# TOWARD THE DEVELOPMENT OF A SECURITY CULTURE MODEL: A KEY PROFICIENCIES PERSPECTIVE

## Title Page Information

Corresponding author (1): Dr Farkhondeh Hassandoust

Given name: Farkhondeh

Family name: Hassandoust

e-mail: ferry@aut.ac.nz

Affiliation: Auckland University of Technology

Address: 55 Wellesley St E, Auckland, 1010, New Zealand

Author (2): Associate Prof Dr Allen C. Johnston

Given name: Allen

Family name: Johnston

e-mail: ajohnston@cba.ua.edu

Affiliation: Culverhouse College of Business, The University of Alabama

Address: Tuscaloosa, Alabama, 35487, United States

## ABSTRACT

In this research in progress (RIP), we draw on high reliability theory to develop a Security Culture Model that explains how a firm's supportive and practical proficiencies form its organizational security culture. We present initial tests of the model using survey data from 602 professional managers in Australia and New Zealand who are aware of the information security (InfoSec) programs within their respective organizations, 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 emphasize the importance of organizational supportive proficiencies as organizational structure for developing InfoSec practices in a firm. The results of this study provide both academics and practitioners an understanding of the vital organizational dynamics necessary to establish a culture of security.



**Keywords:** Security culture, information security practices, organizational structure, high reliability theory

# TOWARD THE DEVELOMENT OF A SECRITY CULTURE MODEL: A KEY PROFICIENCIES PERSPECTIVE

## INTRODUCTION

The security culture of an organization encompasses the values and beliefs of the firm that direct the security-related behaviors 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 organization 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 organization'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 organization, how the organization will respond to this threat is influenced by its security culture.

For many organizations, 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 (Adkins et al. 2020; Da Veiga et al. 2020; 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 organization are either inactive or ineffective, and how employees communicate and respond to others and to formal and informal organizational forces is unpredictable and unreliable. Moreover, under-developed security cultures leave organizations 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 et al. 2020; 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 organization that direct its employee behaviors and establish the norms of the organization. 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 organizational 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 organizations, these proficiencies emerge organically as the organizations 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 organization 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 organizational theory focused on the firm-level proficiencies that lead to the development of cultural outcomes, High Reliability Theory (HRT). HRT associates an organization'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 organization 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 Security Culture Model that explains a security culture as a product of an organization'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 explain the theory contextualization process we followed to arrive at and test a Security Culture Model. We then conclude with a discussion of its implications to research and practice.

## LITERATURE REVIEW

Security culture as an organizational 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 organizational culture (Dhillon and Backhouse 2001) and should include all socio-cultural countermeasures that support technical security measures (Chen et al. 2015). Further, cultivating a security-aware culture mitigates the privacy and security risks to information assets and IS within organizations (Da Veiga et al. 2020; Da Veiga and Eloff 2010; Nel and Drevin 2019).

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

organizations must emphasize 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). Employees should be equipped with security awareness and training programs to ensure their compliance with InfoSec policy regulations (AlHogail and Mirza 2014; Bulgurcu et al. 2010). InfoSec protection should be a natural part of employees' daily tasks; that is, InfoSec should be integrated into the corporate culture and employees' InfoSec behaviors 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 organizational cultural and behavioral 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 organization that facilitate its culture of security. Moreover, there is a lack of theoretical foundations to support the process of establishing a security culture. For the studies that have made this attempt, they are summarized in the Appendix A.

## THEORIZING A SECURITY CULTURE MODEL

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.

### *High Reliability Theory*

HRT concentrates on the processes that an organization can implement to ensure continued organizational 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 organizations, 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 organizations (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 decentralized and continually practiced operations; and 4) advanced types of trial and error organizational learning. Organizational 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 decentralized bases, compliance happens without surveillance (Weick 1987).

Much of HRT research has focused on specific organizations 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 organizations 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 organizational practice perspective with a focus on the protection mechanisms that organizations can put in place to best react to organizational (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 organizational reliability creates a meaningful lens to assess InfoSec practices within organizations. InfoSec practices can be implemented to assure continued organizational reliability (Speier et al. 2011). Having protective and responsive strategies, practices, and personnel in place can enable the organizations 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 organizations' security procedures should be designed in a way that prevents these intentional actions that can compromise confidential information.

### *HRT Contextualization*

Because HRT is a general theory of organizations that operate in complex and hazardous domains that originated in the health and safety literature, in order to theorize a Security Culture Model, we must engage in a careful contextualization of the theory (Hong et al. 2014). Through contextualization, we are able to present a model that is well aligned with the practical and supportive proficiencies of an organization that promote such a culture – a culture in which the organizational beliefs and values for effective, secure practices are shared by employees throughout the organization (Van Niekerk and Von Solms 2010) and in which employees are assets for security, rather than vulnerabilities (Ruighaver et al. 2007).

As a first step in the process of contextualizing HRT, we can establish an initial research model and hypotheses that reflect HRT in the context of an organizational security culture. This model is presented 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 organizational mechanisms that produce reliable outcomes, such as a security culture.

