio of indirect effect to total effect indicates that 29.3% of the effect of breach costs on ISRA is mediated by TMT attention to cybersecurity. Also, the ratio of indirect effect to direct effect indicates that

Table 1
Descriptive statistics.

Variable	Mean	S.D.	1	2	3	4	5
1. Cybersecurity breach costs	2.323	1.743	1				
2. TMT attention to cybersecurity	3.938	1.724	0.150***	1			
3. ISRA	0.428	0.494	0.112***	0.344***	1		
4. Online presence	2.504	1.335	0.096***	0.121***	0.181***	1	
5. Firm size	2.103	1.084	0.237***	0.188***	0.277***	0.235***	1

$n = 8352$.
*** $p < 0.01$.

Table 2
Hypothesis testing results.

Variables	Hypothesis	β	S.E.
DV: ISRA			
Cybersecurity breach costs	H1	0.028***	0.008
Online Presence		0.041***	0.013
Firm Size		0.077***	0.012
DV: TMT Attention to Cybersecurity			
Cybersecurity breach costs	H2	0.104***	0.027
Online Presence		0.137***	0.043
Firm Size		0.083**	0.041
DV: ISRA			
TMT Attention to Cybersecurity	H3	0.077***	0.008
Cybersecurity breach costs	H4	0.019**	0.008
Online Presence		0.033***	0.012
Firm Size		0.071***	0.011

*** $p<0.01$.
** $p<0.05$.Controls for Year, industry and type of organization included.

the mediated effect is 0.4 times as large as the direct effect of breach costs on ISRA.

5. Discussion

Our study focuses on firm actions in the context of high cybersecurity breach costs. Specifically, we examined the mediating role of TMT attention to cybersecurity in the decision to carry out an ISRA in response to high breach costs over a period. For this, we drew on the attention-based view (Ocasio, 1997) to theorize how the principles of focus of attention, structural distribution of attention, and situated attention can lead to the TMT according greater attention to cybersecurity in response to high breach costs. Moreover, given that the TMT is in the best position to oversee resource allocation, consider business implications, and carry out centralized orchestration of ISRA, TMT attention to cybersecurity mediates the effect of high breach costs on firms' decision to carry out an ISRA. Mediation analysis using data on four waves of the UK Cybersecurity Survey provides evidence for partial mediation by TMT attention to cybersecurity. This means that while there would be cases where the decision to carry out an ISRA might be independently taken by the cybersecurity function, evidence indicates that the TMT also plays an important role in the decision. The study contributes to literature on cybersecurity governance and cybersecurity risk management in the following ways.

Firstly, while the role of the Top Management Team in cybersecurity governance has been stressed early (Dutta and McCrohan, 2002), most research provides frameworks that are modifications to well-known industry standards (e.g. Veiga and Eloff (2007), Nicho (2018), Rebollo et al. (2014)), or is descriptive (Johnston and Hale, 2009; Moulton and Coles, 2003) with limited empirical evidence (Mishra, 2015; Yue and Cakanyildirim, 2007). Against this background, our study extends the literature on firm actions in response to high breach costs by theorizing and providing empirical evidence for the role of the TMT in carrying out ISRAs.

Secondly, our theory and empirical findings change the common "best practice" view of ISRAs portrayed in standards and risk management frameworks as largely preventive measures to calibrate technical security controls and resources. This view neglects their real-world implementation and additional role in response to high breach costs.

Finally, regarding the broader literature in this area, most studies rely on publicly available data on data breaches (Spanos and Angelis, 2016); this neglects a variety of other types of cybersecurity breaches. Even within this data, studies mostly consider public firms for analysis of the financial impact on stock markets. Our analysis alleviates this problem to some extent by examining actual financial impact on the focal firm, and firm actions in response. This empirical evidence complements case studies with a small set of firms that look at firm actions and TMT involvement in cybersecurity. The empirical evidence is especially critical to future research given the lack of hard evidence of the role of cybersecurity governance within firms.

Our study has practical implications for the role of the TMT in cybersecurity governance (AlGhamdi et al., 2020). It impresses the need for the TMT to attend to high breach costs as part of firm responsibility towards stakeholders. ISRAs require managerial decision-making and can be an effective tool for the TMT to exercise their role in improving cybersecurity. Partial mediation in the findings shows that the TMT has a role to play in this decision, although ISRAs may also be carried out without intervention from the TMT. TMTs can leverage their unique position that provides them with a centralized view of cybersecurity within their firms and consider risks in the wider business context, towards ensuring effective resource mobilization to carry out and improve the effectiveness of ISRAs. Firms can benefit from greater TMT attention to cybersecurity as this increased attention resulting in ISRAs can make cybersecurity responsive to changing cybersecurity requirements.

