2020

Deployment of Information Security Practices: The High Reliability Theory Perspective

Farkhondeh Hassandoust

Allen C. Johnston

Deployment of Information Security Practices: The High Reliability Theory Perspective

Completed research paper

Farkhondeh Hassandoust
Business Information Systems Department
Auckland University of Technology
Auckland, New Zealand
Email: ferry@aut.ac.nz

Allen C. Johnston
Culverhouse College of Business
University of Alabama
Tuscaloosa, USA
Email: ajohnston@cba.ua.edu

Abstract

Drawing on high reliability theory, this study investigates how a firm's information security (InfoSec) practices as practical proficiencies form its organisational security culture. We tested the model using survey data from 602 professional managers in Australia and New Zealand who are aware of the InfoSec programmes within their respective organisations, the findings of which suggest a security culture is influenced by a firm's practical proficiencies in the form of InfoSec practices namely prevention, detection and response practices. Our findings also emphasise the importance of organisational supportive proficiencies as organisational structure for improving the impact of InfoSec preventive practices on organisational security culture in a firm. The results of this study provide both academics and practitioners an understanding of the vital organisational dynamics necessary to establish a culture of security.

Keywords Information security practices, security culture, high reliability theory

1 Introduction

The security culture of an organisation encompasses the values and beliefs of the firm that direct the security-related behaviours and assumptions of its employees (Van Niekerk and Von Solms 2010). It is the security culture that reflects both the espoused values and shared tacit assumptions of an organisation as it pertains to security events and both collective and individual responses to those events. When new threats emerge that are not readily addressed in policy, the organisation's security culture may help direct the activities of the employees to produce security outcomes that go above and beyond what is actually prescribed in policy. For instance, in the event that a novel social engineering attack is administered against an organisation, how the organisation will respond to this threat is influenced by its security culture.

For many organisations, however, such a culture doesn't exist, or is under-developed, leaving the firm relatively vulnerable to any number of external and internal threats, errors, or mishaps (Da Veiga and Eloff 2010). Under-developed security cultures can leave a firm less secure, scrambling for guidance and assumptions for security responses in the event of a security incident. In such cases, socio-cultural norms within the organisation are either inactive or ineffective, and how employees communicate and respond to others and to formal and informal organisational forces is unpredictable and unreliable. Moreover, under-developed security cultures leave organisations without the necessary framework for self-inspection, reflection, and consequently, and the opportunity to improve upon its mistakes (Ruighaver et al. 2007). Toward assisting these exposed firms, both academics and practitioners have focused considerable energy on exploring the factors and metrics that are essential to an effective, lasting security culture (Da Veiga and Eloff 2010; Martins and Elofe 2002; Van Niekerk and Von Solms 2010). Yet, despite these efforts, it is still not clear how security cultures are formed and what the key drivers of them are.

In this study, we focus on the practical and supportive proficiencies of an organisation that direct its employee behaviours and establish the norms of the organisation. In this context, we refer to a firm's practical proficiencies as its information security (InfoSec) practices. These are the set of procedures designed to: protect organisational information assets and information systems (IS) (Ahmad et al. 2014); detect any potential security attack (Hamill et al. 2005); react to InfoSec incidents (Baskerville et al. 2014); or take some actions to reduce caused losses (Lu et al. 2017). The supportive proficiencies of a firm are its functional and intellectual arrangements that facilitate its security practices. For most organisations, these proficiencies emerge organically as the organisations engage in the activities that provide value to their stakeholders and position them competitively within their industries (Da Veiga and Martins 2015; Dhillon et al. 2016; Martins and Elofe 2002), but in terms of their impact on a security culture, their emergence is anything but organic and their value is far less understood. For this reason, we ask, what are the key practice and supportive proficiencies of an organisation that are most influential in forming a culture of security and how is this influence formed?

To answer these questions, we can turn to an organisational theory focused on the firm-level proficiencies that lead to the development of cultural outcomes, High Reliability Theory (HRT). HRT associates an organisation's culture with high reliability in that for a culture to take shape, reliable outcomes must come from the assumptions, norms, and decision making practices that occur within the organisation over time (Boin and Schulman 2008). We believe similar patterns of reliable outcomes are also associated with security cultures. This study is part of a larger project with a mixed, multi-study research design. In the current study, we develop and test a model that explains a security culture as a product of an organisation's key practical and supportive proficiencies.

This research manuscript unfolds as follows. First, we present a review of the literature concerning security culture. We then describe HRT and its appropriateness for this study. We then propose a set of hypotheses and test the model. We then conclude with a discussion of its implications to research and practice.

2 Literature Review

2.1 Security Culture

HRT Security culture as an organisational sub-culture with a specific purpose of InfoSec, entails an understanding and awareness of InfoSec issues and policies (Chen et al. 2015; Pfleeger et al. 2015). The aims and objectives of a security culture should be aligned with formal business processes and

organisational culture (Dhillon and Backhouse 2001) and should include all socio-cultural countermeasures that support technical security measures (Chen et al. 2015). Further, cultivating an security-aware culture mitigates the privacy and security risks to information assets and IS within organisations (Da Veiga and Eloff 2010; Nel and Drevin 2019).