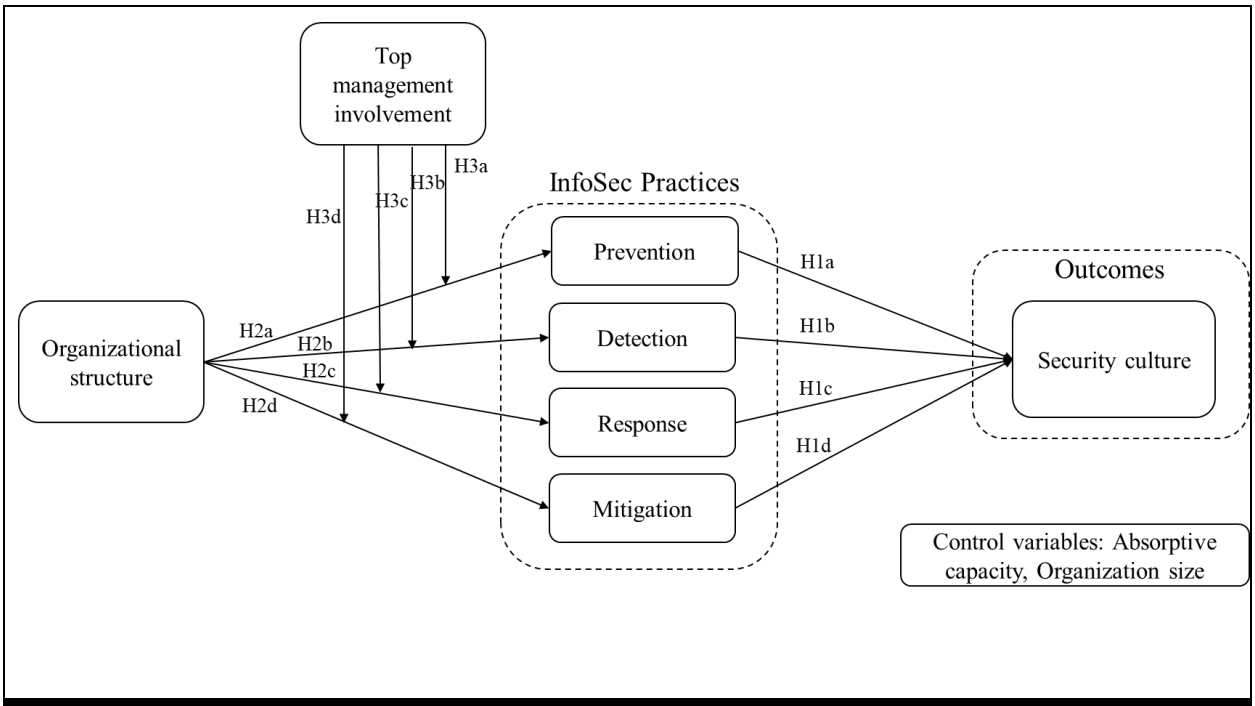


**Figure 1. Security Culture Model**

*Practical Proficiencies*

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 organization. There are a number of broadly recognized InfoSec management frameworks available to instruct organizations 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, organizations face the need to detect new InfoSec threats and new forms of attacks (Antunes et al. 2010). Therefore, organizations require a more response-oriented InfoSec philosophy (validity and exploration) in addition to the existing preventive frameworks.

Having security practices and policies in place helps in forming deeper thoughts and perceptions on information security, which in turn, promotes organizational cultural values on security (Chen et al. 2015). Organizational InfoSec practices are a set of procedures and activities designed to protect the integrity, availability and confidentiality of organizational information assets that include IS (Burns 2019). Effective security policies and the enforcement of the security operations are different in fundamental ways between the two prevention and recovery paradigms (Baskerville et al. 2014). InfoSec practices should be developed in a way that strategically balance security operations across both paradigms (Baskerville et al. 2014). 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). 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).

*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* is an operational-level practice that aims in identifying specific InfoSec behavior such as intrusion and misuse behaviors (Hamill et al. 2005). 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 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, defensive practices should be agile and designed for unexpected and unpredictable risks by promptly adopting customized safeguards (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 that are designed to reinforce response practices aimed at reducing losses by lessening the impact of InfoSec breaches (Sheffi 2005). Mitigation practices boost the ability of organizations 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, organizations may take various approaches such as cross-training employees in InfoSec measures to enable even unskilled employees to perform these measures. If or when an organization 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). Mitigation practices are designed to be activated before an InfoSec breach occurs (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 organizational reliability (Speier et al. 2011). Having protective and responsive strategies, practices, and personnel in place can enable organizations to respond to InfoSec incidents more effectively (Lu et al. 2017). 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, organizations 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 organization. These practices can

be designed with different emphases – either to foster organizational capability to discover (i.e., detect and prevent) unexpected InfoSec incidents or to nurture organizational 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 organization.*

*Supportive Proficiencies*

In the conceptual model, the InfoSec practices are, themselves, influenced by the structure of the organization, a key supportive proficiency. An organizational 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 organizational boundaries" (Child 1984 p. 2). The importance of organizational structures has been discussed for a long period of time. For example, Child has argued the essential role of organizational structure in designing an effective organization (Child 1984). Organizational 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, organizational structure determines and facilitates operational and strategic decision making and monitors the performance and operating mechanisms that transfer instructions on what is expected of organizational employees and how the instructions should be followed (Child 1984). Flexible organizational 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 organization to be able to effectively respond to events in their environment (Grabowski and Roberts 1997). Flexible organizational structures also empower employees to

enact choices that reinforce the organizational culture, which in turn, would change the tempo and nature of organizations in response to internal and external events and changes (Grabowski and Roberts 1997).

