Received: 25 August 2021 | Revised: 20 April 2023 | Accepted: 3 May 2023

DOI: 10.1111/isj.12441

RESEARCH ARTICLE

WILEY

Peering through the lens of high-reliability theory: A competencies driven security culture model of high-reliability organisations

Farkhondeh Hassandoust[1] | **Allen C. Johnston**[2]

[1]Business Information Systems, Auckland University of Technology, Auckland, New Zealand

[2]Information Systems, Statistics, and Management Science, Culverhouse College of Business, The University of Alabama, Tuscaloosa, Alabama, USA

Correspondence
Allen C. Johnston, Information Systems, Statistics, and Management Science, Culverhouse College of Business, The University of Alabama, Tuscaloosa, AL 35487, USA.
Email: ajohnston@cba.ua.edu

Abstract

To improve organisational safety and enhance security efficiency, organisations seek to establish a culture of security that provides a foundation for how employees should approach security. There are several frameworks and models that provide a set of requirements for forming security cultures; however, for many organisations, the requirements of the frameworks are difficult to meet, if not impossible. In this research, we take a different perspective and focus on the core underlying competencies that high-reliability organisations (HROs) have shown to be effective in achieving levels of risk tolerance consistent with the goals of a security culture. In doing so we draw on high-reliability theory to develop a Security Culture Model that explains how a firm's supportive and practical competencies form its organisational security culture. To refine and test the model, we conducted a developmental mixed-method study using interviews and survey data with professional managers involved in the information security (InfoSec) programs within their respective HROs. Our findings emphasise the importance of an organisation's supportive and practical competencies for developing a culture of security. Our results suggest that organisations' security cultures are a product of their InfoSec practices and that organisational mindfulness, top management involvement and organisational structure are key to the development of those practices.

KEYWORDS
high-reliability organisation, high-reliability theory, information security practices, organisational competencies, organisational mindfulness, security culture

1 | INTRODUCTION

While several definitions of security culture exist (Da Veiga et al., 2020; Da Veiga & Martins, 2015; Van Niekerk & Von Solms, 2010), we define it as *an organisational construct that reflects both the shared tacit assumptions and espoused values of an organisation in relation to security events and the collective and individual responses to those events* (Alshaikh, 2020). As employees go about their daily responsibilities, it is the security culture that guides their assumptions about what actions may introduce risk to the organisation, or conversely, reduce such risk. The security culture also guides how employees communicate with each other and respond to formal and informal organisational forces (Karlsson et al., 2015).

For many organisations, however, a security culture does not exist, or is under-developed. In such cases, these organisations are relatively vulnerable to a variety of external and internal threats, errors, or accidents (Da Veiga et al., 2020). These organisations generally lack the ability to coordinate their responses in a timely and meaningful way; with inactive or ineffective socio-cultural norms often the cause (Ruighaver et al., 2007). Moreover, an under-developed security culture leaves an organisation lacking the necessary foundation for self-inspection, reflection and ultimately, error correction and improvement (Karlsson et al., 2015; Ruighaver et al., 2007).

Both academics and practitioners have explored a number of factors and metrics essential to an effective, lasting security culture (Da Veiga & Martins, 2017; Martins & Eloff, 2002; Van Niekerk & Von Solms, 2010). These efforts have produced numerous frameworks and models that serve to explain the requirements of a security culture (Uchendu et al., 2021). These frameworks and models are most often forged from the established concepts of organisational culture research (Schein, 2010) and include important requirements such as security awareness, security policy, user management, national culture, rewards and sanctions, among others. However, recent reviews of the security culture literature argue that the extant frameworks do not account for the underlying supportive competencies that organisations must possess to derive value from implementing the requirements of a security culture (Uchendu et al., 2021). For example, for an organisation to successfully impose sanctions or offer rewards as part of its security culture, it is necessary to first determine if the organisation has the appropriate systems, structures and knowledge to successfully implement them; its competencies. A security culture does not happen by accident and without an appropriate set of competencies to anchor to, it will not be successful (Dube & Mohanty, 2020; Siponen, 2002).

Though multiple definitions exist, a firm's competencies can be described as *its combination of knowledge and actions that allow it to excel in some context relative to others* (Bogner & Thomas, 1992; Kabue & Kilika, 2016). For most organisations, some competencies emerge organically as a byproduct of the various activities they engage in to provide value to their stakeholders and their competitive position within their industries (Dhillon et al., 2016; Martins & Eloff, 2002). A few of these will be identified as core to the organisation's strategic and/or operational success (i.e., its core competencies). A firm's competencies can be further divided among those that are practical in nature versus those that are more supportive. In the context of forming a security culture, we refer to a firm's *practical competencies as the set of actions enacted through its employees to secure its information assets* (Ahmad et al., 2014), while we refer to a firm's *supportive competencies as the set of systems, structures and knowledge that motivate and drive the success of its practical competencies* (Uchendu et al., 2021). The security culture literature is rather clear that the practical competencies of a firm largely equate to its InfoSec practices–the actions organisations engage in to protect from, detect, respond to and reduce losses caused by lapses in security (Baskerville et al., 2014; Lu et al., 2017). Most of the security culture frameworks are oriented around the need to establish effective InfoSec

practices as a determinant of a security culture (Uchendu et al., 2021). The supportive competencies for those InfoSec practices, however, are more difficult to identify and implement, and the security culture literature provides little to no elucidation of what they are and how they help underpin the success of a firm's InfoSec practices.

What the literature does provide, however, is a theoretical basis and practical template for gaining this understanding. Specifically, high-reliability theory (HRT) provides a lens for understanding effective security cultures as products of a firm's practical (i.e., InfoSec practices) and supportive competencies. HRT helps explain that in order for a security culture to form, the assumptions, norms and decision making practices related to security that take place within an organisation must yield positive, reliable outcomes (Boin & Schulman, 2008; Schulman, 2020). High-reliability organisations (HROs) follow the tenets of HRT and can serve as templates for other firms seeking to achieve security resilience through the development of an effective security culture (Burns, 2019). HROs are outstanding sociotechnical systems that can operate an almost error-free environment, where most other organisations are in a perpetual state of incident risk (Salovaara et al., 2019; Weick & Sutcliffe, 2001).

Recently, interest in HRO utilisation has grown among information systems researchers (e.g., Burns, 2019; Butler & Gray, 2006; Salovaara et al., 2019), but HRO studies have not yet investigated InfoSec operations and culture. While research has presented traditional HROs as achieving high-reliability through a cognitive orientation called organisational mindfulness that optimises incident prediction and prioritises safety (Weick et al., 1999), the literature suggests high-reliability is also a function of an HRO's organisational structure and top management involvement. How those supportive competencies interact to form their influence on security cultures through their support of a firm's InfoSec practices, however, has not been expressed in the HRT or HRO literature. To that end, we ask *how do* the *supportive competencies of HROs relate with their InfoSec practices to influence their security cultures?*

To answer this question, we draw from the HRT literature and the insights of HRO security professionals to develop and test a security culture model (SCM) as a reflection of an HRO's InfoSec practices and key supportive competencies. In doing so, we provide academics and practitioners with an understanding of how the vital organisational supportive competencies of firms with established track records of security resiliency interact to influence security cultures. Further, the findings of this study reveal the critical importance of organisational mindfulness, organisational structure and top management involvement to the development of an effective security culture.

The remainder of the manuscript proceeds as follows. In the section that follows (Section 2), we describe the existing literature on security culture, while in Section 3 we discuss HRT, including practical and supportive competencies as well as a conceptual model of an HRO's security culture. In Section 4, we describe our mixed-method research design, where the qualitative results are first presented in support of a SCM and related hypotheses, followed by the results of a quantitative test of the model. We present a discussion of our findings, including a set of meta-inferences and implications for research and practice, as well as limitations and future research directions in Section 5. We conclude the manuscript in Section 6.

2 | PRIOR RESEARCH ON SECURITY CULTURE

A security culture is a typically an organisational subculture, derived from the organisation's overall culture, but specific to the purpose of InfoSec (Chen et al., 2015; Da Veiga & Martins, 2017; Pfleeger et al., 2015). The general purpose for cultivating a security culture is to help control and diminish the security and privacy risks to an organisation's digital assets (Nel & Drevin, 2019). Moreover, the aims and objectives of an organisation's security culture should be aligned with its formal business processes and underlying organisational culture (Dhillon & Backhouse, 2001) and should include all technical controls and socio-cultural countermeasures (Chen et al., 2015).

A security culture is a collection of implicit and explicit forces that form employees' security attitudes and behaviours over time, which plays a significant role in the success of InfoSec management in an organisation (Chen et al., 2015). Organisations are mainly equipped with technical controls and countermeasures in place, while in order

to mitigate InfoSec risks, organisations must emphasise creating and growing a security-aware culture that accounts for the various range of potential InfoSec threats (Nel & Drevin, 2019; O'Brien et al., 2013). InfoSec protection should be a natural part of employees' daily tasks; that is, InfoSec should be integrated into the corporate culture and employees' InfoSec behaviours in the workplace (Thomson et al., 2006).

Security cultures have been examined from a number of perspectives, including the organisational principles and frameworks upon which they are based (e.g., Da Veiga & Martins, 2015; Martins & Eloff, 2002; Ruighaver et al., 2007; Zakaria & Gani, 2003), as well as the organisational cultural and behavioural characteristics that help define them (e.g., Martins & Eloff, 2002). Within this area of study, researchers have explored a number of factors that influence the development of security cultures, such as the role of external environmental factors (e.g., political, socio-cultural) and internal factors, such as chief information security officers (CISOs), top management support, change management, education and training, monitoring and enforcement and security policies (e.g., Ashenden & Sasse, 2013; Chen et al., 2015; Da Veiga et al., 2020), among others. The empirical studies that have explored security cultures are summarised in Table S1 in the supplementary document. However, very few of these studies have focused on the key competencies of an organisation that facilitate its security culture; not just their capabilities, but rather the capabilities to which they have become proficient. So, as it stands, our understanding of the underlying practical and supportive competencies that a firm must possess in order to establish an effective security culture is underdeveloped, at best. Given the importance of sustained focus and repeated success to the development and sustenance of a culture, we believe HRT provides an appropriate lens for developing this understanding.

3 | HIGH-RELIABILITY THEORY

HRT is an established theory, with robust research streams in healthcare, business, sociology and other disciplines (Boin & Schulman, 2008; Sagan, 1995; Wolf, 2005). Many HRT studies have focused on specific organisations that could potentially encounter a major failure with substantial consequences, but have shown themselves to be highly-reliable despite the high-risk environments in which they operate (e.g., nuclear power plants, aircraft carriers, air traffic control; e.g., Porte & Consolini, 1998; Roberts et al., 1994) as a result of a careful procedure by which risks are monitored, assessed and mitigated (Perrow, 1994). These organisations, referred to as HROs, show an immense capacity to react to and learn from incidents, to avoid disabling, and to rearrange their practices to diminish the likelihood of future incidents and prevent major failures (Weick & Sutcliffe, 2001). HROs maintain a minimum level of performance variance by minimising errors, despite a dynamic and complex organisational environment (Butler & Gray, 2006).