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 and 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 culture has been investigated from several aspects, such as defining the culture (e.g., Furnell and Thomson 2009; Van Niekerk and Von Solms 2010), the principles and frameworks on which a security culture could be based (e.g.,Da Veiga and Martins 2015; Martins and Elofe 2002; Ruighaver et al. 2007; Zakaria and Gani 2003), and their organisational cultural and behavioural levels (e.g., Da Veiga and Eloff 2010; Martins and Elofe 2002). Drawing on a security culture framework, previous researchers have explored a number of factors that influence security cultures, such as the role of chief information security officers, top management support, education and training, monitoring and enforcement, and security policies (e.g., Ashenden and Sasse 2013; Chen et al. 2015; Da Veiga 2018; Da Veiga and Eloff 2010; Da Veiga and Martins 2015). However, very few of these studies have focused on the key proficiencies of an organisation that facilitate its culture of security. Moreover, there is a lack of theoretical foundations to support the process of establishing a security culture.

2.2 InfoSec Practices

There are a number of broadly recognised InfoSec management frameworks available to instruct organisations in planning and operating their InfoSec practices such as ISO (Tittle et al. 1986) standards and COBIT (Brand and Boonen 2007) that prescribe formal, technical and InfoSec countermeasures (Åhlfeldt et al. 2007). Most of these InfoSec frameworks are universal in scope with quality control principles such as Plan-Do-Check-Act. Such quality control principles have proven valuable for routine InfoSec activities that support historical comparisons (Baskerville et al. 2014). Sophisticated InfoSec management approaches design controls based on risk analysis and concentrate on preventing the continuation of known InfoSec threats (Baskerville 1988). However, the prevention-oriented frameworks (reliability and exploitation) with their predefined control sets might be less ideal in today's dynamic InfoSec threat environment (Baskerville et al. 2014). In this environment, organisations face the need to detect new InfoSec threats and new forms of attacks (Antunes et al. 2010). Therefore, organisations require a more response-oriented InfoSec philosophy (validity and exploration) in addition to the existing preventive frameworks.

Organisational InfoSec practices are a set of procedures and activities designed to protect the integrity, availability and confidentiality of organisational information assets that include IS (Burns 2019). InfoSec practices can be categorized into four classes based on their intent, namely detection, prevention, response and mitigation (Lu et al. 2017; Lu et al. 2019). Prevention is the most commonly used InfoSec strategy to proactively protect information assets from being breached or exploited (Ahmad et al. 2014; Liu et al. 2001). Prevention strategies are developed to be activated before an InfoSec breach happens (Lu et al. 2017). *Prevention* practices can be implemented to avoid information leakage. Examples include a periodic clean desk practice for sensitive documents (Ahmad et al. 2014), encrypting information flowing over networks to prevent leakage and using firewalls to filter network traffic (Zalenski 2002). *Detection* practices are designed to be utilized before or sometimes during an InfoSec breach (Lu et al. 2017). For effectiveness, the detection of an attack and subsequent reporting to the InfoSec managers must be timely (Hamill et al. 2005). This reported information should be actionable such as based on whether an attack has begun, when the attack began, and what is the scope of the attack (Henauer 2003; Stytz 2004).

Response practices are intended to react to InfoSec incidents that either have occurred or are happening (Baskerville et al. 2014). Response practices include appropriate corrective actions against identified attacks and short-term responses such as mobilizing equipment to respond to the emergency and bringing necessary systems and services back online (Ahmad et al. 2014; Speier et al. 2011). The response stage can be divided into two phases: the reaction phase, where appropriate actions are taken against the attack, and the recovery phase, where the situation is restored to its original state (Hamill et al. 2005; Saydjari 2004). *Mitigation* is a set of preplanned practices aimed at reducing losses by lessening the impact of InfoSec breaches (Sheffi 2005). Mitigation practices boost the ability of organisations to recover before severe and enduring effects materialize (Lu et al. 2017). In

an endeavor to mitigate the detrimental effects and ease the painful consequences of an InfoSec breach, organisations may take various approaches such as cross-training employees in InfoSec measures to enable even unskilled employees to perform these measures.

2.3 Organisational Structure

An organisational structure is defined as " the formal allocation of work roles and the administrative mechanisms to control and integrate work activities, including those that cross formal organisational boundaries" (Child 1984 p. 2). The importance of organisational structures has been discussed for a long period of time. For example, Child has argued the essential role of organisational structure in designing an effective organisation (Child 1984). Organisational structure assigns human and technical resources to the activities that need to be done and the supportive mechanisms for their coordination (Rocha Flores et al. 2014). Further, organisational structure determines and facilitates operational and strategic decision making and monitors the performance and operating mechanisms that transfer instructions on what is expected of organisational employees and how the instructions should be followed (Child 1984).

Organisational structure plays a key role in making an InfoSec governance plan successful (Von Solms and Von Solms 2004). In an InfoSec context, organisational structure is defined as the organisation of InfoSec functions (Kraemer and Carayon 2007) and refers to the formal and informal structures that expresses the organisational hierarchy. As such, it involves the processes that combine people into workgroups and establishes who does what and how to communicate to get the tasks completed (Warkentin and Johnston 2008). Kayworth and Whitten (Kayworth and Whitten 2010) classified organisational structure as either a formal organisational structure or a coordinating structure (see Figure 1). Formal organisational structure refers to the formalized structures that are implemented to support the management of InfoSec matters within an organisation (Rocha Flores et al. 2014).

According to (Kayworth and Whitten 2010), formal organisational structures may include having a formal InfoSec unit within the organisation whose mission is to secure the organisation's information assets. The purpose of this unit is to develop and implement the organisation's standards and practices governing organisation-wide InfoSec. Coordinating organisational structures refer to formal and informal meetings among a group of people responsible for InfoSec tasks and representatives from various business units in the organisation to facilitate the communication of strategic business plans between business and InfoSec functions (Kayworth and Whitten 2010; Rocha Flores et al. 2014).