Organizational structure plays a key role in making an InfoSec governance plan successful (Von Solms and Von Solms 2004). In an InfoSec context, organizational structure is defined as the organization of InfoSec functions (Kraemer and Carayon 2007) and refers to the formal and informal structures that expresses the organizational 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 organizational structure as either a formal organizational structure or a coordinating structure (see Figure 1). Formal organizational structure refers to the formalized structures that are implemented to support the management of InfoSec matters within an organization (Rocha Flores et al. 2014).

According to (Kayworth and Whitten 2010), formal organizational structures may include having a formal InfoSec unit within the organization whose mission is to secure the organization's information assets. The purpose of this unit is to develop and implement the organization's standards and practices governing organization-wide InfoSec. Further, in the formal organizational structures, there are InfoSec executives (i.e., security top manager) with leadership responsibility over InfoSec functions to facilitate strategic alignment between security and business goals. Formal organizational structures may also include a formal unit as an internal audit function that conducts assessment of InfoSec controls and practices and reports the results to top management.

Coordinating organizational structures refer to formal and informal meetings among a group of people responsible for InfoSec tasks and representatives from various business units in the organization to facilitate the communication of strategic business plans between business and InfoSec functions (Kayworth and Whitten 2010; Rocha Flores et al. 2014). Coordinating organizational structures consist of InfoSec steering committees and liaisons to represent the organization's InfoSec function, assisting business units in InfoSec risk assessments, and providing security advice in line with the organization's security policies (Kayworth and Whitten 2010). Through this structure, the InfoSec function gains valuable insights from the business to facilitate strategic decision making and security pressures are communicated with business managers through this channel.

As a key supportive proficiency of an organization, an organizational structure ensures the alignment between the organization's security functions and business strategies, facilitates the effective organization 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, organizational structure is manifested through the two forms of structure: 1) a formalized structure which refers to a centralized InfoSec function and supports the development and positioning of uniform organization-wide security practices. A formalized structure also supports the handling of InfoSec matters throughout the organization (Rocha Flores et al. 2014) and 2) a coordinating structure which refers to the utilization of a variety of coordinating InfoSec committees and groups that meet to discuss important InfoSec issues both formally and informally. To more thoroughly understand the positive impact of organizational structure as a

supportive proficiency for the development of a security culture, the following hypotheses are postulated:

*H2(a-d): Organizational structure is positively associated with the InfoSec practices of an organization, namely prevention (a), detection (b), response (c), and mitigation (d).*

Top management involvement is another key supportive proficiency of an organization and is considered a moderator of the relationships between its organizational structure and InfoSec practices. Involvement refers to top management's psychological state and the degree of importance management places on a specific concern (i.e., InfoSec) (Jarvenpaa and Ives 1991). Although top management belief, participation, and involvement contribute to greater InfoSec achievement in an organization, involvement is the more effective way of support (Barton et al. 2016). Top management commitment to InfoSec can lead to organizational change that mitigates security risks in the organization (Barton et al. 2016). Top management specifies which issues are an organization's strategic issues, and as a result, which issues receive the organizational 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). The design of InfoSec practices is related to top management commitment (Barton et al. 2016; Knapp et al. 2006) and organizational structure within an organization (Rocha Flores and Ekstedt 2016). Without top management involvement, the organizational structure will not be able to effectively enforce an organization's InfoSec policies or be taken seriously by employees (Knapp et al. 2006). Top management support is necessary in order to effectively handle InfoSec issues. Without top management involvement, even a robust structure with comprehensive InfoSec practices will not guarantee InfoSec enforcement across the organization (Knapp et al. 2006).

Top management involvement is critical in InfoSec practices whereby an organization's goals and structures are defined in relation to InfoSec (Singh et al. 2014). Moreover, top management support in line with organizational structure, in terms of staff responsibility and allocation, financial funding, and political backing, 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 have ever happened; and resilience that entails efforts to deal with (i.e., respond and mitigate InfoSec) incidents once they become manifest [27, 28]. Therefore, in HROs, top management support is required to assist in the development and implementation of organization-wide InfoSec practices (i.e., formal structure) and in the utilization of various coordinating InfoSec committees (i.e., informal structure) to better implement InfoSec procedures. The aim is to avoid InfoSec breaches, or to detect an attack and promptly report it to the InfoSec managers, or to take appropriate corrective actions against identified attacks, or to reduce losses by lessening the impact of InfoSec breaches. Therefore, we hypothesize the following:

*H3(a-d): A firm's top management involvement positively moderates the impact of its organizational structure on InfoSec practices, namely prevention (a), detection (b), response (c), and mitigation (d).*

At this stage in the process of contextualizing HRT to form a Security Culture Model, we have an initial research model, complete with a core set of practical and supportive proficiencies and associated hypotheses. The next steps in the theorizing process (Hong et al. 2014) are for us to

test this initial model and its associated hypotheses. Based on these results, we will then thoroughly evaluate the context of an organizational security culture to identify additional practical and supportive proficiencies, revise the model to include those factors, consider the interaction of those factors with initial core elements of the model, and then ultimately test the revised model and any alternative models that may improve its explanatory efficacy. Toward achieving these theorizing steps, we plan to conduct a mixed, multi-study research design.