From the perspective of IT personnel, the findings impress the need for the cybersecurity function to keep the TMT informed and involved in effective response. Doing this may improve management buy-in for resource-intensive ISRAs. It can also help improve the quality and scope of ISRAs if the TMT champions the risk assessment exercise.

6. Conclusion

Our objective in this paper was to answer the research question: How do cybersecurity breach costs and TMT attention to cybersecurity influence firm decision to carry out an ISRA? Towards this end, we develop theory using the attention-based view and test our hypotheses with firm level data. We find empirical evidence that TMT attention to cybersecurity partially mediates the decision to carry out an ISRA in response to high breach costs over a period. While working towards this conclusion, we also find evidence that high breach costs result in greater TMT attention to cybersecurity, while also making it more likely that firms will carry out an ISRA.

This study advances our understanding of the role of top management in firm response to breaches, and the decision to carry out an ISRA. This is important because ISRAs are critical for maintaining cybersecurity, through downstream implications for technical and policy controls. Future research can develop and test theory to explain how TMTs may be involved in high-level decision-making regarding other operational aspects of cybersecurity such as policy design or the choice of software or hardware solutions for monitoring and breach prevention.

Declaration of Competing Interest

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

CRediT authorship contribution statement

Faheem Ahmed Shaikh: Conceptualization, Methodology, Investigation, Writing – original draft. **Mikko Siponen:** Writing – review & editing, Supervision.

Data availability

The data is publicly accessible and the manuscript has the URL to access it.

APPENDIX A

Questions making up variable 'Online Presence'

Question: Which of the following, if any, does your organization currently have or use?:

1. Accounts or pages on social media sites (e.g. Facebook or Twitter).
2. The ability for your customers to order, book or pay for products or services online.
3. An online bank account your organization or your clients pay into.
4. An industrial control system.
5. Personal information about your customers held electronically.
6. The ability for people to donate online.
7. The ability for your beneficiaries or service users to access services online

References

Ahmad, A., Maynard, S.B., Shanks, G., 2015. A case analysis of information systems and security incident responses. Int. J. Inf. Manag. 35 (6), 717–723. doi:10.1016/j.ijinfomgt.2015.08.001.

AlGhamdi, S., Win, K.T., Vlahu-Gjorgievska, E., 2020. Information security governance challenges and critical success factors: systematic review. Comput. Secur. 99, 39. doi:10.1016/j.cose.2020.102030, Article 102030.

Andrus, J.L., Withers, M.C., Courtright, S.H., Boivie, S., 2019. Go your own way: exploring the causes of top executive turnover. Strat. Manag. J. 40 (7), 1151–1168. doi:10.1002/smj.3020.

Angwin, D., Paroutis, S., Mitson, S., 2009. Connecting up strategy: are senior strategy directors a missing link? Calif. Manag. Rev. 51 (3), 74–94. doi:10.2307/41166494.

Banker, R.D., Hu, N., Pavlou, P.A., Luftman, J., 2011. CIO reporting structure, strategic positioning, and firm performance. MIS Q. 35 (2), 487–504. doi:10.2307/23044053.

Baron, R.M., Kenny, D.A., 1986. The moderator-mediator variable distinction in social psychological research: conceptual, strategic, and statistical considerations. J. Pers. Soc. Psychol. 51 (6), 1173–1182. doi:10.1037/0022-3514.51.6.1173.

Benaroch, M., Chernobai, A., 2017. Operational IT failures, IT value destruction, and board-level IT governance changes. MIS Q. 41 (3), 729–762. doi:10.25300/MISQ/2017/41.3.04.

Bojanc, R., Jerman-Blažič, B., 2008. An economic modelling approach to information security risk management. Int. J. Inf. Manag. 28 (5), 413–422. doi:10.1016/j.ijinfomgt.2008.02.002.

Borrett, M., Carter, R., Wespi, A., 2014. How is cyber threat evolving and what do organisations need to consider? J. Bus. Contin. Emer. Plan. 7 (2), 163–171.