3 Theoretical Background

To understand how a firm's practical and supportive proficiencies have a controlling influence over its culture of security, we first need to understand how security cultures are formed and the factors that are important to their presence. 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.

3.1 High Reliability Theory

HRT concentrates on the processes that an organisation can implement to ensure continued organisational reliability and mitigate or even eliminate the possibility of incidents (Roberts 1990a; Roberts 1990b). Although these processes and strategies are not always completely developed or entirely implemented in organisations, taken together, these strategies suggest the elements of a complete system for preventing catastrophes (Morone and Woodhouse 1986; Perrow 1994). HRT demands safety, and there are two strategies for achieving safety: anticipation that entails efforts to predict and prevent possible incidents from occurring before they have ever happened; and resilience, efforts to deal with incidents once they become manifest (Perrow 1994; Wildavsky 1988).

There are four critical causal factors for achieving high reliability in organisations (Perrow 1994; Sagan 1995): 1) top managers put safety and reliability first as a goal; 2) setting up high levels of redundancy in personnel and technical safety measures; 3) developing a 'high reliability culture' in decentralised and continually practiced operations; and 4) advanced types of trial and error organisational learning. Organisational culture is part of 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).

Much of HRT research has focused on specific organisations that could potentially experience a major failure with substantial consequences but have shown themselves to be highly reliable despite their

high risk environment (e.g., aircraft carriers, air traffic control, and nuclear power plants) (e.g., Porte and Consolini 1998; Roberts et al. 1994) as a result of a deliberate process by which risks are monitored, evaluated, and mitigated (Perrow 1994). These organisations show an immense capacity to react to and learn from such incidents, avoid disabling, and to restructure their procedures to mitigate future incidents and avoid major failures (Weick and Sutcliffe 2001). There is a growing body of literature describing the complementary nature of HRT from an integration of organisational practice perspective with a focus on the protection mechanisms that organisations can put in place to best react to organisational (security) disruption (Rijpma 1997).

HRT has developed robust research streams across business, sociology, healthcare, and other disciplines (e.g., Boin and Schulman 2008; Sagan 1995; Wolf 2005). While HRT has not been widely applied in InfoSec research, its focus on organisational reliability creates a meaningful lens to assess InfoSec practices within organisations. InfoSec practices can be implemented to assure continued organisational reliability (Speier et al. 2011). Having protective and responsive strategies, practices, and personnel in place can enable the organisations to respond more effectively (Lu et al. 2017). HRT has implications for intentional events as illustrated by changes in IS and InfoSec systems. For example, computer hackers have become highly sophisticated in their ability to transmit increasingly elaborate InfoSec threats. Therefore, computer software programs and organisations' security procedures should be designed in a way that prevents these intentional actions that can compromise confidential information.

4 Research Model and Hypothesis Development

We establish an initial research model and hypotheses that reflect HRT in the context of an organisational security culture, as shown in Figure 1. Because HRT focuses on processes that result in highly reliable outcomes, it helps explain the practical and supportive proficiencies that lead to the organisational mechanisms that produce reliable outcomes, such as a security culture.

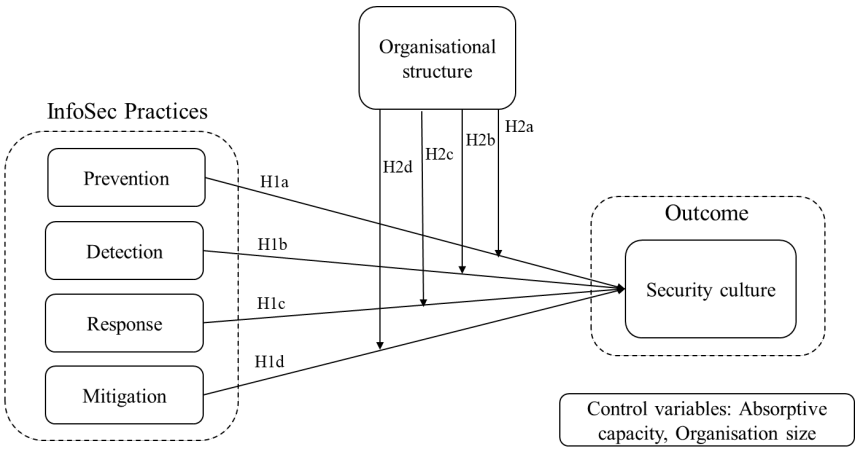

Figure 1: Proposed research model

In this conceptual model security culture is presented as an outcome of InfoSec practices, namely prevention, detection, response, and mitigation practices. These are practical proficiencies of an organisation. 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, following which a response takes place (Baskerville et al. 2014). Detection is an operational-level practice that aims in identifying specific InfoSec behaviour such as intrusion and misuse behaviours (Hamill et al. 2005). Response practices are designed to take effect during or after an InfoSec breach has happened (Lu et al. 2017). Attacks are sophisticated and generally difficult to evaluate in advance. Thus, countermeasure practices should be agile and designed for unexpected and unpredictable risks by promptly adopting customized safeguards (Baskerville et al. 2014). Mitigation practices are designed to be activated before an InfoSec breach occurs (Lu et al. 2017). If or when an organisation suffers a crisis, further measures include developing alternative material sources as back-up processes, focusing on resilience, reconsidering the IS design and maintaining redundancy (Lu et al. 2017).

According to HRT, if common InfoSec controls and practices are correctly implemented, they are able to reduce security risks (Barton et al. 2016) and assure organisational reliability (Speier et al. 2011).