HRT provides explanations of the processes and practices an organisation can execute to guarantee continuous organisational reliability and mitigate or even reduce the probability of incidents (Roberts, 1990a, 1990b). HRT focuses on the processes of a dynamic situation and provides insights related to the time period leading up to an incident. HRT helps explain that an incident happens because an organisation has failed to be reliable and has not followed recommended practices. HRT further explains that HROs demand safety and follow two strategies for achieving it, anticipation and resilience. Through anticipation, HROs attempt to avoid possible incidents, while through resilience HROs attempt to deal with incidents once they are realised (Perrow, 1994; Wildavsky, 1988). HRT anticipates safety outcomes for organisations that engage in high-reliability practices (Rosa, 2005). Therefore, HRT strongly promotes the need to build an organisational culture that puts safety first—a strong culture that encourages responsiveness and vigilance to potential incidents. HRT's focus on HROs allows it to serve as an appropriate and meaningful lens through which to inform our understanding of cyber safety cultures in organisations. In this context of cyber safety, the culture of interest is a security culture.

HRT scholars have explored security cultures that put a premium on reliability and generally agree that reliability is the ability to conduct and sustain error-free operations and practices. Included in these practices are (1) top managers prioritising safety and reliability as a goal; (2) setting up high levels of redundancy in technical safety measures

and workforce personnel; (3) developing a 'high-reliability culture' in decentralised, constantly practiced operations; and (4) advancing trial and error types of organisational learning (Perrow, 1994; Sagan, 1995). These initiatives and practices identified by HRT can be construed as efforts to directly or indirectly attend to the challenges caused by complex systems and interactions (Weick et al., 1999). An HRO's organisational culture is part of a high-reliability process, as it establishes a homogenous set of assumptions, norms and decision premises. When these are invoked on local and decentralised bases, compliance happens without surveillance (Weick, 1987). Although these strategies and processes are not always completely developed or entirely employed in organisations (Morone & Woodhouse, 1986; Perrow, 1994), taken together, the strategies recommend two broad components of reliable, security cultures; their practical and supportive competencies.

3.1 | Practical competencies: InfoSec Practices

According to HRT, there should be a set of core practices designed to prevent certain events and incidents from occurring (Boin & Schulman, 2008; O'Neil & Krane, 2012). These represent the practical competencies an HRO should engage in toward the development of a security culture. According to HRT, the practical competencies of an HRO that help establish its security culture include many of the common InfoSec practices that firms typically use to reduce security risks (Barton et al., 2016) and assure organisational reliability (Speier et al., 2011). InfoSec practices are a set of procedures and activities designed to protect the availability, integrity and confidentiality of organisational information assets that include IS (Burns, 2019). HROs rely heavily on these InfoSec practices, executing them at a high level of competency.

InfoSec practices can be categorised into four classes based on their intent: detection, prevention, response and mitigation (Lu et al., 2017; Lu et al., 2019). Detection and prevention practices share the primary task of thwarting breaches while response and mitigation practices are more related to buttressing recovery when a disruption occurs (Lu et al., 2017). Prevention practices operate until the moment a security incident happens, followed by a response (Baskerville et al., 2014). Ensuring preventative and responsive practices are in place can enable HROs to respond to InfoSec incidents more effectively (Lu et al., 2017). Automated InfoSec practices decrease the risk of a number of InfoSec threats (Barton et al., 2016; Friedberg et al., 2015), but employees' InfoSec compliance improves the usefulness of nonautomated InfoSec practices (Montesdioca & Maçada, 2015; Siponen et al., 2007).

3.2 | Supportive competencies: Organisational mindfulness, organisational structure and top management involvement

According to the HRT literature, the success of an organisation's practical competencies is predicated on its supportive competencies. The literature further describes organisational mindfulness, organisational structure and top management involvement as key supportive competencies able to drive successful organisational endeavours. To that extent, we focus on these three competencies as key supportive competencies for an organisation's InfoSec practices.

3.2.1 | Organisational mindfulness

HRT scholars suggest that in order to move closer to achieving a sufficient condition of reliability, organisations must also become 'mindful'. Organisations cease to operate effectively when their attention is scattered, which, in turn, causes employees to 'misestimate, misunderstand, and mis-specify what they think they face' (Weick, 2009, pp. 850). Moreover, previous studies delineate a dominant cognitive orientation as the main difference between

traditional organisations and HROs (Roberts, 1990b; Roberts & Bea, 2001; Weick & Sutcliffe, 2001). HROs concentrate and learn from failures rather than successes (Weick et al., 1999). The distinctive cognitive mindset that allows HROs to manage and cope with incidents and threats is an orientation called organisational mindfulness. It is defined as '*a combination of ongoing scrutiny of existing expectations, continuous refinement and differentiation of expectations based on newer experiences, willingness and capability to invent new expectations that make sense of unprecedented events, a more nuanced appreciation of context and ways to deal with it, and identification of new dimensions of context that improve foresight and current functioning*' (Weick & Sutcliffe, 2001, pp. 42). According to van de Walle and Turoff (2008), p. 6) 'mindfulness is less about decision making and more about inquiry and interpretation grounded in capabilities for action' within organisations.

Organisational mindfulness is a collective capability that encompasses five organisational-level characteristics: *Preoccupation with failure* is the first dimension of organisational mindfulness and refers to operating with a wariness of unexpected incidents (e.g., InfoSec), which is countered by reporting mistakes and engaging in open discussions (Ray et al., 2011; Vogus & Sutcliffe, 2007). *Reluctance to simplify* is the second dimension of organisational mindfulness and refers to taking deliberate steps to question assumptions and process information in a way that generates new knowledge and nuanced ongoing operations (Ray et al., 2011; Vogus & Sutcliffe, 2007). The third dimension of organisational mindfulness is *sensitivity to operations*, which involves a situational understanding that allows organisations to make ongoing adjustments to prevent incidents from accumulating (Ray et al., 2011). *Commitment to resilience* is the fourth dimension of organisational mindfulness and involves developing capabilities to detect, mitigate and respond to incidents before they have a chance to inflict even more serious harm (e.g., InfoSec incidents) (Ray et al., 2011; Vogus & Sutcliffe, 2007). The final dimension of organisational mindfulness is *deference to expertise*, which means individuals with the most expertise and knowledge have the authority to make decisions regardless of their rank (Ray et al., 2011; Vogus & Sutcliffe, 2007). If a high-reliability mindset does not exist among the managers running an organisation, no set of rules and practices will ever produce an HRO.

Mindful organisations have a rich awareness of the details needed to perceive cues and interpret them, and a capability to respond to incidents (Weick et al., 1999). Mindful organisations do not prescribe to old ways of thinking and responding to incidents. They pay close attention to new possibilities, stay alert to current happenings within the organisation, are keen to consider alternative perspectives, are interested in investigating failures, and refuse to function on autopilot (Ray et al., 2011; Weick & Sutcliffe, 2001). There are unique adaptive processes and strategies in the mindful practices of HROs that enable them to avoid or mitigate incidents. HROs learn from mistakes (Weick & Sutcliffe, 2001), actively look for what they do not know (Roberts & Bea, 2001), pay attention to details, and make arrangements in a way that encourages rich thinking and the capacity to respond to incidents (Weick, 2009). Moreover, there is a conceptual and empirical linkage between organisational mindfulness and a wide variety of organisational outcomes, such as improving routines and practices that establish expectations or heuristics, increasing affective and normative organisational commitment, providing more opportunity outcomes, and enhancing individuals' mindfulness (Vogus & Sutcliffe, 2012).

In the InfoSec context, organisational mindfulness has been proposed as a prospective framework for effective security policy administration (Parrish et al., 2008), such as InfoSec practices. It has also been suggested that organisational mindfulness supports individuals' use of mindfulness techniques when seeking to avoid InfoSec threats (e.g., social engineering) (Jensen et al., 2017). Considering the importance of InfoSec issues in organisations, increasing mindfulness provides novel opportunities to advance their competency in executing InfoSec practices and, ultimately, their organisational security cultures (Burns, 2019).

3.2.2 | Organisational structure

An organisational structure as another supportive competency is defined as "*the formal allocation of work roles and the administrative mechanisms to control and integrate work activities, including those that cross formal*

organizational boundaries" (Child, 1984 p. 2). Organisational structures assign human and technical resources to the activities that need to be performed and the supportive mechanisms for their coordination (Rocha Flores et al., 2014). Further, organisational structures determine and facilitate operational and strategic decision making and monitor the operating mechanisms that provide instructions for what is expected of organisational employees while also explaining how the instructions should be followed (Child, 1984). Flexible organisational structures have a rapid tempo in their buildup and maturation stages, as well as a bureaucracy for the maintenance and resolution stage, which enables the organisation to effectively respond to incidents in its environment (Grabowski & Roberts, 1997).

Coordinating organisational structures refer to formal and informal meetings between those responsible for InfoSec tasks in an HRO and representatives from various business units within the organisation in order to facilitate the communication of strategic business plans focused on both business and InfoSec functions (Kayworth & Whitten, 2010; Rocha Flores et al., 2014). Coordinating organisational structures consist of forming InfoSec steering committees and liaisons to represent the HRO's InfoSec function, assisting business units in InfoSec risk assessments, and providing security advice in line with the organisation's security policies (Kayworth & Whitten, 2010). Through these structures, the InfoSec function gains valuable insights from the business units to facilitate strategic decision making while also being able to communicate security pressures with business managers.

3.2.3 | Top management involvement

Top management involvement is another key supportive competency of an HRO's InfoSec practices. HRT suggests that top managers should place safety and reliability first as a goal in order to achieve high-reliability in organisations (Perrow, 1994; Sagan, 1995). Involvement refers to top management's engagement in the specific concerns of their organisation (Jarvenpaa & Ives, 1991). A commitment by top management to InfoSec practices can lead to organisational changes that mitigate security risks in the organisation (Barton et al., 2016). It is therefore the responsibility of top management to break down cultural and organisational barriers in an organisation in order to encourage collaboration on security issues (Knapp et al., 2006).

Technology helps to achieve security-related goals, but management's involvement in changing the culture and ensuring security effectiveness plays a critical role. Evidence suggests that after top management (e.g., the CEO) changes their attitude toward InfoSec and becomes actively involved in InfoSec issues, there are considerable changes in employee compliance with InfoSec policies and improvements in security culture (Hu, Dinev, Hart, & Cooke, 2012). Moreover, organisations with stronger top management support and involvement in security activities engage in more preventive security behaviours (Masrek, Harun, Ramli, & Prasetyo, 2019).

3.3 | Conceptual model

Figure 1 presents a conceptual model of an HRO's security culture, based on the HRT literature. As the model depicts, an HRO's security culture is reliant upon its practical competencies in discovering and managing unexpected events through InfoSec practices, which itself is dependent upon the supportive competencies of organisational mindfulness, organisational structure and top management involvement. Other supportive competencies may exist, but the HRT literature is not explicit in identifying them. Further, how these supportive competencies relate with one another, with InfoSec practices, and security culture is still unclear in the HRT literature. For that reason, an exploration of the practices of HROs would be beneficial to the further elaboration of Figure 1 as a research model and testable set of hypotheses. This exploration, as well as a subsequent empirical test of the resulting research model, is the purpose of the mixed-methods research design described next.