Cavusoglu, H., Mishra, B., Raghunathan, S., 2005. The value of intrusion detection systems in information technology security architecture. Inf. Syst. Res. 16 (1), 28–46. doi:10.1287/isre.1050.0041.

Cavusoglu, H., Raghunathan, S., Yue, W.T., 2008. Decision-theoretic and game-theoretic approaches to IT security investment. J. Manag. Inf. Syst. 25 (2), 281–304. doi:10.2753/Mis0742-1222250211.

Cerullo, V., Cerullo, M.J., 2004. Business continuity planning: a comprehensive approach. Inf. Syst. Manag. 21 (3), 70–78. doi:10.1201/1078/44432.21.3.20040601/82480.11.

Chang, Y.B., Cho, W., 2017. The risk implications of mergers and acquisitions with information technology firms. J. Manag. Inf. Syst. 34 (1), 232–267. doi:10.1080/07421222.2017.1297641.

Chopra, A., Chaudhary, M., 2020. Implementing an Information Security Management System: Security management Based on ISO 27001 Guidelines, 1st ed. Apress, Berkeley, CA doi:10.1007/978-1-4842-5413-4.

DCMS. (2021). Cyber Security Breaches Survey 2021. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021

Deloitte. (2004). Sarbanes-Oxley Section 404: 10 Threats to Compliance. Retrieved November 10 from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-aers-assur-ten-threats-sep2004.pdf

Douglas, D., 2014. Target CEO Resigns After Massive Data Breach May 5, 2014. The Washington Post https://www.washingtonpost.com/business/economy/target-ceo-resigns-after-massive-data-breach/2014/05/05/ef6cbee2-d457-11e3-8a78-8fe50322a72c_story.html.

Dutta, A., McCrohan, K., 2002. Management's role in information security in a cyber economy. Calif. Manag. Rev. 45 (1), 67–87. doi:10.2307/41166154.

Enns, H.G., Huff, S.L., Higgins, C.A., 2003. CIO lateral influence behaviors: gaining peers' commitment to strategic information systems. MIS Q. 27 (1), 155–176. doi:10.2307/30036522.

Feng, C., Wang, T., 2019. Does CIO risk appetite matter? Evidence from information security breach incidents. Int. J. Account. Inf. Syst. 32, 59–75. doi:10.1016/j.accinf.2018.11.001.

Fiske, S.T., Taylor, S.E., 2013. Social Cognition: From Brains to Culture, 2nd ed. Sage doi:10.1016/j.cose.2015.12.006.

GDPR. (2018). *General Data Protection Regulation - Right to Compensation and Liability*. https://gdprinfo.eu/en-article-82

Geiger, M.A., North, D.S., 2006. Does hiring a new CFO change things? An investigation of changes in discretionary accruals. Account. Rev. 81 (4), 781–809.

Goel, S., Shawky, H.A., 2009. Estimating the market impact of security breach announcements on firm value. Inf. Manag. 46 (7), 404–410. doi:10.1016/j.im.2009.06.005.

Goode, S., Hoehle, H., Venkatesh, V., Brown, S.A., 2017. User compensation as a data breach recovery action: an investigation of the Sony Playstation network breach. MIS Q. 41 (3), 703–727.

Gwebu, K.L., Wang, J., Wang, L., 2018. The role of corporate reputation and crisis response strategies in data breach management. J. Manag. Inf. Syst. 35 (2), 683–714. doi:10.1080/07421222.2018.1451962.

Hambrick, D.C., Mason, P.A., 1984. Upper echelons - the organization as a reflection of its top managers. Acad. Manag. Rev. 9 (2), 193–206. doi:10.2307/258434.

Haunschild, P.R., Sullivan, B.N., 2002. Learning from complexity: effects of prior accidents and incidents on airlines' learning. Adm. Sci. Q. 47 (4), 609–643. doi:10.2307/3094911.

Hillman, A.J., Dalziel, T., 2003. Boards of directors and firm performance: integrating agency and resource dependence perspectives. Acad. Manag. Rev. 28 (3), 383–396. doi:10.2307/30040728.