Automated InfoSec prevention practices reduce risk from some InfoSec threats (Barton et al. 2016; Friedberg et al. 2015), but employees' InfoSec compliance increases the effectiveness of non-automated InfoSec practices (Montesdioca and Maçada 2015; Siponen et al. 2007).

Based on HRT, in order to maintain reliability and safety, organisations should concentrate on a set of practices to mitigate or even prevent potential incidents (Roberts 1990a; Roberts 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 in an organisation. These practices can be designed with different emphases – either to foster organisational capability to discover (i.e., detect and prevent) unexpected InfoSec incidents or to nurture organisational capability to manage (i.e., respond and mitigate) unexpected InfoSec events. Thus, we hypothesize the following:

H1(a-d): Prevention (a), detection (b), response (c), and mitigation (d) practices are positively associated with the security culture in an organisation.

Flexible organisational structures have a rapid tempo for their buildup and maturation stages, as well as a bureaucracy for the maintenance and resolution phase which equips the organisation to be able to effectively respond to events in their environment (Grabowski and Roberts 1997). Flexible organisational structures also empower employees to enact choices that reinforce the organisational culture, which in turn, would change the tempo and nature of organisations in response to internal and external events and changes (Grabowski and Roberts 1997).

As a key supportive proficiency of an organisation, an organisational structure ensures the alignment between the organisation's security practices, functions and business strategies, facilitates the effective organisation of its InfoSec function, contributes to its successful implementation and coordination of InfoSec plans and practices (Kayworth and 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 and Von Solms 2004). In this study, organisational structure is manifested through the two forms of structure: 1) a formalised structure which refers to a centralised InfoSec function and supports the development and positioning of uniform organisation-wide security practices. A formalised structure also supports the handling of InfoSec matters throughout the organisation (Rocha Flores et al. 2014) and 2) a coordinating structure which refers to the utilisation of a variety of coordinating InfoSec committees and groups that meet to discuss important InfoSec issues both formally and informally. With the support of the formal and coordinating structure, the InfoSec function gains valuable insights from the business to facilitate strategic decision making and security culture is better enforced through this channel. To more thoroughly understand the positive impact of organisational structure as a supportive proficiency for the development of a security culture, the following hypotheses are postulated:

H2(a-d): Organisational structure has positively moderated the relationships between InfoSec practices of an organisation, namely prevention (a), detection (b), response (c), mitigation (d) and the security culture in organisation.

5 Research Design

The assessment of the proposed research model was conducted via a survey of 602 AUS and NZ security professionals who are aware of their organisational security-related policies, with responsibilities across a range of roles and company sizes. The data collection has been conducted through the Cint platform, a third-party market research industry. The measurement items on InfoSec practices (detection, prevention, response and mitigation) were adopted from Lu and colleagues (2017). For organisational structure, we adopted items from Rocha Flores and colleagues (2014). The six items measuring security culture were adopted from Chen et al (Chen et al. 2015). A summary of the conceptual definition of each construct and related measurement items, is presented in the Appendix A. A five-point Likert scale (strongly disagree, disagree, neither agree nor disagree, agree and strongly agree) was used to measure all of these key constructs. All the constructs of the measurement model are first-order reflective constructs except organisational structure that considered as a formative second-order construct with two reflective first-order factors including formal structure and coordinating structure. In terms of organisational roles, 38.7% of participants were chief executive officers, 18.1% of participants were a senior manager in the IT or Security department, 13.4% were chief information officer or chief information security officer. Almost half of the companies (47.9%) were in small size with 1-19 employees, 29.5% of the companies were in medium size (20-199 employees), and 22.6% of the companies were in large size (over 200

employees). Majority of the companies had been located in Australia (70.7%) and most of them were in business for more than five years (64.5%).

5.1 Measurement Model Assessment

We used Partial Least Squares – Structural Equation Modeling (PLS-SEM) SmartPLS 3.0 software to assess the measurement and structural models. PLS-SEM has been adopted as the most common approach in quantitative research studies to examine the relationships between variables in human information security behaviours (Bulgurcu et al. 2010; Rocha Flores et al. 2014; Warkentin et al. 2016) and is recommended for testing models that contain formative constructs (Petter et al. 2007).

To reduce the potential for common method bias (CMB), we followed procedural guideline established in the literature (MacKenzie et al. 2011). The implemented procedural and statistical remedies include Harman's single factor test (Harman 1976), Lindell and Whitney's (2001) marker variable test, Full collinearity and multicollinearity assessment approaches (Kock 2015; Petter et al. 2007). Overall, the results from these techniques support that CMB is not a significant issue for this study. The validity and reliability of the measurement model is tested through the evaluation of loadings or correlation weights, internal consistency, convergent validity, and discriminant validity (Hair et al. 2019). All the items reported a loading greater than 0.7. For internal consistency, the values of Cronbach's alpha and Composite Reliability (CR) should be between 0.7 and 0.95. The evaluation of these estimates revealed that all of the constructs were within acceptable thresholds. Convergent validity can be tested through the evaluation of Average Variance Extracted (AVE) values that should be above 0.5 for each composite (Hair et al. 2019). The assessment of AVE values indicated that all were above the cut-off value of 0.5. The discriminant validity of the constructs was examined by testing the HeteroTrait-MonoTrait (HTMT) criterion (Hair et al. 2017). For conceptually similar constructs, HTMT values greater than 0.9 suggest the lack of discriminant validity between the constructs. The HTMT value should be lower than the thresholds of 0.9 (Gold et al. 2001; Teo et al. 2008). $HTMT_{inference}$ yields specificity rates of 80% or higher in terms of inter-construct correlations as high as 0.95. In general, $HTMT_{.90}$ and $HTMT_{inference}$ approaches detect discriminant validity issues reliability (Henseler et al. 2015). In our study, based on the $HTMT_{.90}$ and $HTMT_{inference}$ criterion, the results show an acceptable level of discriminant validity for each pair of constructs.