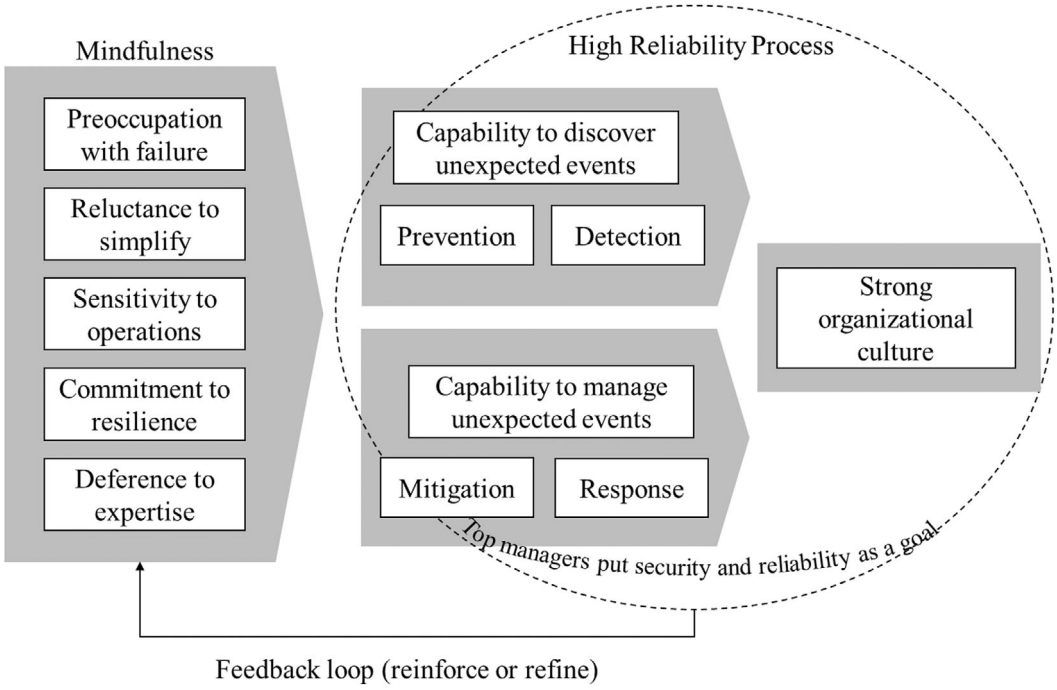

FIGURE 1 High-reliability theory-derived conceptual security culture model of an high-reliability organisation.

4 | MIXED METHODS RESEARCH DESIGN AND RESULTS

A mixed-methods research design includes elements of both qualitative and quantitative methods (Tashakkori et al., 1998). Mixed methods designs are appropriate when an exploration of a phenomenon is needed to better understand it for the purpose of explanation beyond what a single approach could provide (Venkatesh et al., 2013). This is the case for this study, where the HRT and HRO literature is rather limited in its presentation and reporting on the supportive and practice competencies of HROs that help form a culture of security. Mixed methods designs allow for stronger inferences that may be required when developing particular aspects of a research (Venkatesh et al., 2016)—which in this case of this study is how the supportive competencies of organisational mindfulness, organisational structure, and top management involvement interact to influence InfoSec practices and, ultimately, a security culture. Further, in IS field, since the nature of the context changes rapidly, and researchers usually face issues making significant insights based on existing theories and viewpoints, mixed-methods approaches are particularly appropriate (Venkatesh et al., 2013). Given the lack of research on how the supportive competencies of an HRO work together to support their InfoSec practices and our desire to provide an empirically supported SCM, the mixed-methods approach is appropriate.

This study's mixed methods design follows a developmental purpose, since we conducted a qualitative study first and used the results from that phase, in concert with the HRT literature, to develop the research model and associated hypotheses tested in the second phase of the study (Tashakkori et al., 1998; Teddlie & Tashakkori, 2009; Venkatesh et al., 2013; Venkatesh et al., 2016). In Table S2 of the supplementary document, we explain how we followed the established criteria and requirements of a developmental mixed-methods research design established by Venkatesh and colleagues (Venkatesh et al., 2013; Venkatesh et al., 2016). Specifically for this study, during the qualitative phase (phase 1 of the study), we (1) conducted interviews with security professionals employed by HROs in the U.S. to affirm organisational mindfulness, organisational structure and top management involvement as key

supportive competencies of an HRO's InfoSec practices; and (2) analysed the interview data and categorised the themes that emerged from those data to elaborate on our conceptual model and form a SCM and associated set of testable hypotheses. In the quantitative phase (phase 2 of the study), we empirically tested the SCM and its associated hypotheses through survey data collected from a sample of U.S. security professionals to ascertain how the key supportive competencies derived from the first phase of the research relate with InfoSec practices in forming a firm's security culture. The details of both phases of the developmental mixed-methods design are presented next, followed by a discussion in which the meta-inferences are presented and discussed relative to their implications for research and practice.

4.1 | Phase 1: Qualitative study design

For the qualitative phase, we utilised an interpretive phenomenological approach (IPA) (Creswell & Poth, 2016; Pietkiewicz & Smith, 2014) to leverage interview data from cybersecurity professionals employed by companies matching the criteria of HROs, thus helping us to contextualise and operationalise supportive competencies in a SCM. Their respective organisations' status as an HRO was determined through the opinions of other cybersecurity professionals who had recently either worked at or contracted with the organisations in some manner. Because IPA, at its core, is an interpretive method, we followed several suggestions and principles of an interpretive approach for data collection and analysis to provide criticality of our interpretations and present transparency in our data analysis and results (Smith & Fieldsend, 2021). Guidance for the interviews was derived from the HRT, which enabled us to inspect the applicability and operationalization of the theory and the conceptual model presented in Figure 1.

The interview data were analysed using Nvivo v12 following a pattern matching technique (Sinkovics, 2018), whereby the data were iteratively coded according to themes and the relationships among the themes and then compared with the security culture research model to identify variances or gaps in the model as it stands relative to the reality expressed by the interviewees. This analysis of the interview data involved two researchers, working independently. As a measure of analysis reliability, an interrater reliability score of 0.7730 was produced, suggesting a substantial agreement between the researchers (Landis & Koch, 1977). Theoretical saturation was obtained after 15 interviews, based on an a priori 'stopping criterion' provided by the literature to aid recognition of thematic 'saturation' among interviewees (Teddlie & Tashakkori, 2009). Another five interviews were conducted to ensure that thematic saturation had been achieved (Francis et al., 2010). The themes were examined for similarity and grouped accordingly. The themes were then linked to appropriate interview quotes from the transcripts and formed the basis of the SCM and associated hypotheses presented next.

4.2 | Building and hypothesizing the security culture model

The results of the interviews suggest organisational mindfulness, as well as organisational structure and top management involvement are indeed key supportive competencies that provide direct support to an HRO's InfoSec practices and indirect support to its culture of security. A summary of interviewees' demographic information and themes with supporting quotes is presented in Tables S3, S4 in the supplementary document. Presented below are what we consider to be the most explicit and informative statements made in the interviews, combined with insights from the HRT literature to provide support for a set of testable hypotheses.

4.2.1 | Organisational mindfulness

Organisational mindfulness concentrates on an organisation's competency to recognise cues, understand them, and react properly (Butler & Gray, 2006). In the InfoSec context of HROs, each dimension of organisational mindfulness

should be addressed to establish InfoSec practices, strategies and outcomes. In terms of organisational mindfulness, in general, as a supportive competency in a firm's InfoSec practices and security culture, the best expression of this relationship from the interview data is when one interviewee claimed that '*there's a lot of things in place and what that means is if there are events or situations that occur, there are root cause analysis. And they were undertaking Lessons Learned exercises afterwards to try and ensure that these things don't happen again*.' In making this claim, the interviewee also identified the existence of one of the key dimensions of organisational mindfulness—preoccupation with failure within his company. A preoccupation with failure is necessary in InfoSec practices as organisations run in environments with dynamic security threats (Baskerville et al., 2014). Paying attention to mistakes and failures helps prevent the overconfidence that can emerge when employees think success is common and routine (Butler & Gray, 2006). It is part of the dynamic nature of InfoSec practices that previously effective InfoSec practices and strategies can become outdated as security threats evolve (Burns, 2019). Former InfoSec researchers have argued that individuals learn from their prior security failures by treating them as 'teachable moments' that can ultimately help improve InfoSec practices (Burns et al., 2017). This preoccupation with failure provides a firm with an opportunity to discover unexpected events when they occur through prevention and detection practices and then manage them appropriately through mitigation and response techniques—an example of practical competencies being supported by the competency of organisational mindfulness.

The interviewees made other statements that suggest organisational mindfulness is a supportive competency required for effective InfoSec practices. For example, one interviewee stated, '*For the most part our employees understand who knows what and often just go to that person for support rather than guessing or relying on guidance from their superiors. We kind of encourage that…. I think it's helped us avoid some problems*.' This statement not only points to the presence of one of the key dimensions of organisational mindfulness, deference to expertise, but also suggests a connection with the InfoSec practices of prevention and detection as well as with a general security culture within the firm, indirectly. HROs that practice deference to expertise enable agility in their InfoSec operations (Butler & Gray, 2006). Indeed, the most senior managers of the security team do not always have the necessary expertise to deal with every InfoSec threat (Burns, 2019).

Interviewees also identified the relationship of another important dimension of organisational mindfulness—reluctance to simplify interpretations, with their firms' InfoSec practices. For example, an interviewee mentioned that '[W]e *try to take a very thoughtful and non-reactive approach to security. I think if anything, like most organizations, people more so want to grow their security operations than their efforts. So I don't think anyone's looking to simplify things*.' This statement clearly links the resistance to simplification with the InfoSec practices of the firm, and similar to the prior highlighted quotes, it also suggests organisational mindfulness provides indirect support to a culture of security that is non-reactive, thoughtful and purposeful. An implication of the unwillingness to simplify the InfoSec environment is that prior InfoSec assumptions and practices are regularly re-evaluated (Burns, 2019). For example, in a data breach incident, a simplified interpretation could automatically point to bad luck, employee errors, or programmer carelessness. HROs deliberately attempt to avoid these destructive simplifications and instead accept the complication of the issue with a healthy scepticism of policies, procedures and practices (Carlo et al., 2012).

The other two dimensions of organisational mindfulness, sensitivity to operations and commitment to resilience, were also mentioned by interviewees in support of their respective firms' InfoSec practices. For instance, in terms of the supportive competency of sensitivity to operations, one interviewee stated, '*If we have a technology that makes it difficult for an individual to do their job, then we've got to find a better way because the business has to run regardlessly. Regardless of the technology we have. So if we've implemented controls or monitoring or whatever that makes it difficult for that person to accomplish what they need to accomplish, then we need to back off and find an alternative*.' Researchers have also highlighted the need for ongoing attention and sensitivity to operations in the InfoSec domain, which results in maximising the security of organisations by addressing the factors that precede incidents and minimising their impact as they occur (Burns, 2019). Organisations' mission, practices and the sensitivity of information and systems play an essential role in InfoSec risk assessments (NIST, 2012). As there are no impenetrable systems and all organisations are either being hacked or will be, it is essential for HROs to commit themselves to

resilience in response to rapidly evolving security threat vectors (Carlo et al., 2012; Njenga & Brown, 2012). Again, an organisation's competency in preventing, detecting, responding and mitigating security threats is clearly linked to a heightened awareness of its operations and what is working and not working relative to controls and monitoring.