HISCOX. (2020). Hiscox Cyber Readiness Report. https://www.hiscox.co.uk/sites/uk/files/documents/2020-06/Hiscox_Cyber_Readiness_Report_2020_UK.PDF

Homeland Security. (2021). Cybersecurity Glossary. Retrieved 10 October 2021 from https://niccs.cisa.gov/about-niccs/cybersecurity-glossary

Iacobucci, D., Saldanha, N., Deng, X., 2007. A meditation on mediation: evidence that structural equations models perform better than regressions. J. Consum. Psychol. 17 (2), 139–153. doi:10.1016/S1057-7408(07)70020-7.

ISO, 2018. ISO/IEC 27005: 2018: Information Technology–Security Techniques–Information Security Risk Management. International Organization for Standardization https://www.iso.org/standard/75281.html.

IT Governance Institute, 2006. Information Security governance: Guidance for Boards of Directors and Executive Management, 2nd ed. ISACA.

Johnston, A.C., Hale, R., 2009. Improved security through information security governance. Commun. ACM 52 (1), 126–129. doi:10.1145/1435417.1435446.

Khan, F., Kim, J.H., Mathiassen, L., Moore, R., 2021. Data breach management: an integrated risk model. Inf. Manag. 58 (1). doi:10.1016/j.im.2020.103392.

Knight, R., Nurse, J.R.C., 2020. A framework for effective corporate communication after cyber security incidents. Comput. Secur. 99, 18. doi:10.1016/j.cose.2020.102036, Article 102036.

Kwon, J., Johnson, M.E., 2013. Health-care security strategies for data protection and regulatory compliance. J. Manag. Inf. Syst. 30 (2), 41–65. doi:10.2753/Mis0742-1222300202.

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

Landoll, D.J., 2016. Information Security Policies, Procedures, and Standards: A Practitioner's Reference, 1st ed. Auerbach Publications doi:10.1201/9781315372785.

Li, C., Sun, L., Ettredge, M., 2010. Financial executive qualifications, financial executive turnover, and adverse SOX 404 opinions. J. Account. Econ. 50 (1), 93–110. doi:10.1016/j.jacceco.2010.01.003.