5.2 Structural Model Assessment and Hypothesis Testing

The structural model evaluation includes assessing collinearity among the exogenous constructs, checking the significance and relevance of path coefficients, and examining the model's predictive accuracy and relevance model (Hair et al. 2019). To examine collinearity among the constructs, the Variance Inflation Factor (VIF) for each exogenous construct of the model was evaluated. While VIF values should not be greater than 5, values less than 3 are seen as ideal values (Hair et al. 2019). The assessment of VIF values indicated that all the values were less than 2.37, indicating no cause for concern with respect to collinearity issues. To determine the statistical significance of the path coefficients, we ran the bootstrapping routine at a 5% significance level with 10000 bootstrapping subsamples (Streukens and Leroi-Werelds 2016). To assess the second-order constructs, we followed steps for component-based model estimation by creating a new data file with the latent variable scores (two-stage approach) (Wright et al. 2012). The two-stage approach assesses the first-order constructs' scores during the first-stage then these scores are used as indicators for the second-order constructs in the second-stage (Duarte and Amaro 2018; Hair et al. 2011). The results of the structural model's evaluation are shown in Figure 2.

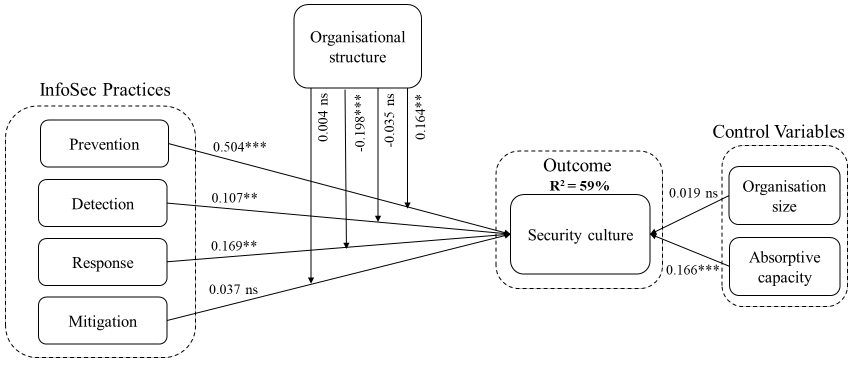

*Figure 2: Structural model results, **p<0.01, ***p<0.001 and ns = non-significant*

All hypotheses were supported except for three hypotheses: H1d on the positive association between mitigation practices and security culture (path coefficient (β) = 0.037, p = 0.531); H2b and H2d, which hypothesised positive moderation effects of organisational structure on the relationships between detection and mitigation practices, and security culture, were mot supported (β = -0.035, 0.004, p <0.05, respectively), were not supported. R^2 explains the variance of the endogenous constructs to assess the predictive power of the research model (Chin and Dibbern 2010; Duarte and Amaro 2018). The InfoSec practices explains 59% of the variances in security culture. Two control variables, organisation size and absorptive capacity, were also tested. Absorptive capacity had a positive significant relationship with the security culture variables (β = 0.166 *p* <0.001), indicating that organisations readiness to engage in InfoSec activities based on prior knowledge and resources would show a greater level of valuing the importance of information security in the organisations. Organisation size had no significant relationship with security culture. Moreover, none of the hypothesized paths changed their signs or the significance levels of any of the paths.

6 Discussion and Contributions

Under-developed security cultures leave organisations without the necessary framework for self-inspection and reflection. Despite prior academic and practitioners' attempts, it is still not clear how security cultures are formed and what the key drivers of them are. Toward addressing this research gap, we leveraged HRT to develop and test a research model that explores how practical efficiencies shape security culture in organisations, and the role of supportive proficiencies like organisational structure in this process. Test results show that some practical proficiencies namely protection, detection and response inform the security culture. Security culture is most influenced by the InfoSec prevention practices. This suggests that InfoSec practices, with an emphasis on fostering organisational capability to protect information assets from unexpected InfoSec incidents or nurturing organisational strategies to be activated before an InfoSec breach happens, have a substantial role in helping InfoSec to become part of the norms and values in an organisation.

The findings of our research also underscore that ensuring the alignment between security functions and business strategies facilitates the effective implementation and coordination of protection practices. However, it depicts a reverse influence on the response practices. This may indicate that more pressure from organisational structure may alleviate the organisations' agility in the preparation for practices that need to be designed for unexpected and unpredictable risks to promote organisational security culture. Future research should identify additional practical and supportive proficiencies to better explain InfoSec practices in organisations. The findings of our research also highlight the difficulties in enforcing InfoSec practices through organisational structure in the organisations. This may indicate that although organisational structure plays a critical role in implementation of InfoSec practices in the organizations but does not play a significant role in improving the detection and mitigation practices alignment with security culture. The fact that organisational structure was not found to moderate the relationship between detection and mitigation practices and security culture may suggest that organisational structure either do not play a part in helping align their detection and response InfoSec practices with its security culture or are simply ineffective in doing so. Either way, this is an important outcome in that this form of strategic guidance is typically what the literature suggests is expected of top managers. Given the relative lack of InfoSec research at the organizational level, our study provides some needed insight that can help academics and practitioners to understand how firm-level security-related outcomes are formed due to both supportive and practical dynamics. Many previous studies have investigated the behavioural side of InfoSec to evaluate which organizational, and managerial factors influence effective InfoSec management practices. While individual-level studies have increased the understanding of employee InfoSec compliance and misuse behaviours, they have not paid as much attention to investigating the effects of organizational factors on security outcomes.

