PACIS 2020 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

6-22-2020

The Establishment of Information Security Knowledge Sharing in Organizations: Antecedents and Consequences

Farkhondeh Hassandoust

Subasinghage Maduka Nuwangi

Allen C. Johnston

The Establishment of Information Security Knowledge Sharing in Organizations: Antecedents and Consequences

Completed Research Paper

Farkhondeh Hassandoust
Auckland University of Technology
Auckland, New Zealand
farkhondeh.hassandoust@aut.ac.nz

Subasinghage Maduka Nuwangi
Auckland University of Technology
Auckland, New Zealand
maduka.subasinghage@aut.ac.nz

Allen C. Johnston
The University of Alabama
Tuscaloosa, Alabama
ajohnston@cba.ua.edu

Abstract

Drawing on the extant literature on information security and neo-institutional theory, we develop and test a theoretical model to investigate the antecedents and consequences of the establishment of information security knowledge sharing (ISKS) in organizations. The model was tested using survey data from 403 top managers, who are aware of information security policies of their organizations. Our results suggest that external information security knowledge resources find their way into the organization by normative, mimetic, and coercive means, but much of their influence on ISKS practices are mediated by ISKS beliefs held by top management. Results highlight that firms face uncertainty in their ISKS practices and find themselves simply mirroring the practices of their peers without a real understanding of how that approach fits their organization's capacity for ISKS. Our findings emphasize the importance of ISKS practices for ensuring security compliance and the establishment and proliferation of an effective security culture.

Keywords: Information security knowledge sharing, neo-institutional theory, security compliance, security culture

Introduction

The key focus in information security (InfoSec) has shifted to the more holistic approach of InfoSec management encompassing organizational, technological and social aspects (Rocha Flores et al. 2014). A holistic InfoSec approach highlights the essential role of the 'human' factor in order to ensure the InfoSec management function within organizations is able to defend against attackers who have developed advanced attack techniques targeting organizational employees.

The lack of InfoSec knowledge among an organization's employees increases its vulnerability to InfoSec threats (Bauer et al. 2017), and there are a number of reasons why employees may lack this knowledge (Rocha Flores et al. 2014). It might be due to the low-level engagement of employees when developing different InfoSec policies or the way rules and regulations are communicated to them in terms of their responsibility for the protection of information assets. One way in which organizations have approached this problem is through knowledge sharing (Zakaria 2006). Knowledge sharing is manifested through informal (e.g., informal advisory services) and formal (e.g., education programs) mechanisms in organizations (Rhodes et al. 2008). For organizations to improve their employee's InfoSec knowledge and subsequent ability to help defend their organization, there is a critical need for the organization to establish effective InfoSec knowledge sharing (ISKS) practices – the platform, format, and processes by which InfoSec knowledge is shared among organizational employees.

Many previous studies have investigated the human side of InfoSec with two main focuses: 1) to understand risky behaviors among individuals (e.g., Boss et al. 2015; Ifinedo 2012); and 2) to evaluate which organizational and managerial factors influence InfoSec management practices (e.g., Knapp et al. 2006; Rocha Flores et al. 2014). While individual-level studies have increased the understanding of employee InfoSec compliance or misuse behaviors, they have not paid enough attention to the effect of organizational factors on security outcomes; factors such as organizational InfoSec policies. A number of studies have evaluated the InfoSec best practice frameworks and their organizational mechanisms, such as organizational processes and InfoSec awareness programs (e.g., Kayworth and Whitten 2010; Knapp et al. 2006); however, research which investigates the organizational structures and procedures of transferring security-related knowledge to employees in organizations is scarce.

On the other hand, top management's belief in and commitment to InfoSec is essential in achieving effective InfoSec procedures and driving organizational changes in relation to InfoSec activities in organizations (Barton et al. 2016; Bulgurcu et al. 2010; Hu et al. 2007). There are internal organizational structures and external institutional factors (e.g., government regulation) influencing top management's belief in InfoSec (Barton et al. 2016; Liang et al. 2007). These institutional factors also affect top management's decisions on the establishment of an integrated framework for capturing and sharing security knowledge to mitigate InfoSec risks within organizations (Rocha Flores et al. 2014). Drawing on the extant InfoSec literature and neo-institutional theory, we develop a theoretical model to explain the factors affecting the establishment of ISKS practices in organizations. Toward this purpose, we ask the question: Which institutional factors have a significant influence on the establishment of ISKS practices in organizations?