Li, H., No, W.G., Boritz, J.E., 2020. Are external auditors concerned about cyber incidents? Evidence from audit fees. Audit.: J. Pract. Theory 39 (1), 151–171. doi:10.2308/ajpt-52593.
Liu, C.-W., Huang, P., Lucas, H.C., 2020. Centralized IT decision making and cybersecurity breaches: evidence from U.S. Higher education institutions. J. Manag. Inf. Syst. 37 (3), 758–787. doi:10.1080/07421222.2020.1790190.
Marcellus, R.L., Dada, M., 1991. Interactive process quality improvement. Manag. Sci. 37 (11), 1365–1376. doi:10.1287/mnsc.37.11.1365.
March, J.G., and Simon, H.A. (1958). Organizations.
Mehmetoglu, M., 2018. Medsem: a stata package for statistical mediation analysis. Int. J. Comput. Econ. Econometr. 8 (1), 63–78.
Menz, M., 2012. Functional top management team members: a review, synthesis, and research agenda. J. Manag. 38 (1), 45–80. doi:10.1177/0149206311421830.
Miller, G.P. (2014). The compliance function: an overview. *NYU Law and Economics Research Paper No. 14-36*.
Mishra, S., 2015. Organizational objectives for information security governance: a value focused assessment. Inf. Comput. Secur. 23 (2), 122–144. doi:10.1108/ICS-02-2014-0016.
Moulton, R., Coles, R.S., 2003. Applying information security governance. Comput. Secur. 22 (7), 580–584. doi:10.1016/S0167-4048(03)00705-3.
Ng, Z.X., Ahmad, A., Maynard, S.B., 2013. *Information security management: Factors that influence security investments in SMEs* Australasian Information Security Management Conference.
Nicho, M., 2018. A process model for implementing information systems security governance. Inf. Comput. Secur. 26 (1), 10–38. doi:10.1108/Ics-07-2016-0061.
NIST, 2021. Cybersecurity Basics Glossary. National Institute of Standards and Technology Retrieved 10 October 2021 from https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary .
Nolan, C., Lawyer, G., Dodd, R.M., 2019. Cybersecurity: today's most pressing governance issue. J. Cyber Policy 4 (3), 425–441. doi:10.1080/23738871.2019.1673458.
Nolan, R., McFarlan, F.W., 2005. Information technology and the board of directors. Harv. Bus. Rev. 83 (10), 96.
Ocasio, W., 1997. Towards an attention-based view of the firm. Strat. Manag. J. 18, 187–206. https://doi.org/10.1002/(SICI)1097-0266(199707)18:1+<3C187::AID-SMJ936>3E3.0.CO;2-K.
Ocasio, W., Rhee, L., and Milner, D. (2020). *Attention, knowledge, and organizational learning*. https://doi.org/10.1093/oxfordhb/9780190263362.013.33
Peterson, R.S., Owens, P.D., Martorana, P.V., 1999. Cause or effect? An Investigation of the Relationship Between TMT Group Dynamics and Organizational Performance. JAI Press, Greenwich, CT Vol. 2.
Rasoulian, S., Grégoire, Y., Legoux, R., Sénécal, S., 2017. Service crisis recovery and firm performance: insights from information breach announcements. J. Acad. Mark. Sci. 45 (6), 789–806. doi:10.1007/s11747-017-0543-8.
Raza, H., Baptista, J., Constantinides, P., 2018. Paradoxical tensions between digital innovation and information security compliance in a large financial services organization. The 34th EGOS Colloquium.
Rebollo, O., Mellado, D., Fernandez-Medina, E., 2014. ISGcloud: a security governance framework for cloud computing. Comput. J. 58 (10), 2233–2254. doi:10.1093/comjnl/bxu141.
Rerup, C., 2009. Attentional triangulation: learning from unexpected rare crises. Org. Sci. 20 (5), 876–893. doi:10.1287/orsc.1090.0467.
Rothrock, R.A., Kaplan, J., Van der Oord, F., 2018. The board's role in managing cybersecurity risks. MIT Sloan Manag. Rev. 59 (2), 12–15.
Sambamurthy, V., Zmud, R.W., 1999. Arrangements for information technology governance: a theory of multiple contingencies. MIS Q. 23 (2), 261–290. doi:10.2307/249754.
Santos, O., 2018. Developing Cybersecurity Programs and Policies, 3rd ed. Pearson IT Publication.
Say, G., Vasudeva, G., 2020. Learning from digital failures? The effectiveness of firms' divestiture and management turnover responses to data breaches. Strategy Sci. 5 (2), 117–142. doi:10.1287/stsc.2020.0106.
Sen, R., Borle, S., 2015. Estimating the contextual risk of data breach: an empirical approach. J. Manag. Inf. Syst. 32 (2), 314–341. doi:10.1080/07421222.2015.1063315.
Seshadri, S., Shapira, Z., 2001. Managerial allocation of time and effort: the effects of interruptions. Manag. Sci. 47 (5), 647–662. doi:10.1287/mnsc.47.5.647.10481.
Shedden, P., Smith, W., Ahmad, A., 2010. Information security risk assessment: towards a business practice perspective. The 8th Australian Information Security Management Conference.
Shedden, P., Smith, W., Scheepers, R., Ahmad, A., 2009. Towards a knowledge perspective in information security risk assessments – an illustrative case study. The 9th Australian Information Security Management Conference.
Simon, H.A., 1991. Bounded rationality and organizational learning. Org. Sci. 2 (1), 125–134. doi:10.1287/orsc.2.1.125.
Siponen, M., Willison, R., 2009. Information security management standards: problems and solutions. Inf. Manag. 46 (5), 267–270. doi:10.1016/j.im.2008.12.007.