## RESEARCH DESIGN

The first study (Study 1) in this multi-study design is exploratory and serves to provide some initial feedback on the theorized Security Culture Model presented in Figure 1. This is the study presented in this RIP. A subsequent study (Study 2) will be conducted to further refine and test the initial Security Culture Model. That study is currently in progress.

### *Study 1*

The initial, exploratory assessment of the Security Culture Model was conducted via a survey of 602 AUS and NZ security professionals, 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 (Lu et al. 2017). For organizational structure, we adopted items from Rocha Flores and colleagues (Rocha Flores et al. 2014). The six items measuring security culture were adopted from Chen et al (Chen et al. 2015). For top management involvement, we adopted items from Liang and colleagues (Liang et al. 2007). 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 organizational structure that considered as a formative second-order construct with two reflective first-order factors including formal structure and coordinating structure. The measurement items are presented in Appendix B.

The demographic description of the sample is provided in Table 1. In terms of organizational roles, majority of participants were chief executive officers (38.7%). Almost half of the companies (47.9%) were in small size with 1-19 employees, majority had been located in Australia (70.7%) and most of them were in business for more than five years (64.5%).

**Table 1. Demographic Information of Participants - Study 1**

| ***Demographic Information*** | | ***Frequency*** | ***Percentage*** |
|---|---|---|---|
| Roles | Chief Executive Officer | 216 | 35.9% |
| | Chief Information Officer | 106 | 17.6% |
| | Chief Information Security Officer | 26 | 4.3% |
| | A senior manager in the IT department | 93 | 15.4% |
| | A senior manager in the Security department | 33 | 5.5% |
| | Owner | 49 | 8.1% |
| | No management position | 30 | 5% |
| | Others (e.g., compliance manager, credit performance manager, managing director, technical team leader, privacy officer, operation manager) | 49 | 8.1% |
| Company size (number of employees) | 1 - 19 | 250 | 41.5% |
| | 20 - 199 | 205 | 34.1% |
| | Over 200 | 147 | 24.4% |
| Organization location | Australia | 426 | 70.7% |
| | New Zealand | 176 | 29.3% |
| Organization in business | Less than a year | 34 | 5.6% |
| | 1 - 4 years | 183 | 30.4% |
| | More than 5 years | 385 | 64% |
| Industry type | Agriculture | 29 | 4.8% |
| | Manufacturing | 60 | 10% |
| | Financial Services | 72 | 12% |

| | | | |
|---|---|---|---|
| | Mass media | 18 | 3% |
| | Insurance | 12 | 2% |
| | Health care | 38 | 6.3% |
| | Hospitality | 26 | 4.3% |
| | Electronics | 43 | 7.1% |
| | Music/Film | 17 | 2.8% |
| | Education | 35 | 5.8% |
| | Pharmaceutical | 4 | 0.7% |
| | Telecommunication | 29 | 4.8% |
| | Construction | 47 | 7.8% |
| | Services | 113 | 18.8% |
| | Retail | 28 | 4.7% |
| | Others (e.g., accounting, architecture, arts, automotive, defence, government, non for profit, and human resources) | 31 | 5.1% |

*Data Analysis and Results of Study 1*

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 behaviors (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) as well as exploratory research (Gefen et al. 2011). This study is an exploratory research and uses a model with formative construct (organizational structure), therefore PLS is a suitable tool for this study.

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 are presented in Appendix C. Overall, the results from these techniques support that CMB is not a significant issue for this study.

*Measurement Model Assessment of Study 1*

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). According to Hair and colleagues (Hair et al. 2019), the loading should be greater than 0.708 to test if a construct explains more than 50 percent of the item's variance. Non-contributing items should be removed from the measurement model. 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, as shown in Table 2.

**Table 2. Convergent Validity Testing - Study 1**

| ***Construct*** | ***Item*** | ***Std. loading of each item*** | ***Cronbach's Alpha (α)*** | ***Composite Reliability (CR)*** | ***Average Variance Extracted (AVE)*** |
|---|---|---|---|---|---|
| Absorptive capacity | ABSC1 | 0.718 | 0.756 | 0.845 | 0.578 |
| | ABSC2 | 0.722 | | | |
| | ABSC3 | 0.802 | | | |
| | ABSC4 | 0.794 | | | |
| Detection | DET1 | 0.793 | 0.873 | 0.908 | 0.663 |
| | DET2 | 0.819 | | | |
| | DET3 | 0.836 | | | |
| | DET4 | 0.805 | | | |
| | DET5 | 0.817 | | | |
| Prevention | PREV1 | 0.705 | 0.843 | 0.885 | 0.561 |
| | PREV2 | 0.731 | | | |
| | PREV3 | 0.717 | | | |
| | PREV4 | 0.771 | | | |
| | PREV5 | 0.787 | | | |
| | PREV6 | 0.780 | | | |
| Response | RESP1 | 0.703 | 0.907 | 0.925 | 0.607 |
| | RESP2 | 0.794 | | | |
| | RESP3 | 0.778 | | | |
| | RESP4 | 0.824 | | | |
| | RESP5 | 0.832 | | | |