The establishment of effective ISKS practices entails organizational processes through which to conduct informal or formal InfoSec education and training programs, to generate well-established InfoSec guidelines and procedures, and to advise on reactions to InfoSec incidents (Rocha Flores et al. 2014). The establishment of ISKS practices improves its InfoSec processes in different ways, such as its InfoSec risk appetite and its InfoSec governance and business activities. All these information flows among organizational members can lead to changes in organizational culture by creating an environment that promotes and nurtures shared InfoSec values and beliefs (Van Niekerk and Von Solms 2010). The establishment of ISKS practices also improves the overall InfoSec compliance in organizations by promoting the effective implementation of InfoSec standards and policies that are able to minimize InfoSec risks in organizations (AlKalbani et al. 2015). Therefore, this study also seeks empirical evidence to answer the second research question: What are the consequences of the establishment of ISKS practices in organizations? The results of answering these questions can shed light on the important factors that should be taken into consideration to promote the establishment of ISKS practices and, ultimately, enhance the security compliance and security culture in organizations.

Conceptual Background

Information Security Knowledge Sharing (ISKS)

Digital technologies have created opportunities for computer crimes in which hackers and unauthorized users can gain access to organizational data. Therefore, it is important that organizations take necessary actions to improve the InfoSec awareness of their employees by establishing relevant organizational practices and strategies (e.g., security awareness programs and training of backup procedures). An organization's ISKS practices can minimize the danger of malicious attacks by increasing the InfoSec awareness of its employees. ISKS refers to the sharing of information and knowledge about organizational practices and strategies which can safeguard an organization's information assets, such as customer data, product information, and sales information (Rocha Flores et al. 2014; Safa and Von Solms 2016). Organizations may utilize formal mechanisms (e.g. training employees on general InfoSec threats and training on compliance with the security policies of the organization) and informal mechanisms (e.g. conducting informal meetings or discussions related to InfoSec) to share security knowledge (Rocha Flores and Antonsen 2013). Among the papers discussed the antecedents and consequences of ISKS. For example, according to Barton et al. (2016), memetic mechanisms influence top management belief in IS security mechanisms and top management belief increases the top management participation in IS security activities. Higher the level of top management participation, higher the level of IS security assimilation. Rocha Flores et al. (2014) explained that organizational structure and processes which can coordinate the implemented ISKS mechanisms positively influence ISKS establishment. According to Chen et al. (2015), there are positive associations between espoused values of the information security programs, security monitoring and information security culture in organizations. As per Da Veiga and Martins (2015), information security training and awareness is a significant factor in positively influencing an information security culture. ISKS practices minimize the costs related to security management by enhancing security awareness; one of the main mechanisms for mitigating the risk of InfoSec breaches (Safa and Von Solms 2016; Safa et al. 2016b). However, there is a general lack of motivation for InfoSec knowledge sharing among professionals (Safa et al. 2016a). Based on an understanding of ISKS practices in organizations, we can elaborate on a set of internal factors that influence how external InfoSec knowledge resources are translated into ISKS practices and how said practices ultimately influenced organizational security-related outcomes. Those internal factors are listed below.

Top Management Belief in ISKS

Top management beliefs regarding the potential of ISKS establishment plays an important role in implementing security mechanisms in organizations (Hsu et al. 2012). A top-down approach, where top managers influence employees to share security knowledge enables the integration of security strategy with overall business strategies (Barton et al. 2016). When top managers believe that ISKS practices provide benefits to the organizations, they tend to support the planning, development and implementation of ISKS initiatives (Jarvenpaa and Ives 1991; Liang et al. 2007). Top managers are more likely to support IS security policies and procedures that they perceive as fair and good quality. Top managers often have a lack of commitment to the establishment of ISKS, but they can be motivated by external and internal factors, such as government regulations and expectations of real time data accessibility, respectively (Tejay and Barton 2013). According to Hu et al. (2007), external factors are more powerful than the internal factors in influencing top managers with regard to InfoSec issues.

Absorptive Capacity

Absorptive capacity refers to the organizational readiness to engage in certain activities based on prior related knowledge and resources (Barton et al. 2016). An organization's absorptive capacity to engage in InfoSec activities can be improved by conducting InfoSec training programs (Zahra and George 2002) and by establishing technical teams to support employees during InfoSec threats. The development of absorptive capacity depends on feedback loops (Todorova and Durisin 2007), where increased knowledge in the ISKS practices supports the future enhancements of InfoSec in the organization. Previous literature on absorptive capacity explains the impact of absorptive capacity on innovation (Cohen and Levinthal 1990), organizational learning (Lane et al. 2006; Lane and Lubatkin 1998), and information technology implementations (Harrington and Guimaraes 2005). We consider that top management belief and absorptive capacity enhance the ability of the organizations to establish ISKS practices, which ultimately influence organizational security-related outcomes such as security compliance and security culture.