In terms of commitment to resilience, one interviewee stated, '*We have a resiliency office, we do a lot of testing. There is a cyber component that is baked into all of it. Intriguing, and that is about small innovations. I think they are well thought out. So it is that idea that once again because we have a complex structure for security, a small innovation.*' This quote represents another clear link between a firm's organisational mindfulness as a supportive competency for its InfoSec practices and its security culture which, by definition, is an environment that encourages and develops shared security attitudes, values, beliefs and norms in an organisation (Van Niekerk & Von Solms, 2010). Organisations' mission, practices and the sensitivity of information and systems play an essential role in InfoSec risk assessments (NIST, 2012). As there are no impenetrable systems and all organisations are either being hacked or will be, it is essential for HROs to commit themselves to resilience in response to rapidly evolving security threat vectors (Carlo et al., 2012; Njenga & Brown, 2012). Based on this understanding from the HRT and HRO literature, as well as results from the qualitative phase of this study, we propose the following hypotheses:

H1(a–d): Organisational mindfulness is positively associated with the InfoSec practices of an organisation, namely prevention (a), detection (b), response (c) and mitigation (d).

4.2.2 | Organisational structure

Formal organisational structures may include a formal InfoSec unit within the organisation whose mission it is to secure the organisation's information assets (Kayworth & Whitten, 2010). The purpose of this unit is to develop and implement the organisation's standards and practices governing organisation-wide InfoSec. Further, in the formal organisational structures, there are InfoSec executives (e.g., security top manager) with leadership responsibility for InfoSec functions that facilitate strategic alignment between security and business goals. Formal organisational structures may also include a formal unit as an internal audit function that conducts assessments of InfoSec controls and practices and reports the results to top management. On the other hand, coordinating organisational structures refers to formal and informal meetings between those responsible for InfoSec tasks in an HRO and representatives from various business units. This organisational structure consists of forming InfoSec steering committees and liaisons to represent the HRO's InfoSec function (Kayworth & Whitten, 2010). An organisational structure ensures the alignment between an organisation's security functions and its business strategies, facilitates the effective organisation of its InfoSec function, contributes to the successful implementation and coordination of InfoSec plans and practices (Kayworth & Whitten, 2010; Rocha Flores et al., 2014), and clarifies where its InfoSec compliance monitoring and enforcement should be established (it should not be part of the IT department) (Von Solms & Von Solms, 2004).

The interview data provided us with an assurance that organisational structure, like organisational mindfulness, serves as a competency that supports a firm's InfoSec practices and security culture. For instance, consider the interviewee statement, '*I think there's probably a lot of other security departments that are similar, where they're responsible for the whole organization's security, but they don't necessarily have the influence or power to make the change because of where they sit in the organization.*' This statement clearly points to the formal organisational hierarchy as a determinant of security outcomes. Another interviewee stated, '*I[n] general, the structure of our organization hurts its security effort only because I believe that the concern for information security and risk mitigation in our business is not as understood or appreciated at the highest level of the business as it could be.*' While this interviewee was pointing to a problematic situation, the comment highlights the supportive nature of a firm's organisational structure and its InfoSec practices and security culture in general. The coordinating structure of an HRO is also exhibited in the interviews as an important aspect of organisational structure, with an interviewee referencing the role of coordinated awareness training by stating, '*I think that because there is a provision for information security tools like Splunk or Tenable or security awareness training because there is an investment.*' As such, we hypothesize:

H2(a–d): Organisational structure is positively associated with the InfoSec practices of an organisation, namely prevention (a), detection (b), response (c) and mitigation (d).

4.2.3 | Top management involvement

Considerable research has been undertaken to assess the impact of top management involvement on InfoSec policies, procedures and performance (e.g., Barton et al., 2016; Knapp et al., 2006; Singh et al., 2014). Top management specifies the issues that are strategic to an organisation and will receive the organisational commitment and resources required for effective development and implementation of InfoSec initiatives and practices (Boss et al., 2009; Bulgurcu et al., 2010; Dutton et al., 2001). In HROs, top management support is required in order to promote the development and execution of organisation-wide InfoSec practices to better implement InfoSec procedures and avoid InfoSec breaches. Top management support is necessary in order to effectively handle InfoSec issues, but without top management involvement, even a robust structure with comprehensive InfoSec practices will not guarantee InfoSec enforcement across the organisation (Knapp et al., 2006). Top management involvement is critical in InfoSec practices whereby an organisation's goals and structures are defined in relation to InfoSec (Singh et al., 2014). Moreover, top management support is required for any InfoSec readiness initiative to be successful (Elyas et al., 2015).

Drawing on HRT, there are two strategies for achieving (InfoSec) safety: anticipation (prevention and detection of InfoSec incidents) that entails efforts to predict and prevent possible (InfoSec) incidents from occurring before they happen; and resilience (response and mitigation) that entails efforts to deal with incidents once they become manifest (Perrow, 1994; Wildavsky, 1988). In HROs, top management involvement is required to assist in the development and implementation of organisation-wide InfoSec practices that enable both strategies. The aim is to avoid InfoSec breaches, or to detect an attack and promptly report them to the InfoSec managers, or to take appropriate corrective actions against identified attacks, or to reduce losses by lessening the impact of InfoSec breaches. Either way, an HRO's top management is involved in not only planning the strategies, but in their execution.

Results from the qualitative phase of this study mostly reflect a direct influence of top management involvement on InfoSec practices, but not necessarily from a positive perspective. For example, one interviewee stated, '*People on the higher levels pretty much they ignore security protocol and there's no way to enforce it upon them*,' while another said, '*So even though I'm closer to agency leadership than I have been before, I still feel like where my security office sits in the structure, I think it hurts the security efforts, mainly because it associates all security efforts with IT*.' Another interview added, '*They're responsible for the whole organization's security, but they don't necessarily have the influence or power to make the change*.' Overall, these quotes lend some support to the position of top management involvement as a direct determinant of an organisation's InfoSec practices, but vary in terms of having a positive or negative effect. Given the ambiguity of these findings, we can lean more heavily on the HRT literature's general positive positioning of top management support relative to security practices and posit the following hypotheses:

H3(a–d): An organisation's top management involvement is positively associated with its InfoSec practices, namely prevention (a), detection (b), response (c) and mitigation (d).

4.2.4 | Security culture model

We believe the qualitative findings presented above help to elaborate our conceptual model as a SCM by adding organisational mindfulness, organisational structure and top management involvement as distinct supportive competencies of an HRO's InfoSec. In the SCM (see Figure 2), we see the importance of supportive competencies—organisational mindfulness, organisational structure and top management involvement—in driving HRO's InfoSec practices. In this model, security culture is presented as an outcome of practical

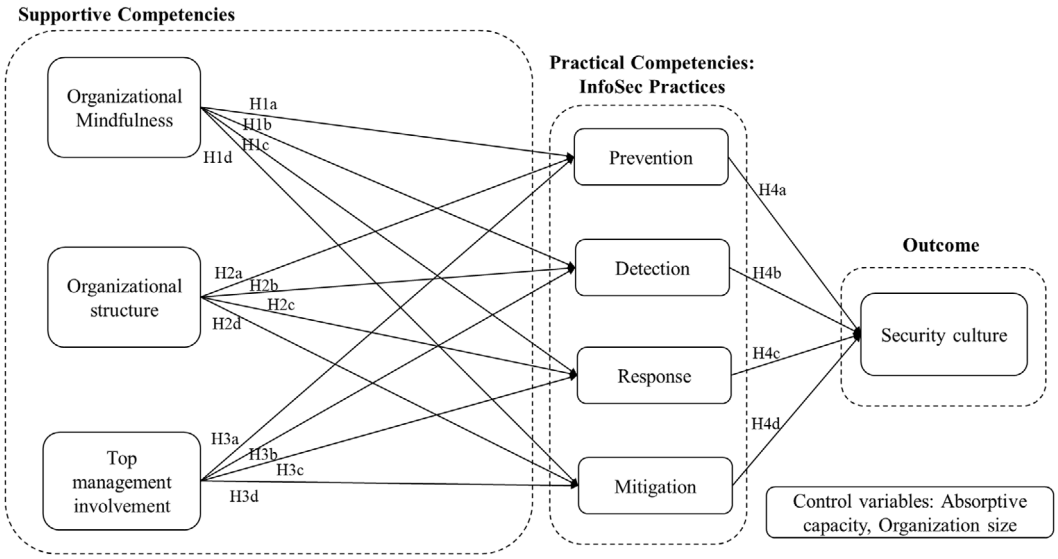

FIGURE 2 Security culture model.

competencies—InfoSec practices—namely prevention, detection, response and mitigation practices. A summary of the conceptual definition of each construct is presented in Table S5 in the supplementary document.

Based on HRT, in order to maintain reliability and safety, HROs should concentrate on a set of practices that mitigate or even prevent potential incidents (Roberts, 1990a, 1990b). Therefore, in the InfoSec context, a set of InfoSec practices should be designed and employed to create an atmosphere that promotes employees' positive InfoSec-related attitude and beliefs, leading to InfoSec becoming part of the norms and values of an organisation. These practices can be designed with different emphases—either to foster an organisation's ability to discover (i.e., detect and prevent) unexpected InfoSec incidents or to nurture organisational capabilities to manage (i.e., respond and mitigate) unexpected InfoSec events. Multiple security culture frameworks account for the role of InfoSec practices as a determinant of a security culture, including the MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) framework (Georgiadou et al., 2021), the cyber-security culture framework (Georgiadou et al., 2022), and the information security culture framework (Da Veiga & Eloff, 2010), among others. For each of these frameworks, the InfoSec practices of prevention, detection, response and mitigation are practical organisational competencies that directly shape the culture of security within an organisation. Thus, we hypothesize the following:

H5(a–d): Prevention (a), detection (b), response (c) and mitigation (d) practices are positively associated with the security culture of an organisation.

4.3 | Phase 2: Quantitative study design

In the second phase of our mixed-methods design, we empirically tested the SCM that was developed based on the literature and the input from the first phase of this study. The SCM and hypotheses were tested using survey data collected from a sample of U.S. cybersecurity professionals from a wide range of roles and industries. The survey was conducted using the Qualtrics platform and a third-party data collection company (Cint) over a period of two weeks. After removing the incomplete responses of the survey, there were 840 responses from the United States. In terms of organisational roles, the majority of participants were chief executive officers (25%). Less than half of the

companies (40.2%) were of medium size with 20–199 employees, around 18% of them were from electronic, technology and IT industries, and most of them had been in business for more than 5 years (58.1%). The demographic description of the sample is presented in Table S6 in the supplementary document.