| | | | | | |
|---|---|---|---|---|---|
| | RESP6 | 0.812 | | | |
| | RESP7 | 0.753 | | | |
| | RESP8 | 0.727 | | | |
| Mitigation | MITG1 | 0.804 | 0.858 | 0.898 | 0.638 |
| | MITG2 | 0.768 | | | |
| | MITG3 | 0.845 | | | |
| | MITG4 | 0.813 | | | |
| | MITG5 | 0.760 | | | |
| Top management involvement | TOPP1 | 0.874 | 0.851 | 0.910 | 0.771 |
| | TOPP2 | 0.897 | | | |
| | TOPP3 | 0.863 | | | |
| Organizational structure - Formal | FSTR1 | 1.000 | 1.000 | 1.000 | 1.000 |
| Organizational structure - Coordinating | COSTR1 | 0.829 | 0.855 | 0.902 | 0.697 |
| | COSTR2 | 0.814 | | | |
| | COSTR3 | 0.857 | | | |
| | COSTR4 | 0.840 | | | |
| Security culture | SECU1 | 0.775 | 0.886 | 0.913 | 0.637 |
| | SECU2 | 0.821 | | | |
| | SECU3 | 0.785 | | | |
| | SECU4 | 0.804 | | | |
| | SECU5 | 0.801 | | | |
| | SECU6 | 0.804 | | | |

For a formative higher-order construct, the weights of the lower-order constructs represent actionable drivers of the higher-order construct (Becker et al. 2012; Duarte and Amaro 2018). The weights of the first-order constructs (formal structure and coordinating structure) on the second-order construct (organizational structure) and their significance are examined (see Table 3).

**Table 3. Indicator Reliability for Formative Construct (organizational structure) – Study 1**

| | ***Indicator weights*** | ***VIF*** | ***t-statistics*** |
|---|---|---|---|
| Formal structure | 0.238* | 1.493 | 2.015 |
| Coordinating structure | 0.914*** | 1.482 | 4.497 |
| Note: *p<0.05 and ***p<0.001 | | | |

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. Table 4 presents the values of the $HTMT_{.90}$ criterion for discriminant validity of the constructs.

**Table 4. HTMT Values for Discriminant Validity – Study 1**

| | Coordinating structure | Detection | Formal structure | Mitigation | Prevention | Response | Security culture |
|---|---|---|---|---|---|---|---|
| Detection | 0.140 | | | | | | |
| Formal structure | 0.616 | 0.038 | | | | | |
| Mitigation | 0.189 | 0.615 | 0.118 | | | | |
| Prevention | 0.198 | 0.613 | 0.151 | 0.878 | | | |
| Response | 0.120 | 0.565 | 0.074 | 0.863 | 0.886 | | |
| Security culture | 0.149 | 0.558 | 0.116 | 0.687 | 0.850 | 0.714 | |
| Top management involvement | 0.100 | 0.439 | 0.034 | 0.632 | 0.665 | 0.667 | 0.535 |

*Structural Model Assessment and Hypothesis Testing of Study 1*

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.

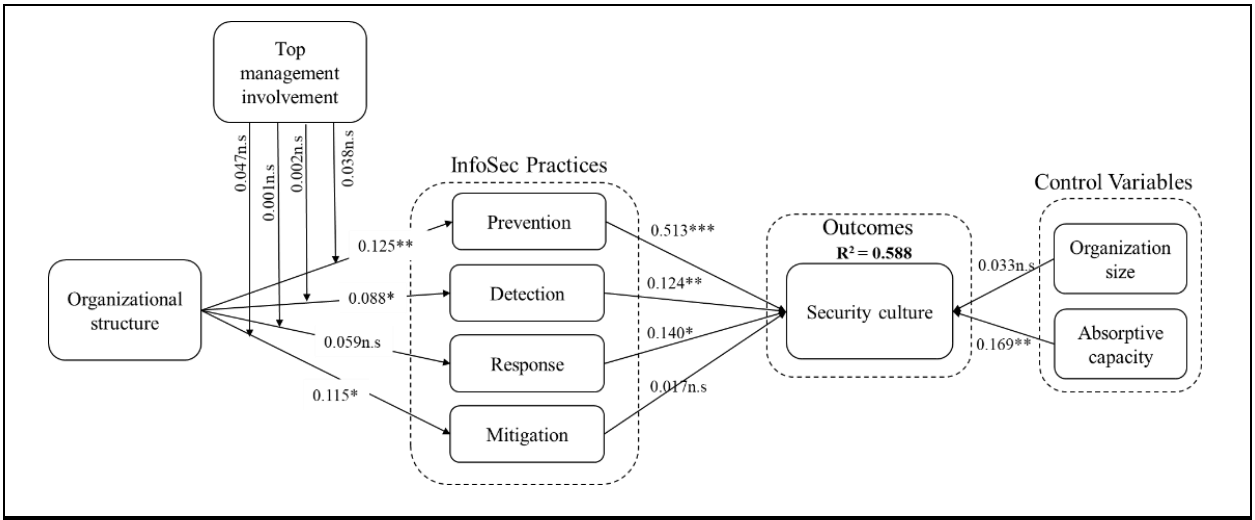


**Figure 2. Structural Model Results – Study 1**
*p<0.05, **p<0.01 and ***p<0.001

In terms of hypothesis testing, hypotheses H1(a-d), which hypothesized the positive association between InfoSec practices (detection, prevention and response) and security culture in organizations, were supported (path coefficients = 0.513, 0.124, 0.140, $p$=0.000, 0.004, 0.018, respectively), except the relationship between mitigation and security culture (path coefficient =