7 Conclusions, Limitations and Future Research

In this study, we explored the role of practical proficiencies in forming security culture in organisations. We also examined the role of supportive proficiencies, such as organisational structure on InfoSec practices namely prevention, detection, response and mitigation. The results of this study provide strong support for the influence of prevention, detection and response practices on security culture.

The results of this study should be viewed in the light of its limitations. First, the cross-sectional design of the data collection method using a single point in time may limit the implications of the results. This

is because cross-sectional data does not capture organisational processes and changes and may not be suitable for establishing causal relationships. Second, organisational structure did not improve the impact of InfoSec practices on security culture. Future research should take a closer look into the reasons for this lack of significant moderating influence and may explore other organisational supportive proficiencies to better explain the reinforcement between InfoSec practice and security culture in organisations.

8 References

Åhlfeldt, R.-M., Spagnoletti, P., and Sindre, G. 2007. "Improving the Information Security Model by Using Tfi," *IFIP International Information Security Conference*: Springer, pp. 73-84.

Ahmad, A., Maynard, S. B., and Park, S. 2014. "Information Security Strategies: Towards an Organizational Multi-Strategy Perspective," *Journal of Intelligent Manufacturing* (25:2), pp. 357-370.

Antunes, J., Neves, N., Correia, M., Verissimo, P., and Neves, R. 2010. "Vulnerability Discovery with Attack Injection," *IEEE Transactions on Software Engineering* (36:3), pp. 357-370.

Ashenden, D., and Sasse, A. 2013. "Cisos and Organisational Culture: Their Own Worst Enemy?," *Computers & Security* (39), pp. 396-405.

Barton, K. A., Tejay, G., Lane, M., and Terrell, S. 2016. "Information System Security Commitment: A Study of External Influences on Senior Management," *Computers & Security* (59), pp. 9-25.

Baskerville, R. 1988. *Designing Information Systems Security*. John Wiley & Sons, Inc.

Baskerville, R., Spagnoletti, P., and Kim, J. 2014. "Incident-Centered Information Security: Managing a Strategic Balance between Prevention and Response," *Information & Management* (51:1), pp. 138-151.

Boin, A., and Schulman, P. 2008. "Assessing Nasa's Safety Culture: The Limits and Possibilities of High-Reliability Theory," *Public Administration Review* (68:6), pp. 1050-1062.

Brand, K., and Boonen, H. 2007. *It Governance Based on Cobit® 4.1-a Management Guide*. Van Haren.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), pp. 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), pp. 14-27.

Chen, Y., Ramamurthy, K., and Wen, K.-W. 2015. "Impacts of Comprehensive Information Security Programs on Information Security Culture," *Journal of Computer Information Systems* (55:3), pp. 11-19.

Child, J. 1984. *Organization: A Guide to Problems and Practice*. Sage.

Chin, W. W., and 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*. Springer, pp. 171-193.

Da Veiga, A. 2018. "An Approach to Information Security Culture Change Combining Adkar and the Isca Questionnaire to Aid Transition to the Desired Culture," *Information & Computer Security*).

Da Veiga, A., and Eloff, J. H. 2010. "A Framework and Assessment Instrument for Information Security Culture," *Computers & Security* (29:2), pp. 196-207.

Da Veiga, A., and Martins, N. 2015. "Improving the Information Security Culture through Monitoring and Implementation Actions Illustrated through a Case Study," *Computers & Security* (49), pp. 162-176.

Dhillon, G., and Backhouse, J. 2001. "Current Directions in Is Security Research: Towards Socio-Organizational Perspectives," *Information systems journal* (11:2), pp. 127-153.

Dhillon, G., Syed, R., and Pedron, C. 2016. "Interpreting Information Security Culture: An Organizational Transformation Case Study," *Computers & Security* (56), pp. 63-69.

Duarte, P., and Amaro, S. 2018. "Methods for Modelling Reflective-Formative Second Order Constructs in Pls," *Journal of Hospitality and Tourism Technology* (9:3), pp. 259-313.

Friedberg, I., Skopik, F., Settanni, G., and Fiedler, R. 2015. "Combating Advanced Persistent Threats: From Network Event Correlation to Incident Detection," *Computers & Security* (48), pp. 35-57.

Furnell, S., and Thomson, K.-L. 2009. "From Culture to Disobedience: Recognising the Varying User Acceptance of It Security," *Computer fraud & security* (2009:2), pp. 5-10.

Gold, A. H., Malhotra, A., and Segars, A. H. 2001. "Knowledge Management: An Organizational Capabilities Perspective," *Journal of Management Information Systems* (18:1), pp. 185-214.

Grabowski, M., and Roberts, K. 1997. "Risk Mitigation in Large-Scale Systems: Lessons from High Reliability Organizations," *California Management Review* (39:4), pp. 152-161.

Hair, J. F., Ringle, C. M., and Sarstedt, M. 2011. "Pls-Sem: Indeed a Silver Bullet," *Journal of Marketing theory and Practice* (19:2), pp. 139-152.

Hair, J. F., Risher, J. J., Sarstedt, M., and Ringle, C. M. 2019. "When to Use and How to Report the Results of Pls-Sem," *European Business Review* (31:1), pp. 2-24.

Hair, J. F., Sarstedt, M., Ringle, C. M., and Gudergan, S. P. 2017. *Advanced Issues in Partial Least Squares Structural Equation Modeling*. saGe publications.