In terms of survey instrumentation, organisational mindfulness, as a second-order reflective construct, was adopted from Ray and colleagues (Ray et al., 2011) and includes five reflective first-order constructs, namely preoccupation with failure, reluctance to simplify, sensitivity to operations, commitment to resilience and deference to expertise. The measurement items for organisational structure were adopted from Rocha Flores and colleagues (Rocha Flores et al., 2014). For InfoSec practices including detection, prevention, response and mitigation, we adopted items from Lu and colleagues (Lu et al., 2017). For security culture, we adopted the six items from Chen et al. (2015). For top management involvement, we adopted items from Liang et al. (2007). We applied a five-point Likert scale (strongly disagree, disagree, neither agree nor disagree, agree and strongly agree) to measure the key constructs of this study. All the constructs of the model are first-order reflective constructs except organisational structure, which is a formative second-order construct with two reflective first-order factors—formal structure and coordinating structure. The measurement items are presented in Table S7 in the supplementary document.

We applied Partial Least Squares-Structural Equation Modelling (PLS-SEM) SmartPLS 3.0 software to test the measurement and structural models of this study. PLS-SEM has been widely used in quantitative studies to assess the relationships between variables/factors in human information security behaviours (Bulgurcu et al., 2010; Rocha Flores et al., 2014; Warkentin et al., 2016) and is recommended for examining models that include formative constructs (Petter et al., 2007) as well as exploratory research (Gefen et al., 2011). PLS is an appropriate tool for this study since it is exploratory research and uses a model with a formative construct (organisational structure). PLS-SEM can be used to analyse data with a small sample size and normal distribution is not a requirement in PLS-SEM.

To minimise and test for common method bias (CMB), we followed procedural guidance and statistical tests provided in the literature (MacKenzie et al., 2011). The applied procedural guidance and statistical tests are presented in Table S8 in the supplementary document. In general, the findings from the statistical tests suggest that CMB is not a significant issue for this research.

4.4 | Quantitative results

4.4.1 | Measurement model assessment

In terms of the validity and reliability of the measurement model, according to Hair and colleagues (Hair et al., 2016), for exploratory research, factors loading greater than 0.4 and less than 0.7 can be maintained if AVE is satisfied. The items causing issues in AVE discriminant validity were removed and the remaining items reported a loading greater than 0.6. Regarding the internal consistency, the values of Composite Reliability and Cronbach's alpha were assessed. For exploratory research, a Cronbach's alpha value between 0.6 and 0.95 is acceptable (Taber, 2018). The reported internal consistency revealed that all of the constructs were within the acceptable ranges. The assessment of convergent validity using AVE values indicated that all were above the cut-off value of 0.5, as shown in Table 1.

In a formative higher-order construct, the weights of the lower-order constructs signify drivers of the higher-order construct (Becker et al., 2012; Duarte & Amaro, 2018). We tested the weights and the significance of the first-order constructs (formal structure and coordinating structure) on the second-order construct (organisational structure; 0.238* and 0.914***, respectively). The HeteroTrait-MonoTrait (HTMT) criterion were used for examining the discriminant validity of the constructs (Hair et al., 2017). HTMT values greater than 0.9 indicate the lack of discriminant validity between conceptually similar constructs. The thresholds of lower than 0.9 is acceptable for HTMT value (Gold et al., 2001; Teo et al., 2008). $HTMT_{inference}$ generates rates of 80% or higher in terms of inter-construct correlations as high as 0.95. Overall, $HTMT_{.90}$ and $HTMT_{inference}$ approaches identify discriminant

TABLE 1 Convergent validity testing.

Construct	Item	Std. loading of each item	Composite reliability (CR)	Cronbach's alpha	Average variance extracted (AVE)
Detection	DET2	0.820	0.877	0.813	0.641
	DET3	0.823			
	DET4	0.767			
	DET5	0.791			
Prevention	PREV1	0.769	0.875	0.828	0.539
	PREV2	0.686			
	PREV3	0.720			
	PREV4	0.703			
	PREV5	0.756			
	PREV6	0.766			
Response	RESP2	0.703	0.849	0.789	0.530
	RESP3	0.752			
	RESP4	0.745			
	RESP5	0.722			
	RESP6	0.719			
Mitigation	MITG3	0.793	0.847	0.769	0.648
	MITG4	0.819			
	MITG5	0.803			
Top management involvement	TOPP1	0.823	0.870	0.796	0.690
	TOPP2	0.838			
	TOPP3	0.831			
Security culture	SECU1	0.774	0.877	0.852	0.544
	SECU2	0.704			
	SECU3	0.715			
	SECU4	0.731			
	SECU5	0.736			
	SECU6	0.763			
Mindfulness–Preoccupation with failure	PRF1	0.715	0.841	0.799	0.515
	PRF2	0.712			
	PRF3	0.627			
	PRF4	0.767			
	PRF5	0.759			
Mindfulness–Reluctance to simplify	REL1	0.736	0.814	0.843	0.523
	REL2	0.717			
	REL3	0.700			
	REL4	0.739			
Mindfulness–Sensitivity to operations	SEN1	0.781	0.847	0.770	0.649
	SEN2	0.823			
	SEN3	0.812			

TABLE 1 (Continued)

Construct	Item	Std. loading of each item	Composite reliability (CR)	Cronbach's alpha	Average variance extracted (AVE)
Mindfulness–Commitment to resilience	COM1	0.828	0.798	0.710	0.570
	COM2	0.775			
	COM3	0.652			
Mindfulness–Deference to expertise	DEF1	0.747	0.836	0.723	0.630
	DEF2	0.783			
	DEF3	0.847			
Organisational structure–Formal	FSTR1	1.000	1.000	1.000	1.000
Organisational structure–Coordinating	COSTR1	0.784	0.876	0.812	0.639
	COSTR2	0.803			
	COSTR3	0.791			
	COSTR4	0.819			

validity issues (Henseler et al., 2015). To meet the $HTMT_{.90}$ and $HTMT_{inference}$ criterion, we dropped the items that violated the 0.90 thresholds. The remaining items for each pair of constructs presented an acceptable level of discriminant validity. For the discriminant validity of the constructs, the values of the $HTMT_{.90}$ criterion are shown in Table S9 in the supplementary document.

4.4.2 | Structural model assessment

A structural model assessment includes examining the significance and relevance of path coefficients, to assess collinearity among the exogenous constructs, and evaluate the relevance model and the model's predictive accuracy (Hair et al., 2019). The Variance Inflation Factor (VIF) for each exogenous construct of the model was tested to check for collinearity among the constructs. VIF values less than three are ideal values, and VIF values should not be greater than five (Hair et al., 2019). The evaluation of VIF values revealed that all the values were less than 2.37, suggesting no collinearity issues. Using SEM-PLS, we ran the bootstrapping routine with 10 000 bootstrapping subsamples at a 5% significance level to identify the statistical significance of the path coefficients (Streukens & Leroi-Werelds, 2016). To test the second-order constructs, we followed component-based model estimation by creating a new data file with latent variable scores (two-stage approach) (Wright et al., 2012). The two-stage approach tests the first-order constructs' scores during the first-stage and then these scores are treated as indicators for the second-order constructs in the second-stage (Duarte & Amaro, 2018; Hair et al., 2011). The results of the structural model's assessment are presented in Figure 3.

In terms of hypothesis testing, hypotheses H1(a–d), which hypothesized the positive association between organisational mindfulness and InfoSec practices in organisations, were supported (path coefficients = 0.121, 0.213, 0.358, 0.224, $p = 0.002$, 0.000, 0.000, 0.000, respectively). These findings indicate that organisational mindfulness is a key supportive competency for driving security culture. H2(a–d), which hypothesized the positive influence of organisational structure on InfoSec practices, namely prevention and response, were supported (path coefficients = 0.095, 0.132, $p = 0.020$, 0.002, respectively), except for the relationship between organisational structure, detection and mitigation (path coefficient = 0.040, 0.074, $p = 0.307$, 0.067, respectively). These hypotheses suggest that ensuring the alignment between security functions and business strategies facilitates the effective implementation and coordination of some InfoSec practices in

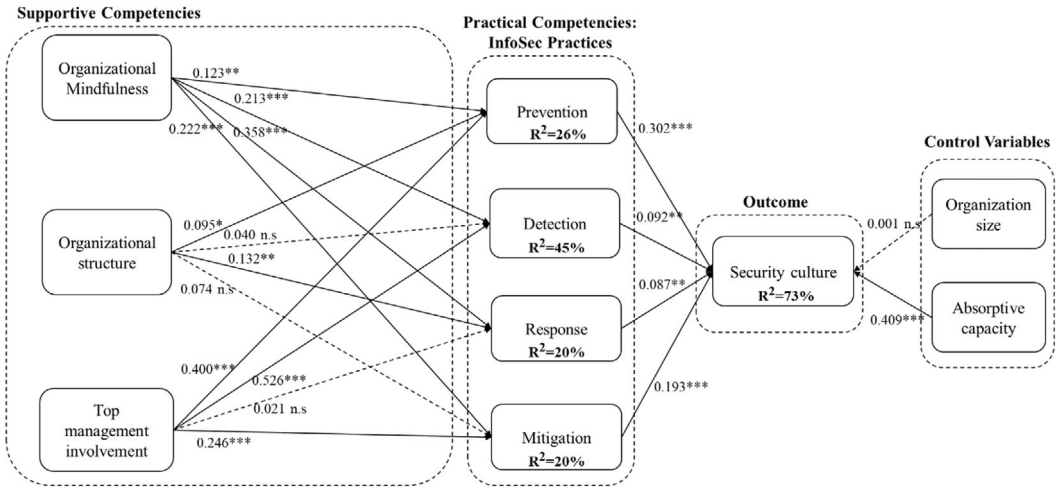

FIGURE 3 Structural model results, $^{*}p < 0.05$, $^{**}p < 0.01$ and $^{***}p < 0.001$.

organisations. Moreover, significant differences exist between the paths of organisational mindfulness and InfoSec practices compared to the paths of organisational structure and top management involvement and InfoSec practices.

H3(a–d), which hypothesized the positive relationships between top management involvement and InfoSec practices, were supported (path coefficients = 0.400, 0.536, 0.246, $p = 0.000$, 0.000, 0.000, respectively), except for the relationship between top management involvement and response (path coefficient = 0.021, $p = 0.604$). These hypotheses suggest that ensuring the engagement of top management in security activities facilitates the effective implementation and coordination of InfoSec practices in organisations, but their involvement in incident response activities is less important.

H5(a–d), which hypothesized the positive association between InfoSec practices (prevention, detection, response and mitigation) and security culture in organisations, were supported (path coefficients = 0.301, 0.092, 0.087, 0.193, $p = 0.000$, 0.000, 0.003, 0.000, respectively). InfoSec practices that emphasise the importance of fostering organisational capability in order to discover (detect and prevent) unexpected InfoSec incidents or to nurture organisational capability to manage and respond to unexpected InfoSec events, could lead to InfoSec becoming part of an organisation's norms and values.