0.017, $p = 0.790$). The InfoSec practices with the emphasis to foster organizational capability to discover (detect and prevent) unexpected InfoSec incidents or to nurture organizational capability to manage and respond unexpected InfoSec events, would lead to InfoSec becoming part of the norms and values in an organization. However, the capability of an organization in designing a set of preplanned practices to reduce the impact of losses (mitigate) may not directly shape organizational security culture, as these plans will not be feasibly practiced until an incident happens. H2(a-d), which hypothesized the positive influence of organizational structure on InfoSec practices namely prevention, detection, response and mitigation, were supported (path coefficients = 0.125, 0.088, 0.059, 0.115 $p = 0.002$, 0.036, 0.112, 0.010 , respectively). These hypotheses infer that ensuring the alignment between security functions and business strategies, facilitates the effective implementation and coordination of InfoSec practices in organizations. H3(a-d), which hypothesized positive moderation effects of top management involvement on the relationships between organizational structure and InfoSec practices, were mot supported (path coefficients = 0.038, 0.002, 0.001, 0.047 $p < 0.05$, respectively), perhaps indicative of a limited ability on their part to steer organizational mechanisms toward the support of InfoSec practices, even when motivated to do so.

$R^2$ 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 organizational structure explains 34%, 15%, 35% and 32% of the variances in prevention, detection, response and mitigation, respectively. Combined, these InfoSec practices explain 59% of the variance in security culture. We have also applied the predictive sample reuse technique ($Q^2$) to assess predictive relevance using a blindfolding procedure. If $Q^2 > 0$, the model has predictive relevance, whereas $Q^2 < 0$ demonstrates a lack of predictive relevance (Chin and Dibbern 2010).

The predictive relevance of prevention, detection, response and mitigation practices were obtained using two-stage approach, with the values of 0.450, 0.287, 0.446 and 0.450, respectively. The predictive relevance of security culture was obtained using a two-stage approach, with the value of 0.365.

Two control variables, organization size and absorptive capacity, were also in Study 1. Absorptive capacity had a positive significant relationship with the security culture variables (path coefficients = 0.169 $p$ <0.01), indicating that organizations 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 organizations. Organization 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.

At this point in the theorizing process of a Security Culture Model, we have a reasonably well designed and supported model, based solely on insights provided by HRT. Based on these results, we plan to continue with Study 2 in order to thoroughly evaluate the context of an organizational security culture and identify additional practical and supportive proficiencies, revise the model to include those factors, consider the interaction of those factors with initial core elements of the model, and then ultimately test the revised model and any alternative models that may improve its explanatory efficacy.

## DISCUSSION

Organizations may easily miss the subtle interplay between security and reliability that can cause unexpected outcomes. Many security failures trigger by a reliability issue. Each reliable

organization has to understand the factors that contribute to developing a culture of security in order to persist sustainable practices (Adkins et al. 2020). Under-developed security cultures leave organizations 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 organizations, and the role of supportive proficiencies like organizational structure and top management involvement in this process. Test results of the initial model 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 organizational capability to protect information assets from unexpected InfoSec incidents or nurturing organizational 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 organization.

The findings of our research also underscore that ensuring the alignment between security functions and business strategies facilitates the effective implementation and coordination of InfoSec practices. However, it does not depict a strong influence on the InfoSec practices. Future research should identify additional practical and supportive proficiencies to better explain InfoSec practices in organizations. The findings of our research also highlight the difficulties managers often face in implementing InfoSec practices in their organizations. The fact that top management involvement was not found to moderate the relationship between organizational structure and InfoSec practices may suggest that top managers either do not play a part in helping align their organization's structures with its InfoSec practices or are simply ineffective in doing

so. While their involvement in helping formalize the structures relative to the InfoSec practices in the first place is required, their involvement isn't a requirement for success. 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. Future research, including the ongoing second part of this RIP (Study 2), should take a closer look into the reasons for this lack of significant moderating influence.

## CONCLUSIONS, LIMITATIONS AND FUTURE RESEARCH

In this preliminary study, we explored the role of practical proficiencies in forming security culture in organizations. We also examined the role of supportive proficiencies, such as organizational structure and top management involvement, 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 organizational processes and changes and may not be suitable for establishing causal relationships. Second, organizational structure did not explain high variances in InfoSec practices. Future research may explore other organizational supportive proficiencies to better explain InfoSec practice in organizations.