Hamill, J. T., Deckro, R. F., and Kloeber Jr, J. M. 2005. "Evaluating Information Assurance Strategies," *Decision Support Systems* (39:3), pp. 463-484.

Harman, H. H. 1976. *Modern Factor Analysis*. University of Chicago press.

Henauer, M. 2003. "Early Warning and Information Sharing," *Workshop on cyber security and contingency planning: threats and infrastructure protection, Zurich, Switzerland*, pp. 55-62.

Henseler, J., Ringle, C. M., and 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), pp. 115-135.

Kayworth, T., and Whitten, D. 2010. "Effective Information Security Requires a Balance of Social and Technology Factors," *MIS Quarterly Executive* (9:3), pp. 2012-2052.

Kock, N. 2015. "Common Method Bias in Pls-Sem: A Full Collinearity Assessment Approach," *International Journal of e-Collaboration* (11:4), pp. 1-10.

Kraemer, S., and Carayon, P. 2007. "Human Errors and Violations in Computer and Information Security: The Viewpoint of Network Administrators and Security Specialists," *Applied Ergonomics* (38:2), pp. 143-154.

Lindell, M. K., and Whitney, D. J. 2001. "Accounting for Common Method Variance in Cross-Sectional Research Designs," *Journal of Applied Psychology* (86:1), p. 114.

Liu, S., Sullivan, J., and Ormaner, J. 2001. "A Practical Approach to Enterprise It Security," *IT Professional* (3:5), pp. 35-42.

Lu, G., Koufteros, X., and 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), pp. 234-248.

Lu, G., Koufteros, X., Talluri, S., and Hult, G. T. M. 2019. "Deployment of Supply Chain Security Practices: Antecedents and Consequences," *Decision Sciences* (50:3), pp. 459-497.

MacKenzie, S. B., Podsakoff, P. M., and Podsakoff, N. P. 2011. "Construct Measurement and Validation Procedures in Mis and Behavioral Research: Integrating New and Existing Techniques," *MIS Quarterly* (35:2), pp. 293-334.

Martins, A., and Elofe, J. 2002. "Information Security Culture," in *Security in the Information Society*. Springer, pp. 203-214.

Montesdioca, G. P. Z., and Maçada, A. C. G. 2015. "Measuring User Satisfaction with Information Security Practices," *Computers & Security* (48), pp. 267-280.

Morone, J. G., and Woodhouse, E. J. 1986. "Averting Catastrophe: Strategies for Regulating Risky Technologies,").

Nel, F., and Drevin, L. 2019. "Key Elements of an Information Security Culture in Organisations," *Information & Computer Security* (27:2), pp. 146-164.

O'Brien, J., Islam, S., Bao, S., Weng, F., Xiong, W., and Ma, A. 2013. "Information Security Culture: Literature Review," *Unpublished Working Paper, University of Melbourne*).

Perrow, C. 1994. "The Limits of Safety: The Enhancement of a Theory of Accidents," *Journal of Contingencies and Crisis Management* (2:4), pp. 212-220.

Petter, S., Straub, D., and Rai, A. 2007. "Specifying Formative Constructs in Information Systems Research," *MIS Quarterly* (31:4), pp. 623-656.

Pfleeger, C., Pfleeger, S. L., and Jonathan, M. 2015. *Security in Computing*, (5th ed.). Upper Saddle River, NJ: Prentice-Hall.

Porte, T. L., and 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), pp. 847-852.

Rijpma, J. A. 1997. "Complexity, Tight–Coupling and Reliability: Connecting Normal Accidents Theory and High Reliability Theory," *Journal of Contingencies and Crisis Management* (5:1), pp. 15-23.

Roberts, K. H. 1990a. "Managing High Reliability Organizations," *California Management Review* (32:4), pp. 101-113.

Roberts, K. H. 1990b. "Some Characteristics of One Type of High Reliability Organization," *Organization Science* (1:2), pp. 160-176.

Roberts, K. H., Rousseau, D. M., and 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), pp. 141-161.

Rocha Flores, W., Antonsen, E., and Ekstedt, M. 2014. "Information Security Knowledge Sharing in Organizations: Investigating the Effect of Behavioral Information Security Governance and National Culture," *Computers & Security* (43), pp. 90-110.

Ruighaver, A. B., Maynard, S. B., and Chang, S. 2007. "Organisational Security Culture: Extending the End-User Perspective," *Computers & security* (26:1), pp. 56-62.