In terms of the predictive power of the SCM, organisational mindfulness, organisational structure and top management involvement explain 26%, 45%, 20% and 20% of the variances in prevention, detection, response and mitigation, respectively. Combined, these InfoSec practices explain 73% of the variance in security culture. We also used the predictive sample reuse technique (Q^2) to check predictive relevance applying a blindfolding process. The model has predictive relevance if $Q^2 > 0$, while it demonstrates a lack of predictive relevance, if $Q^2 < 0$ (Chin & Dibbern, 2010). The predictive relevance of prevention, detection, response and mitigation practices were obtained using a two-stage approach, with the values of 0.374, 0.477, 0.232 and 0.282, respectively. The predictive relevance of security culture was obtained using a two-stage approach, with the value of 0.619.

Two control variables, organisation size and absorptive capacity, were also tested. Absorptive capacity had a positive significant relationship with security culture (path coefficient = 0.409, $p = 0.000$), signifying that organisations' readiness to engage in InfoSec activities based on prior knowledge and resources results in a greater valuing of information security in organisations. Organisation size had no significant relationship with security culture.

5 | DISCUSSION

Security cultures are well-established as fundamental to an organisation's effectiveness in managing risk and compliance activities; however, how they are formed and their key supporting organisational competencies are still not well understood. For this reason, the purpose of this study was to provide an explanation of how the supportive competencies of HROs relate with their InfoSec practices to influence their security cultures. Some organisations are better at some things than others, each organisation holding a set of critical competencies that allow it to exceed in some ways that others cannot. The mixed-methods developmental research design used in this study provided us with keen insights into what these key competencies are and how they relate in forming an effective culture of security.

The qualitative study in phase 1 of this research affirmed the HRT literature's suggestion that organisational mindfulness, organisational structure and top management involvement are relevant supportive competencies for a firm's security practices and provided an understanding of how they relate in providing their support. The empirical study in phase 2 quantified this support, providing some differentiation in terms of the exact nature by which the InfoSec practices of prevention, detection, response and mitigation are supported, or not. Next, as presented in Table 2, we bridged these two sets of findings to provide a set of meta-inferences (Creswell & Creswell, 2017; Venkatesh et al., 2013; Venkatesh et al., 2016).

5.1 | Meta-Inferences and theoretical implications

In this section, following the guidelines from Venkatesh and colleagues (Venkatesh et al., 2013; Venkatesh et al., 2016), we elaborate on the meta-inferences presented in Table 2 to discuss their direct implications to HRT which underpinned this research. Through this lens, we view security culture as an organic product of HROs and examine the underlying competencies they have that contribute to the culture. Even though HRT focuses on the processes organisations rely on to ensure continued success in dealing with potential disruptions, such as InfoSec threats, it has not been applied in the extant security culture literature. This presents an opportunity for this current research to leverage its focus on underlying organisational competencies as a new perspective to explain the drivers of security culture.

5.1.1 | Meta-inference 1: Organisational mindfulness is a critical supportive competency for an effective culture of security

We found organisational mindfulness to be a key supportive competency for driving security culture in an HRO. Organisational mindfulness is an important supportive competency in that it serves as an intellectual arrangement that is commonly associated with HROs. We found that organisational mindfulness not only fully supports InfoSec practices, but it does so more completely than organisational structural arrangements and top management support. This outcome suggests that organisations should depend less on their top management and organisational structure to establish and build a security culture—that is, focusing less on their reporting hierarchy and committee responsibilities to InfoSec—and more on developing every aspect of organisational mindfulness.

A mindful organisation is well positioned to foster all of the important InfoSec practices needed to provide a holistic risk management and compliance approach. Although hackers have developed more sophisticated attacks that evade organisational structure procedures, organisations should still be able to properly react to attacks if they embrace mindful agile processing (Jensen et al., 2017). This finding is in line with HRT's principles that emphasise the role of mindfulness for enhancing organisation's awareness and alertness to mobilise a contingent reaction and a safe organisational culture (Boin & Schulman, 2008; van de Walle & Turoff, 2008). According to HRT, a mindful

TABLE 2 Summary of meta-inferences.

Phase 1 results: Qualitative study	Phase 2 results: Quantitative study	Meta-inference
Each dimension of organisational mindfulness including preoccupation with failure, reluctance to simplify, sensitivity to operations, commitment to resilience and deference to expertise were expressed by security professionals as important supportive competencies from which to establish and engage in effective InfoSec practices.	The results of the survey of U.S. security professionals showed organisational mindfulness to be a positive direct determinant of InfoSec practices and an indirect determinant of security culture.	Consensus: For organisations to reach the level of resiliency found in the security culture of HROs, they must develop their overall level of organisational mindfulness.
The security professionals' interview data provided us with some assurance that organisational structure, including its formal and coordinating dimensions, serves as an important supportive competency from which to establish and engage in effective InfoSec practices.	Based on the results of the survey of U.S. security professionals, organisational structure serves as a positive direct determinant of an organisation's prevention and response InfoSec practices, but not its detection and mitigation practices.	Consensus: For organisations to reach the level of resiliency found in the security culture of HROs, they should expect their formal and coordinating organisational structures to help their efforts, but look to other supporting competencies, such as informal social arrangements, to aid their detection and mitigation practices.
The security professionals' interview data provided us with some assurance that top management involvement serves as an important supportive competency from which to establish and engage in effective InfoSec practices, but are less certain in terms of the positive or negative nature of the effect.	Based on the results of the survey of U.S. security professionals, top management involvement serves as a positive direct determinant of an organisation's prevention, detection and mitigation practices, but not its response practices.	Consensus: For organisations to reach the level of resiliency found in the security culture of HROs, they should expect the involvement of their top management to help their efforts, but look to other supporting competencies, such as external support agencies (e.g., NISP, ISACA) for support of their responses to security incidents.

organisation can distribute the values of care and caution, respect for attentiveness and procedures to promote a reliable and safe culture throughout the organisation.

5.1.2 | Meta-inference 2: Organisational structure is a necessary but not sufficient supporting competency for an effective culture of security

Based on HRT, HROs are characterised by safety norms and structures that reinforce their goals, mission and culture by focusing on organisations' practices, procedures, policies and job responsibilities (Grabowski & Roberts, 1997). Moreover, flexible and informal organisational structures can empower employees, teams and organisations to reinforce an organisational safety culture through prevention and response to internal and external incidents (Grabowski & Roberts, 1997). In pointing to a set of supportive competencies that are critical to a security culture, our findings suggest that an organisation's formal and coordinating arrangements indirectly influence its security

culture by way of their ability to partially support its InfoSec practices. Interestingly, their ability to influence the organisation's InfoSec detection and mitigation practices were not supported. It is quite possible this is due to the nature of detection and mitigation (minimising consequences in the case of failure) practices being less inclusive of the entire organisation and more of an isolated responsibility of the InfoSec function through the management of its technical controls. We also found that although organisational structure controls the establishment of InfoSec policies and practices, there is a need for informal social arrangements to help drive a firm's protection from and reaction to unexpected InfoSec incidents. For example, employees' informal social groups have the ability to inform and steer certain security perspectives and behaviours among their members (Johnston et al., 2019).

5.1.3 | Meta-inference 3: Top management involvement is a necessary but not sufficient supporting competency for an effective culture of security

Top management involvement was also found to be a supportive competency an organisation can rely on to promote its culture of security. Top management engagement in security practices has shown strong positive impact on practical competencies in HROs, which is in line with one of HRT's core tenets, which highlights that top managers should place safety and reliability first as a goal in order to achieve high-reliability and safety in organisations. In HROs, top managers' decision making and involvement in safety activities can reduce the unintended consequences and mitigate the safety risks by practicing revocable actions, and ensuring to maintain consistency among actions and procedures throughout all parts of the organisation (Grabowski & Roberts, 1997).

In terms of its influence on practical competencies, the effect of top management involvement in how detection, prevention and mitigation practices are conducted, suggests that these functions are a greater responsibility of top management than responsive practices. This finding potentially echoes the earlier point we made that responsive practices designed to provide remedies for dynamic security incidents are the realm of the InfoSec function and security teams rather than the organisation as a whole. Our findings from the thematic analysis also report this issue. For example, one of the interviewees (security manager) stated that '*I know there is a security issue, I'm the last one invited. Not saying that I don't appreciate that, because I don't like to be blown up either*.'

It is important to consider that any study investigating security-related topics may have the potential risk of dual use of research findings for legitimate and malicious intentions (Rath et al., 2014). Research on organisational security can aid organisations in how to better equip and protect themselves against security incidents. However, these research results may also potentially help hackers in identifying key practices in which organisations are most equipped/susceptible and exploiting those weaknesses in their attack strategies. The risk of dual use of this study's results is very low because this study investigates how to leverage organisational competencies to better improve organisational security culture, rather than examining what makes security incidents more effective.

5.2 | Implications for research and practice

This research makes several contributions to research. First, we provide a deconstructed view of the supportive and practical competencies a firm needs in order to establish a security culture. While previous studies have presented frameworks and factors that influence security cultures, their focus has been on lower-level, discrete determinants of culture, such as the influence of education and training, monitoring and enforcement and security policies, that may or may not match the competencies of an organisation. In other words, while prior research has provided several recipes for security cultures, it has not considered whether organisations have the ingredients on hand to execute the recipe. As such, our study takes a more foundational view of culture, focusing on the underlying competencies prescribed by HRT and HROs that form a fabric of influence that weaves across the entire organisation. As such, our contribution to understanding security culture is in establishing the higher-level, organisational-wide

competencies that organisations should focus on in order to shape their own cultures—a perspective that has not yet been explored among the numerous frameworks and models on the subject.

Second, our research highlights the concept of organisational mindfulness as part of the prescription for successful security cultures. This finding could provide revolutionary insight for the security culture literature. As the literature reveals, there are many factors that are considered requirements of an effective security culture. However, our research suggests that for these factors to be successfully introduced and utilised in a culture, organisations would benefit from taking steps to become more mindful. The literature on organisational mindfulness is quite prescriptive in how this can be achieved (Ndubisi & Al-Shuridah, 2019), with some guidance specific to its development relative to resiliency (Klockner, 2017).

In terms of practical implications, our research gives organisations and organisational managers some understanding of how their structural and practical competencies interplay to support or develop a security culture. The impact of these competencies on security outcomes is not always clear and by providing empirical support for organisational managers' contribution, our findings should either reinforce their decisions or give credence to any necessary restructuring or development of a collective state of mindfulness. Top management involvement varies within industries. In HROs, due to the importance of safety, besides chief information officers, generally there are CISOs, who are responsible for establishing and maintaining the organisation's vision and strategy to protect the organisation's assets (e.g., data and technology). It is important to have an official role as CISO in HROs due to several reasons. For example, since the chief finance officer (CFO)'s focus is on maintaining a rational budget rather than meeting the needs of the information security program, if the organisation does not have an CISO who can regularly communicate with the CFO, there will not be enough awareness of the needs of the security functions, and allocated funding will probably be inadequate, which leads to the lack of support and implementation of practical competencies and security frameworks within organisations (Karanja, 2017; Maynard et al., 2018).