| **Appendix A. Previous Studies on Security Culture** | | | | |
|---|---|---|---|---|
| Author(s) Year | Determinant factors | Theory/ Framework | Method | Main Finding(s) |
| (Ashenden and Sasse 2013) | Role of Chief Information Security Officers (CISOs) | Organizational change programs framework | Interview with the CISOs – Qualitative study | CISOs struggle to gain credibility within their organization because of a perceived lack of power, confusion about their role identity, and their inability to engage effectively with employees. |
| (Chen et al. 2015) | Security policies, Security, education, training and awareness programs, Security monitoring | Schein's organizational culture theory, Van Niekerk and Von Solms' security culture framework | Web-based survey – Quantitative study | Positive associations between espoused values of the SETA programs, security monitoring and information security culture in organizations. No significant relationship between security policies and security culture in organizations. |
| (Da Veiga and Martins 2015) | Information asset management, Information security management, change management, user management, Information security policies, Information security program, Trust, Training and awareness | Information security culture assessment | Case study – Qualitative study | Information security training and awareness is a significant factor in positively influencing an information security culture. |
| (Da Veiga 2018) | Change management, Information asset management, Information security leadership, Information security management, Information security policies, Information security program, Trust, User management, Training and awareness, Privacy perception | Information security culture assessment | Survey - Quantitative study | Information security culture change management approach was found to be useful in defining change management interventions for organizations. |
| (Lim et al. 2010) | Senior management support and involvement, Assignment of security responsibilities, Enforcement of information security policies, Security awareness, Security training, Allocation of security budget | - | Case study – Qualitative study | It is critical to embed information security culture in a holistic manner that includes senior management support and involvement to encourage awareness through mandatory training with a clear assignment of responsibility and constant enforcement of security policies and procedures. |

| | | | | |
|---|---|---|---|---|
| (Nel and Drevin 2019) | Leadership and governance, Security management and operations, security policies, security program management, User security management, Technology protection and operations, and Change. | Da Veiga and Eloff (2010)'s framework | Online survey - Quantitative study | An initial framework of information security culture aspects has been constructed that can be used to ensure that an organization incorporates all key aspects in its own information security culture. |

**Appendix B. The Measurement Items of Constructs**

| *Constructs* | *Items* *Statements* | *Source* |
|---|---|---|
| Absorptive capacity | • ABSC1: Prior to the InfoSec practices, our employees in general had extensive awareness in security countermeasures in their work processes<br>• ABSC2: It is well known who can help solve problems associated with the information security<br>• ABSC3: Our company can provide adequate technical support to implement InfoSec practices<br>• ABSC4: Our company provides information security training opportunities to employees on a regular basis | (Liang et al. 2007) |
| Detection | • DETC1: We use active measures such as video and sensors to be able to detect security breaches.<br>• DETC2: We use sophisticated technologies to detect if security have been compromised.<br>• DETC3: We monitor and synthesise information regarding security breaches.<br>• DETC4: We do conduct periodic assessments of our security policies, procedures.<br>• DETC5: We have procedures to detect security failures or near failures. | (Lu et al. 2017) |
| Mitigation | • MITG1: We cross-train our employees as a mechanism to deal with potential disruptions.<br>• MITG2: We have backup processes that can assist us at times of crises.<br>• MITG3: We have strategies to use more standard parts to reduce the risk of disruptions.<br>• MITG4: We developed alternative material sources in case of disruptions.<br>• MITG5: We simplified jobs to the extent that unskilled employee can perform a variety of them in case of a crisis. | (Lu et al. 2017) |
| Organizational structure | *Formal organizational structure*<br>• FSTR1: We have an organizational unit with explicit responsibility for organising and coordinating information security efforts as well as handling incidents.<br>*Coordinating organizational structure*<br>• COSTR1: There is a committee, comprised of representatives from various business units, which coordinates corporate security initiatives.<br>• COSTR2: There is a committee, which deals with matters of strategic information security and related decision-making. | (Rocha Flores et al. 2014) |

| | | |
|---|---|---|
| | • COSTR3: Tactical and operative managers are involved in information security decision-making, which is related to their unit, responsibilities and/or subordinates.<br>• COSTR4: In our organization, people responsible for security and representatives from various business units meet to discuss important security issues both formally and informally. | |
| Prevention | • PERV1: Our security risk management strategy can be characterised as proactive.<br>• PERV2: When it comes to security, our strategy focuses on prevention.<br>• PERV3: We hold all third-parties accountable for security.<br>• PERV4: We only approve third-parties/partners (irrespective of tier) that have a security risk management programme in place.<br>• PERV5: We educate employees about security practices.<br>• PERV6: We have a process that notifies partners across tiers if the security is threatened. | (Lu et al. 2017) |
| Response | • RESP1: We know what to do when we encounter security breaches or crises.<br>• RESP2: We have designated a group of employees as first respondents in case of a crisis.<br>• RESP3: There is a definite chain of command in case of a security emergency.<br>• RESP4: We have protocols for communication when a crisis arises.<br>• RESP5: We have a well-defined contingency plan to react to serious security breaches.<br>• RESP6: We do have a disaster recovery plan.<br>• RESP7: We have a specific process to reinstate operations in case of a major crisis/disruption.<br>• RESP8: We have strategies for recovery action after disruptions. | (Lu et al. 2017) |
| Security culture | • SECU1: Employees value the importance of security of information and computer systems.<br>• SECU2: In my organization, a culture exists that promotes good security and privacy practices.<br>• SECU3: Security (of information and systems) has traditionally been considered an important organizational value.<br>• SECU4: Practicing good security of information and systems is the accepted way of doing business in my organization.<br>• SECU5: The overall environment in my organization fosters security-minded thinking in all our actions.<br>• SECU6: Information and systems security is a key norm shared by all organizational members/employees. | (Knapp et al. 2006) and (Chen et al. 2015) |
| Top management involvement | The senior management of our firm actively:<br>• TOPP1: Articulates a vision for the organizational use of security practices<br>• TOPP2: Formulated a strategy for the organizational use of security practices<br>• TOPP3: Established goals and standards to monitor the security practices | (Liang et al. 2007) |