Sagan, S. D. 1995. *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons*. Princeton University Press.
Saydjari, O. S. 2004. "Cyber Defense: Art to Science," *Communications of the ACM* (47:3), pp. 52-57.
Sheffi, Y. 2005. "The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage," *MIT Press Books* (1).
Siponen, M., Pahnila, S., and Mahmood, A. 2007. "Employees' Adherence to Information Security Policies: An Empirical Study," *IFIP International Information Security Conference*: Springer, pp. 133-144.
Speier, C., Whipple, J. M., Closs, D. J., and Voss, M. D. 2011. "Global Supply Chain Design Considerations: Mitigating Product Safety and Security Risks," *Journal of Operations Management* (29:7-8), pp. 721-736.
Streukens, S., and 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), pp. 618-632.
Stytz, M. R. 2004. "Considering Defense in Depth for Software Applications," *IEEE Security & Privacy* (2:1), pp. 72-75.
Teo, T. S., Srivastava, S. C., and Jiang, L. 2008. "Trust and Electronic Government Success: An Empirical Study," *Journal of Management Information Systems* (25:3), pp. 99-132.
Thomson, K.-L., Von Solms, R., and Louw, L. 2006. "Cultivating an Organizational Information Security Culture," *Computer Fraud & Security* (2006:10), pp. 7-11.
Tomlin, B. 2006. "On the Value of Mitigation and Contingency Strategies for Managing Supply Chain Disruption Risks," *Management Science* (52:5), pp. 639-657.
Van Niekerk, J., and Von Solms, R. 2010. "Information Security Culture: A Management Perspective," *Computers & Security* (29:4), pp. 476-486.
Von Solms, B., and Von Solms, R. 2004. "The 10 Deadly Sins of Information Security Management," *Computers & Security* (23:5), pp. 371-376.
Warkentin, M., and Johnston, A. C. 2008. "It Governance and Organizational Design for Security Management," in *Information Security: Policies, Processes, and Practices,* D.W. Straub, S.E. Goodman and R. Baskerville (eds.). New York: Advances in Management Information Systems, pp. 46-68.
Warkentin, M., Johnston, A. C., Shropshire, J., and Barnett, W. D. 2016. "Continuance of Protective Security Behavior: A Longitudinal Study," *Decision Support Systems* (92), pp. 25-35.
Weick, K. E. 1987. "Organizational Culture as a Source of High Reliability," *California Management Review* (29:2), pp. 112-127.
Weick, K. E., and Sutcliffe, K. M. 2001. "Managing the Unexpected: Assuring High Performance in an Age of Complexity." San Francisco, CA: Jossey Bass Publishers.
Wildavsky, A. B. 1988. *Searching for Safety*. Transaction publishers.
Wolf, F. 2005. "Resource Availability, Commitment and Environmental Reliability & Safety: A Study of Petroleum Refineries," *Journal of Contingencies and Crisis Management* (13:1), pp. 2-11.
Wright, R. T., Campbell, D. E., Thatcher, J. B., and Roberts, N. 2012. "Operationalizing Multidimensional Constructs in Structural Equation Modeling: Recommendations for Is Research," *Communications of the Association for Information Systems* (30:1), p. 23.
Zakaria, O., and Gani, A. 2003. "A Conceptual Checklist of Information Security Culture," *2nd European Conference on Information Warfare and Security, Reading, UK*.
Zalenski, R. 2002. "Firewall Technologies," *IEEE Potentials* (21:1), pp. 24-29.

Appendix A. The Conceptual Definition of Constructs and Measurement Items

Dimension	**Definition**
Organizational structure	"The degree to which organizational structures is implemented in the organization to support governance of information security." (Rocha Flores et al. 2014 p.97). *Formal organizational structure* • We have an organizational unit with explicit responsibility for organising and coordinating information security efforts as well as handling incidents. *Coordinating organizational structure* • There is a committee, comprised of representatives from various business units, which coordinates corporate security initiatives. • There is a committee, which deals with matters of strategic information security and related decision-making. • Tactical and operative managers are involved in information security decision-making, which is related to their unit, responsibilities and/or subordinates. • In our organization, people responsible for security and representatives from various business units meet to discuss important security issues both formally and informally.
Prevention	Refers to protecting information assets and IS prior to an incident by prohibiting unauthorized access, destruction, or disclosure, and ensuring their availability, confidentiality, and integrity (Ahmad et al. 2014; Hamill et al. 2005; Liu et al. 2001). • Our security risk management strategy can be characterised as proactive.

	• When it comes to security, our strategy focuses on prevention. • We hold all third-parties accountable for security. • We only approve third-parties/partners (irrespective of tier) that have a security risk management programme in place. • We educate employees about security practices. • We have a process that notifies partners across tiers if the security is threatened.
Detection	Includes measures to detect any impending or continuing attack against information or an IS (Hamill et al. 2005), which allows the organization to react in a targeted manner (Ahmad et al. 2014). • We use active measures such as video and sensors to be able to detect security breaches. • We use sophisticated technologies to detect if security have been compromised. • We monitor and synthesise information regarding security breaches. • We do conduct periodic assessments of our security policies, procedures. • We have procedures to detect security failures or near failures.
Response	"Refers to such principles and practices in organizations that are intended to react to information security incidents that have happened (or are happening)." (Baskerville et al. 2014 p. 139). • We know what to do when we encounter security breaches or crises. • We have designated a group of employees as first respondents in case of a crisis. • There is a definite chain of command in case of a security emergency. • We have protocols for communication when a crisis arises. • We have a well-defined contingency plan to react to serious security breaches. • We do have a disaster recovery plan. • We have a specific process to reinstate operations in case of a major crisis/disruption. • We have strategies for recovery action after disruptions.
Mitigation	Those practices in which the organization takes some actions in advance of a disruption to reduce losses by lessening the impact of InfoSec breaches. (Lu et al. 2017; Tomlin 2006). • We cross-train our employees as a mechanism to deal with potential disruptions. • We have backup processes that can assist us at times of crises. • We have strategies to use more standard parts to reduce the risk of disruptions. • We developed alternative material sources in case of disruptions. • We simplified jobs to the extent that unskilled employee can perform a variety of them in case of a crisis.
Security culture	Defined as a way of doing tasks around InfoSec, including creating an environment that encourages and develops shared security attitudes, values, beliefs, and norms in an organization (Van Niekerk and Von Solms 2010). • Employees value the importance of security of information and computer systems. • In my organization, a culture exists that promotes good security and privacy practices. • Security (of information and systems) has traditionally been considered an important organizational value. • Practicing good security of information and systems is the accepted way of doing business in my organization. • The overall environment in my organization fosters security-minded thinking in all our actions. • Information and systems security is a key norm shared by all organizational members/employees.

Copyright