This research also gives organisational managers an impetus for focusing on the development of organisational mindfulness for achieving a security culture. Organisational managers can inspire organisational mindfulness if they seek multiple and deeper explanations for emerging security issues. Managers can create context by identifying what the organisation expects, supports and rewards in terms of security activities, which in turn promotes security culture. This happens through managers' prioritisation of mindfulness and their establishment of organisational structure and practices including security prevention and detection practices. This study points to a need for organisations to develop a preoccupation with failure, a reluctance to simplify, a sensitivity to operations, a commitment to resilience and a deference to expertise, where otherwise they may not. Admittedly, the concept of organisational mindfulness is sometimes an ambiguous one and its operationalization over time can be a long and daunting journey; however, given this initial foray into the underlying competencies required of a security culture, it seems clear that the benefits of such an effort should outweigh its costs.

5.3 | Limitations and future research directions

The results of this study highlight the influence of a firm's supportive and practical competencies on the development of a security culture, suggesting that as an organisation engages in the practice of threat prevention, detection, response and mitigation, it begins to develop a culture of security, where these practices become entwined in the norms and values of the organisation and its employees. As future threat events occur, the organisation's ability to respond quickly, decisively and effectively is enhanced as everyone is aware of the appropriate response and their role in its execution. The more proficient an organisation is in executing these practices, the stronger their security culture will be.

These results, however, should be viewed in the light of their limitations. First, we collected data from only one population, which may limit the generalizability of this study. For example, while this study included a survey of U.S. security professionals, security professionals from other geographic areas may have a different perspective and

understanding of their firms' supportive and practical competencies. Second, top management participation did not play a large role in the developed model. Although top managers are involved in designing an organisation's strategic alignment and implementing practical competencies, these processes may not be well-integrated enough to improve organisational alignment with InfoSec practices. Future research is needed in order to investigate this issue and better explain the role of top management in establishing InfoSec practices and a security culture in organisations. Third, according to HRT, there could be a feedback loop from high-reliability processes to organisational mindfulness. The entire high-reliability process, including top managers' set of goals, practical competencies and security culture, may also foster and refine the state of organisational mindfulness. Therefore, future studies should investigate the reverse relationships of security culture and HROs' practical and supportive competencies. Moreover, our proposed model may seem a little complex. For a simpler model, future studies could consider utilising the InfoSec processes construct of Rocha Flores et al. (2014) to explore the influence of organisational structure on security culture.

Another limitation of this study, particularly in light of the recent findings presented by Uchendu et al. (2021), is the use of a survey instrument to measure security culture. While the six-item measure of culture by Chen et al. (2015) was validated and has been used successfully in prior research, it does represent a knowledge-focused perspective of culture. As Uchendu et al. (2021) point out, behaviour accompanies knowledge and should be included as an observed assessment of culture. Future research should attend to this recommendation and provide a richer view of security culture.

Finally, there are some important research questions that, although situated outside the scope of the current study, are important to the further exploration and understanding of security cultures. First, scholars should ask if the findings of this study are applicable across all organisational types or if they are restricted solely to those firms that mirror the characteristics of HROs. This is an important question in that, just as not all firms share the same appetite for risk, not all firms have the same appetite for resiliency, or have a level of knowledge sharing required to be mindful. These competencies take time and a focused effort to develop, and it is not clear if certain types of organisations (e.g., small, domestic, regional, etc.) are better positioned to develop them than others. Second, scholars should ask how top management could do more in helping shape the formation of a security culture. Clearly, top management is an important factor in a firm's ability to procure resources and transform them into the security knowledge base of a firm (Hassandoust et al., 2022). However, the findings of these research raise some questions about how top management can support their practical competencies, and ultimately, their security culture. Thirdly, although there is a minor risk of security criminals using this research for nefarious purposes, we considered this point carefully and concluded that the benefits of the research outweigh the minor risks. However, future research should be tuned to the fact that the efforts of an organisation to secure itself could backfire or be used against it by insiders and outsiders with malicious intentions and that the research used to guide their efforts is accessible by both good and bad actors.

6 | CONCLUSION

A strong culture of security is vital to an organisation's ability to reliably mitigate threats that permeate the modern, global business environment; yet, for all the frameworks and models that academia have provided to guide our understanding of how security culture is formed, organisations continue to struggle with its development. To provide a helpful perspective, we looked to HRT and the examples of HROs to articulate a SCM that explains security culture as a product of the supportive and practical competencies of an organisation. Through this model, organisations can understand that their focus should be on enhancing their organisational mindfulness and security practices over their structural arrangements, ultimately following an organic approach to security culture development as a product of their competencies rather than the current discrete set of factors espoused in the literature that may or may not align with their strengths.

ACKNOWLEDGMENT

Open access publishing facilitated by Auckland University of Technology, as part of the Wiley - Auckland University of Technology agreement via the Council of Australian University Librarians.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

ORCID

Farkhondeh Hassandoust https://orcid.org/0000-0001-7190-9527

Allen C. Johnston https://orcid.org/0000-0003-0301-4187

REFERENCES

Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing*, *25*(2), 357–370.

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98*(102003), 102003.

Ashenden, D., & Sasse, A. (2013). CISOs and organisational culture: Their own worst enemy? *Computers & Security*, *39*, 396–405.

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.

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management*, *51*(1), 138–151.

Becker, J. M., Klein, K., & Wetzels, M. (2012). Hierarchical latent variable models in PLS-SEM: Guidelines for using reflective-formative type models. *Long Range Planning*, *45*(5–6), 359–394.

Bogner, W. C., & Thomas, H. (1992). Core competence and competitive advantage: A model and illustrative evidence from the pharmaceutical industry. In *BEBR faculty working paper*. University of Illinois: University of Illinois.

Boin, A., & Schulman, P. (2008). Assessing NASA's safety culture: The limits and possibilities of high-reliability theory. *Public Administration Review*, *68*(6), 1050–1062.

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

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

Burns, A. (2019). Security organizing: A framework for organizational information security mindfulness. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *50*(4), 14–27.

Burns, A., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, *68*, 190–209.

Butler, B. S., & Gray, P. H. (2006). Reliability, mindfulness, and information systems. *MIS Quarterly*, *30*, 211–224.

Carlo, J. L., Lyytinen, K., & Boland, R. J., Jr. (2012). Dialectics of collective minding: Contradictory appropriations of information technology in a high-risk project. *MIS Quarterly*, *36*, 1081–1108.

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems*, *55*(3), 11–19.

Child, J. (1984). *Organization: A guide to problems and practice*. Harper and Row.

Chin, W. W., & Dibbern, J. (2010). An introduction to a permutation based procedure for multi-group PLS analysis: Results of tests of differences on simulated data and a cross cultural analysis of the sourcing of information system services between Germany and the USA. In *Handbook of partial least squares* (pp. 171–193). Springer.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Creswell, J. W., & Poth, C. N. (2016). *Qualitative inquiry and research design: Choosing among five approaches*. Sage Publications.

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, *92*, 1–23.

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196–207.

Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, *49*, 162–176.

Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security*, *70*, 72–94.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal*, *11*(2), 127–153.

Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting information security culture: An organizational transformation case study. *Computers & Security*, *56*, 63–69.

Duarte, P., & Amaro, S. (2018). Methods for modelling reflective-formative second order constructs in PLS. *Journal of Hospitality and Tourism Technology*, *9*(3), 259–313. https://doi.org/10.1108/JHTT-09-2017-0092

Dube, D. P., & Mohanty, R. (2020). Towards development of a cyber security capability maturity model. *International Journal of Business Information Systems*, *34*(1), 104–127.

Dutton, J. E., Ashford, S. J., O'Neill, R. M., & Lawrence, K. A. (2001). Moves that matter: Issue selling and organizational change. *Academy of Management*, *44*(4), 716–736.

Elyas, M., Ahmad, A., Maynard, S. B., & Lonie, A. (2015). Digital forensic readiness: Expert perspectives on a theoretical framework. *Computers & Security*, *52*, 70–89.

Francis, J. J., Johnston, M., Robertson, C., Glidewell, L., Entwistle, V., Eccles, M. P., & Grimshaw, J. M. (2010). What is an adequate sample size? Operationalising data saturation for theory-based interview studies. *Psychology and Health*, *25*(10), 1229–1245.

Friedberg, I., Skopik, F., Settanni, G., & Fiedler, R. (2015). Combating advanced persistent threats: From network event correlation to incident detection. *Computers & Security*, *48*, 35–57.

Gefen, D., Rigdon, E. E., & Straub, D. (2011). Editor's comments: An update and extension to SEM guidelines for administrative and social science research. *MIS Quarterly*, *35*(2), iii–xiv.

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing mitre att&ck risk using a cyber-security culture framework. *Sensors*, *21*(9), 3267.

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022). Detecting insider threat via a cyber-security culture framework. *Journal of Computer Information Systems*, *62*(4), 706–716.

Gold, A. H., Malhotra, A., & Segars, A. H. (2001). Knowledge management: An organizational capabilities perspective. *Journal of Management Information Systems*, *18*(1), 185–214.

Grabowski, M., & Roberts, K. (1997). Risk mitigation in large-scale systems: Lessons from high reliability organizations. *California Management Review*, *39*(4), 152–161.

Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling*. Sage publications.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, *19*(2), 139–152.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2–24.

Hair, J. F., Sarstedt, M., Ringle, C. M., & Gudergan, S. P. (2017). Advanced issues in partial least squares structural equation modeling. Sage Publications.

Hassandoust, F., Subasinghage, M., & Johnson, A. C. (2022). A neo-institutional perspective on the establishment of information security knowledge sharing practices. *Information & Management*, *59*(1), 1–11.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115–135.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615–660.

Jarvenpaa, S. L., & Ives, B. (1991). Executive involvement and participation in the management of information technology. *MIS Quarterly*, *15*(2), 205–227.

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, *34*(2), 597–626.

Johnston, A. C., Gangi, P. D., Howard, J., & Worrell, J. (2019). It takes a village: Understanding the collective security efficacy of employee groups. *Journal of the Association for Information Systems*, *20*(3), 186–212.

Kabue, L. W., & Kilika, J. M. (2016). Firm resources, core competencies and sustainable competitive advantage: An integrative theoretical framework. *Journal of Management and Strategy*, *7*(1), 98–108.

Karanja, E. (2017). The role of the chief information security officer in the management of IT security. *Information & Computer Security*, *25*(3), 300–329.

Karlsson, F., Åström, J., & Karlsson, M. (2015). Information security culture–state-of-the-art review between 2000 and 2013. *Information & Computer Security*, *23*(3), 246–285.

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly Executive*, *9*(3), 2012–2052.

Klockner, K. (2017). Strategically developing a resilient safety culture: Organizational mindfulness and mindful organizing. In P. Arezes (Ed.), *Advances in safety management and human factors. AHFE 2017. Advances in Intelligent Systems and Computing* (Vol. 604). Springer. https://doi.org/10.1007/978-3-319-60525-8_12

Knapp, K. J., Marshall, T. E., Kelly Rainer, R., & Nelson Ford, F. (2006). Information security: management's effect on culture and policy. *Information Management & Computer Security*, *14*(1), 24–36.

Landis, J. R., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics*, *33*, 159–174.

Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management. *MIS Quarterly*, *31*, 59–87.

Lu, G., Koufteros, X., & Lucianetti, L. (2017). Supply chain security: A classification of practices and an empirical study of differential effects and complementarity. *IEEE Transactions on Engineering Management*, *64*(2), 234–248.