| **Appendix C. The Procedural and Statistical Remedies Used in This Study** | |
|---|---|
| Techniques | Actions |
| *Procedural remedies (Podsakoff et al. 2003)* | |
| Protecting participants' anonymity and reducing evaluation apprehension | We guaranteed the anonymity of the participants before they took part in the survey. We assured them that there is no right or wrong answers and asked them to answer the questions as truthfully as possible. |
| Improving scale items | We adopted pre-validated reliable measurement items from the literature. |
| *Statistical remedies* | |
| Harman's single factor test (Harman 1976; Podsakoff and Organ 1986) | All the items were loaded into an exploratory factor analysis to examine the unrotated solution. The exploratory factor analysis of all the measurement items yielded forty-eight factors emerging from the dataset with the first factor extracted accounting 38.78% of the variance, and no factor accounted for the majority of the variance. Therefore, we can assume that CMB is not a major issue to our findings. |
| Lindell and Whitney's (2001) marker variable test | This test uses a theoretically unrelated construct as a control on dependent variables. In this study, we adopted a brand image construct from marketing field that was selected regarding participants' attitude towards Jetstar (Study 1) marketing and advertising campaigns from all media such as radio, TV, Internet, magazines and sponsorship activities. The difference in the comparative models, one with the marker variable and the other without this marker variable was very minor (i.e., 0.1%). The variance in security culture increased from 0.588 to 0.589, after the marker variable was included into the structural model. Also, all the significant paths stayed significant, indicating that CMB is not a major threat. |
| Full collinearity and multicollinearity assessment approaches (Kock 2015; Petter et al. 2007) | Following Kock (Kock 2015), we conducted full collinearity test and found that all VIFs were lower than 3.3. We also used the approach suggested by Petter et al. (Petter et al. 2007) to assess the formative construct validity, which entails testing multicollinearity among the indicators of the formative construct. All of the multicollinearity VIF values were less than 3.3, with values ranging from 1.66 to the highest value of 2.37, thus inferring no cause for concern with respect to CMB.<br>Overall, the results from these techniques support that CMB is not a serious issue for this study. |

## References


Adkins, H., Beyer, B., Blankinship, P., Lewandowski, P., Opera, A., and Stubblefield, A. 2020. "Building Secure and Reliable Systems," CA: O'Reilly Media.

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.

AlHogail, A., and Mirza, A. 2014. "Information Security Culture: A Definition and a Literature Review," *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*: IEEE, pp. 1-7.

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.

Becker, J.-M., Klein, K., and Wetzels, M. 2012. "Hierarchical Latent Variable Models in Pls-Sem: Guidelines for Using Reflective-Formative Type Models," *Long Range Planning* (45:5-6), pp. 359-394.

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.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and 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), pp. 151-164.

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., Astakhova, L. V., Botha, A., and Herselman, M. 2020. "Defining Organisational Information Security Culture—Perspectives from Academia and Industry," *Computers & Security* (92), p. 101713.
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.
Dutton, J. E., Ashford, S. J., O'Neill, R. M., and Lawrence, K. A. 2001. "Moves That Matter: Issue Selling and Organizational Change," *Academy of Management* (44:4), pp. 716-736.
Elyas, M., Ahmad, A., Maynard, S. B., and Lonie, A. 2015. "Digital Forensic Readiness: Expert Perspectives on a Theoretical Framework," *Computers & Security* (52), pp. 70-89.
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.
Gefen, D., Rigdon, E. E., and Straub, D. 2011. "Editor's Comments: An Update and Extension to Sem Guidelines for Administrative and Social Science Research," *MIS Quarterly* (35:2), pp. iii-xiv.
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.
Hong, W., Chan, F. K., Thong, J. Y., Chasalow, L. C., and Dhillon, G. 2014. "A Framework and Guidelines for Context-Specific Theorizing in Information Systems Research," *Information Systems Research* (25:1), pp. 111-136.
Jarvenpaa, S. L., and Ives, B. 1991. "Executive Involvement and Participation in the Management of Information Technology," *MIS Quarterly* (15:2), pp. 205-227.
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.

Knapp, K. J., Marshall, T. E., Kelly Rainer, R., and Nelson Ford, F. 2006. "Information Security: Management's Effect on Culture and Policy," *Information Management & Computer Security* (14:1), pp. 24-36.
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.
Liang, H., Saraf, N., Hu, Q., and Xue, Y. 2007. "Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management," *MIS Quarterly*), pp. 59-87.
Lim, J. S., Ahmad, A., Chang, S., and Maynard, S. B. 2010. "Embedding Information Security Culture Emerging Concerns and Challenges," *Pacific Asia Conference on Information Systems*, p. 43.
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.
Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., and Podsakoff, N. P. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology* (88:5), pp. 879-903.
Podsakoff, P. M., and Organ, D. W. 1986. "Self-Reports in Organizational Research: Problems and Prospects," *Journal of Management* (12:4), pp. 531-544.
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.
Rocha Flores, W., and Ekstedt, M. 2016. "Shaping Intention to Resist Social Engineering through Transformational Leadership, Information Security Culture and Awareness," *Computers & Security* (59), pp. 26-44.
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).
Singh, A. N., Gupta, M., and Ojha, A. 2014. "Identifying Factors of "Organizational Information Security Management"," *Journal of Enterprise Information Management*).
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.
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.