Smith, T.J., Higgs, J.L., Pinsker, R.E., 2018. Do auditors price breach risk in their audit fees? J. Inf. Syst. 33 (2), 177–204. doi:10.2308/isys-52241.
Sobel, M.E., 1987. Direct and indirect effects in linear structural equation models. Sociol. Methods Res. 16 (1), 155–176. doi:10.1177/0049124187016001006.
Spanos, G., Angelis, L., 2016. The impact of information security events to the stock market: a systematic literature review. Comput. Secur. 58, 216–229. doi:10.1016/j.cose.2015.12.006.
Spears, J.L., Barki, H., 2010. User participation in information systems security risk management. MIS Q. 34 (3), 503–522.
Straub, D.W., Welke, R.J., 1998. Coping with systems risk: security planning models for management decision making. MIS Q. 22 (4), 441–469. doi:10.2307/249551.
Sullivan, B.N., 2010. Competition and beyond: problems and attention allocation in the organizational rulemaking process. Org. Sci. 21 (2), 432–450. doi:10.1287/orsc.1090.0436.
Sun, L.L., Srivastava, R.P., Mock, T.J., 2006. An information systems security risk assessment model under the Dempster-Shafer theory of belief functions. J. Manag. Inf. Syst. 22 (4), 109–142. doi:10.2753/Mis0742-1222220405.
Sutton, S.G., Hampton, C., Khazanchi, D., Arnold, V., 2008. Risk analysis in extended enterprise environments: identification of critical risk factors in B2B e-commerce relationships. J. Assoc. Inf. Syst. 9 (3–4), 151–174.
Tallon, P.P., Ramirez, R.V., Short, J.E., 2013. The information artifact in IT governance: toward a theory of information governance. J. Manag. Inf. Syst. 30 (3), 141–177. doi:10.2753/Mis0742-1222300306.
Tuggle, C.S., Sirmon, D.G., Reutzel, C.R., Bierman, L., 2010. Commanding Board of Director attention: investigating how organizational performance and CEO duality affect board members' attention to monitoring. Strat. Manag. J. 31 (9), 946–968. doi:10.1002/smj.847.
Veiga, A.D., Eloff, J.H.P., 2007. An information security governance framework. Inf. Syst. Manag. 24 (4), 361–372. doi:10.1080/10580530701586136.
Vincent, N.E., Higgs, J.L., Pinsker, R.E., 2015. IT governance and the maturity of IT risk management practices. J. Inf. Syst. 31 (1), 59–77. doi:10.2308/isys-51365.
Volchkov, A., 2019. Information Security Governance - Framework and Toolset for CISOs and Decision Makers. CRC Press.
Wang, J.G., Gupta, M., Rao, H.R., 2015. Insider threats in a financial institution: analysis of attack-proneness of information systems applications. MIS Q. 39 (1), 91–105.
Wangen, G., 2016. An initial insight into information security risk assessment practices. 2016 Federated Conference on Computer Science and Information Systems (FedCSIS).
Wangen, G., 2017. Information security risk assessment: a method comparison. Computer (Long Beach Calif) 50 (4), 52–61. doi:10.1109/MC.2017.107.
Wangen, G., Hallstensen, C., Snekkenes, E., 2018. A framework for estimating information security risk assessment method completeness: core unified risk framework, CURF. Int. J. Inf. Secur. 17 (6), 681–699. doi:10.1007/s10207-017-0382-0.
Webb, J., Ahmad, A., Maynard, S.B., Shanks, G., 2014. A situation awareness model for information security risk management. Comput. Secur. 44, 1–15. doi:10.1016/j.cose.2014.04.005.
Weill, P., Ross, J., 2005. A matrixed approach to designing IT governance. MIT Sloan Manag. Rev. 46 (2), 26.
Weishaupl, E., Yasasin, E., Schryen, G., 2018. Information security investments: an exploratory multiple case study on decision-making, evaluation and learning. Comput. Secur. 77, 807–823. doi:10.1016/j.cose.2018.02.001.
Wilshusen, G.C., and Powner, D.A. (2009). *Cybersecurity: Continued efforts are Needed to Protect Information Systems from Evolving Threats*. https://apps.dtic.mil/sti/citations/ADA516401
Yu, J.S., Engleman, R.M., Van de Ven, A.H., 2005. The integration journey: an attention-based view of the merger and acquisition integration process. Org. Stud. 26 (10), 1501–1528. doi:10.1177/0170840605057071.
Yue, W.T., Cakanyildirim, M., 2007. Intrusion prevention in information systems: reactive and proactive responses. J. Manag. Inf. Syst. 24 (1), 329–353. doi:10.2753/Mis0742-1222240110.
Zhao, X., Xue, L., Whinston, A.B., 2013. Managing interdependent information security risks: cyberinsurance, managed security services, and risk pooling arrangements. J. Manag. Inf. Syst. 30 (1), 123–152. doi:10.2753/Mis0742-1222300104.

Dr. Faheem Ahmed Shaikh obtained his Ph.D. in Management Information Systems from Nanyang Business School, Singapore. He is presently a Postdoctoral Research Fellow in the Cybersecurity group at the Faculty of Information Technology, University of Jyväskylä. Prior to his Ph.D., he worked for several years in cybersecurity startups.

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 70 articles in journals including Computers & Security, MIS Quarterly, Journal of the Association for Information Systems, Information & Management, European Journal of Information Systems, Communications of the ACM, IEEE Computer, IEEE IT Professional, among others.