Lu, G., Koufteros, X., Talluri, S., & Hult, G. T. M. (2019). Deployment of supply chain security practices: Antecedents and consequences. *Decision Sciences*, *50*(3), 459–497.

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly*, *35*(2), 293–334.

Martins, A., & Eloff, J. (2002). Information security culture. In *Security in the information society* (pp. 203–214). Springer.

Masrek, M. N., Harun, Q. N., Ramli, I., & Prasetyo, H. (2019). The Role of Top Management in Information Security Practices. In *Paper presented at the The 6th International Conference on Education, Social Sciences and Humanities*.

Maynard, S., Onibere, M., & Ahmad, A. (2018). Defining the strategic role of the chief information security officer. *Pacific Asia Journal of the Association for Information Systems*, *10*(3), 3–86.

Montesdioca, G. P. Z., & Maçada, A. C. G. (2015). Measuring user satisfaction with information security practices. *Computers & Security*, *48*, 267–280.

Morone, J. G., & Woodhouse, E. J. (1986). *Averting catastrophe: Strategies for regulating risky technologies*. University of California Press.

Ndubisi, N. O., & Al-Shuridah, O. (2019). Organizational mindfulness, mindful organizing, and environmental and resource sustainability. *Business Strategy and the Environment*, *28*(3), 436–446.

Nel, F., & Drevin, L. (2019). Key elements of an information security culture in organisations. *Information & Computer Security*, *27*(2), 146–164.

NIST. (2012). Guide for conducting risk assessments. *NIST Special Publication*, 800–830 Retrieved from https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

Njenga, K., & Brown, I. (2012). Conceptualising improvisation in information systems security. *European Journal of Information Systems*, *21*(6), 592–607.

O'Brien, J., Islam, S., Bao, S., Weng, F., Xiong, W., & Ma, A. (2013). *Information security culture: Literature review*. *Unpublished Working Paper*. *University of Melbourne*.

O'Neil, P. D., & Krane, D. (2012). Policy and organizational change in the Federal Aviation Administration: The ontogenesis of a high-reliability organization. *Public Administration Review*, *72*(1), 98–111.

Parrish, J. J. L., Kuhn, J. R., Jr., & Courtney, J. F. (2008). Mindful administration of IS security policies. *Proceedings of the Fourteenth Americas Conference on Information Systems, Toronto, ON, Canada August 14th-17th 2008* (p. 270).

Perrow, C. (1994). The limits of safety: The enhancement of a theory of accidents. *Journal of Contingencies and Crisis Management*, *2*(4), 212–220.

Petter, S., Straub, D., & Rai, A. (2007). Specifying formative constructs in information systems research. *MIS Quarterly*, *31*(4), 623–656.

Pfleeger, C., Pfleeger, S. L., & Jonathan, M. (2015). *Security in computing* (5th ed.). Prentice-Hall.

Pietkiewicz, I., & Smith, J. A. (2014). A practical guide to using interpretative phenomenological analysis in qualitative research psychology. *Psychological Journal*, *20*(1), 7–14.

Porte, T. L., & Consolini, P. (1998). Theoretical and operational challenges of "high-reliability organizations": Air-traffic control and aircraft carriers. *International Journal of Public Administration*, *21*(6–8), 847–852.

Rath, J., Ischi, M., & Perkins, D. (2014). Evolution of different dual-use concepts in international and national law and its implications on research ethics and governance. *Science and Engineering Ethics*, *20*, 769–790.

Ray, J. L., Baker, L. T., & Plowman, D. A. (2011). Organizational mindfulness in business schools. *Academy of Management Learning & Education*, *10*(2), 188–203.

Roberts, K. H. (1990a). Managing high reliability organizations. *California Management Review*, *32*(4), 101–113.

Roberts, K. H. (1990b). Some characteristics of one type of high reliability organization. *Organization Science*, *1*(2), 160–176.

Roberts, K. H., & Bea, R. (2001). Must accidents happen? Lessons from high-reliability organizations. *Academy of Management Perspectives*, *15*(3), 70–78.

Roberts, K. H., Rousseau, D. M., & La Porte, T. R. (1994). The culture of high reliability: Quantitative and qualitative assessment aboard nuclear-powered aircraft carriers. *The Journal of High Technology Management Research*, *5*(1), 141–161.

Rocha Flores, W., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, *43*, 90–110.

Rosa, E. A. (2005). Celebrating a citation classic––And more. *Organization & Environment*, *18*, 229–234.

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security*, *26*(1), 56–62.

Sagan, S. D. (1995). *The limits of safety: Organizations, accidents, and nuclear weapons*. Princeton University Press.

Salovaara, A., Lyytinen, K., & Penttinen, E. (2019). High reliability in digital organizing: Mindlessness, the frame problem, and digital operations. *MIS Quarterly*, *43*(2), 555–578.

Schein, E. H. (2010). *Organizational culture and leadership* (Vol. 2). John Wiley & Sons.

Schulman, P. R. (2020). Organizational structure and safety culture: Conceptual and practical challenges. *Safety Science*, *126*(104), *669*.

Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying factors of "organizational information security management". *Journal of Enterprise Information Management*, *27*(5), 644–667.

Sinkovics, N. (2018). Pattern matching in qualitative analysis. In C. Cassell, A. L. Cunliffe, & G. Grandy (Eds.), *The SAGE handbook of qualitative business and management research methods: Methods and challenges*. Sage Publications.

Siponen, M. (2002). Towards maturity of information security maturity criteria: Six lessons learned from software maturity criteria. *Information Management & Computer Security*., *10*, 210–224.

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: an empirical study. In *New approaches for security, privacy and trust in complex environments: Proceedings of the IFIP TC-11 22nd International Information Security Conference (SEC 2007), 14–16 May 2007* (Vol. 22, pp. 133–144). Springer.

Smith, J. A., & Fieldsend, M. (2021). *Interpretative phenomenological analysis*. American Psychological Association.

Speier, C., Whipple, J. M., Closs, D. J., & Voss, M. D. (2011). Global supply chain design considerations: Mitigating product safety and security risks. *Journal of Operations Management*, *29*(7–8), 721–736.

Streukens, S., & Leroi-Werelds, S. (2016). Bootstrapping and PLS-SEM: A step-by-step guide to get more out of your bootstrap results. *European Management Journal*, *34*(6), 618–632.

Taber, K. S. (2018). The use of Cronbach's alpha when developing and reporting research instruments in science education. *Research in Science Education*, *48*(6), 1273–1296.

Tashakkori, A., Teddlie, C., & Teddlie, C. B. (1998). *Mixed methodology: Combining qualitative and quantitative approaches*. SAGE Publications.

Teddlie, C., & Tashakkori, A. (2009). *Foundations of mixed methods research: Integrating quantitative and qualitative approaches in the social and behavioral sciences*. Sage.

Teo, T. S., Srivastava, S. C., & Jiang, L. (2008). Trust and electronic government success: An empirical study. *Journal of Management Information Systems*, *25*(3), *99*–132.

Thomson, K.-L., Von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security*, *2006*(10), 7–11.

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, *109*(102), 387.

van de Walle, B., & Turoff, M. (2008). Decision support for emergency situations. In *Handbook on decision support systems 2* (pp. 39–63). Springer.

Van Niekerk, J., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, *29*(4), 476–486.

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly*, *37*(1), 21–54.

Venkatesh, V., Brown, S. A., & Sullivan, Y. W. (2016). Guidelines for conducting mixed-methods research: An extension and illustration. *Journal of the Association for Information Systems*, *17*(7), 2–494.

Vogus, T. J., & Sutcliffe, K. M. (2007). The impact of safety organizing, trusted leadership, and care pathways on reported medication errors in hospital nursing units. *Medical Care*, *45*, 997–1002.

Vogus, T. J., & Sutcliffe, K. M. (2012). Organizational mindfulness and mindful organizing: A reconciliation and path forward. *Academy of Management Learning & Education*, *11*(4), 722–735.

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, *23*(5), 371–376.

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems*, *92*, 25–35.

Weick, K. E. (1987). Organizational culture as a source of high reliability. *California Management Review*, *29*(2), 112–127.

Weick, K. E. (2009). *Making sense of the organization* (Vol. 2). John Wiley & Sons.

Weick, K. E., & Sutcliffe, K. M. (2001). *Managing the unexpected: Assuring high performance in an age of complexity*. *In*. Jossey Bass Publishers.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (1999). Organizing for high reliability: Processes of collective mindfulness. *Research in Organizational Behavior*, *21*, 13–81.

Wildavsky, A. B. (1988). *Searching for safety* (Vol. 10). Transaction publishers.

Wolf, F. (2005). Resource availability, commitment and environmental reliability & safety: A study of petroleum refineries. *Journal of Contingencies and Crisis Management*, *3*(1), 81–123.

Wright, R. T., Campbell, D. E., Thatcher, J. B., & Roberts, N. (2012). Operationalizing multidimensional constructs in structural equation modeling: Recommendations for IS research. *Communications of the Association for Information Systems*, *30*(1), *23*.

Zakaria, O., & Gani, A. (2003). A conceptual checklist of information security culture. In *2nd European conference on information warfare and security, Reading*, UK.

AUTHOR BIOGRAPHIES

Farkhondeh Hassandoust is Senior Lecturer in Business Information Systems, at Auckland University of Technology. Farkhondeh's research interests include information security and privacy, IS in healthcare and IS use. Her works have been published in *Information and Management Journal*, *Journal of the American Medical Informatics Association*, *Behaviour and IT*, *IS Frontiers*, among others. She has also presented her works in international conferences such as Internal Conference on Information Systems, European Conference on Information Systems and Pacific Asia Conference on Information Systems. Her research has been supported by grants from Auckland University of Technology Vice-Chancellor's Scholarship and Internet New Zealand.

Allen C. Johnston is the Hewson Professor of Cybersecurity and a Professor of Management Information Systems (MIS) in the Culverhouse College of Business at the University of Alabama. The primary focus of his research is in the areas of behavioural information security, privacy, data loss prevention, collective security and innovation. His research can be found in such outlets as *MIS Quarterly*, *Journal of Information Technology*, *Journal of the AIS*, *European Journal of Information Systems*, *Information Systems Journal*, *Decision Sciences*, *Decision Support Systems* and *Communications of the ACM*, among others. He currently serves as an Associate Editor for *MIS Quarterly* and Senior Editor for *European Journal of Information Systems*, as well as serving on the Editorial Review Board for the *Journal of the AIS*. He is a founding member and current Chair of the IFIP Working Group on Information Systems Security Research (WG8.11/11.13). Dr. Johnston has also served as a consultant, visiting professor or invited speaker at several universities, workshops, panels and companies in the United States and abroad, including as a Visiting Erskine Fellow at the University of Canterbury, Auburn University, Kennesaw State University and the University of Oulu.

SUPPORTING INFORMATION

Additional supporting information can be found online in the Supporting Information section at the end of this article.

How to cite this article: Hassandoust, F., & Johnston, A. C. (2023). Peering through the lens of high-reliability theory: A competencies driven security culture model of high-reliability organisations. *Information Systems Journal*, *33*(5), 1212–1238. https://doi.org/10.1111/isj.12441