Security Compliance

Organizations invest in ensuring the effective implementation of information security policies, standards, and regulations to protect their information assets (Von Solms 2005) and to make certain that their employees follow their organizations' security rules and procedures (Siponen et al. 2010). Previous studies have investigated alternative approaches for improving information security compliance in organizations. For example, Safa and colleagues (2016a) explored the impact of employees' involvement, commitment, personal norms, and attitude on their security compliance behavioral intentions. Yoo and colleagues (2018) investigated the role of employees' psychological ownership and self-efficacy in their security compliance, while Hwang and Cha (2018) explored the role of organizational commitment in employees' compliance. Siponen and colleagues (2010) examined the factors relating to threat appraisal, self-efficacy, normative beliefs, rewards, and deterrence to understand employees' security compliance intentions and behaviors. These studies have primarily focused on the factors related to individuals' attitude, intentions, and behaviors and their compliance with information security policies and standards within organizations. However, there are several organizational level issues that need to be investigated in order to improve security compliance in organizations. The mere investigation of employees' behavior is not sufficient to understand how compliance is achieved in organizations (Daud et al. 2018). The underlying aspects that connect organizational practices with security compliance need to be recognized such as the organizational practices embedded with employees' skills and competencies that are accepted and practiced by them in delivering their job tasks (Kostova 1999). Since everyone in an organization is responsible for complying with information security policies, underlying factors such as information security knowledge sharing practices should be established to strengthen security compliance (Daud et al. 2018).

Security Culture

Cultivating an information security-aware culture minimizes the security and privacy risks to information assets within organizations (Da Veiga and Eloff 2010; Nel and Drevin 2019). Security culture as an organizational sub-culture with a specific goal of information security, involves an understanding and awareness of InfoSec issues and policies (Chen et al. 2015; Pfleeger et al. 2015). An information security culture is a collection of implicit and explicit forces that shape employees' security attitudes and behaviors over time, playing a critical role in the success of information security management in an organization (Chen et al. 2015). Organizations are mostly equipped with technical countermeasures and controls in place but to minimize InfoSec risks, organizations must focus on creating and growing a security-aware culture that accounts for the diverse range of possible InfoSec threats (Nel and Drevin 2019; O'Brien et al. 2013). Organizations should provide employees with security awareness and training programs to ensure employees are well equipped to follow InfoSec policy regulations (Bulgurcu et al. 2010). InfoSec protection should be a natural part of employees' daily activities in the workplace; that is, InfoSec should be integrated into the corporate culture and employees' InfoSec behaviors (Thomson et al. 2006). Previous studies have investigated a number of factors that influence security culture such as the role of chief information security officers, security policy, training, monitoring and enforcement, and top management support (Chen et al. 2015; Da Veiga and Martins 2015). However, very few of these studies have focused on the need to establish a foundation that can cultivate all these activities in one place. Despite the importance of establishing ISKS practices, there is a lack of research on the possible association between ISKS practices and security culture.

Theoretical Background

We argue that beyond internal organizational factors, ISKS practices are influenced by external institutions such as professional associations (e.g., ISO) and regulatory agencies (e.g., FDA). Since neo-institutional theory provides a lens by which to understand the impact of external institutions on organizational decision making and outcomes (Liang et al. 2007), neo-institutional theory has been employed as the theoretical basis of this research.

Neo-Institutional Theory

Neo-institutional theory emerged from the old-institutional theory because the old-institutional theory was lacking explanations for how institutionalization processes generate organizational value (Hu et al. 2007). Based on neo-institutional theory, Meyer and Rowan (1977) discussed how the prevalence of rationalized institutional elements and networks of social organizations influence formal organizational structures. Neo-institutional theory was enhanced by the discussions of DiMaggio and Powell (1983), where they explained that organizations change as per the influences of the actors within the organizational context. Previous research on neo-institutional theory (Greenwood and Suddaby 2006;

Leca et al. 2009) explained how cultural processes and actors affect the institutional arrangements (e.g. organizational practices and structures) within which they operate.

There are two main elements in neo-institutional theory: 1) institutionalization - the process where the organizational formal structure is established (Tolbert and Zucker 1983), and 2) isomorphism – the force on an organizational unit to resemble other units in the same environment (DiMaggio and Powell 1983). Further, neo-institutional theory explains three mechanisms of institutional isomorphic change: normative, mimetic and coercive (DiMaggio and Powell 1983). *Normative mechanisms* occur mainly from social values, social norms, and professionalization. While social values provide desirable methods of comparing and assessing existing behaviors, social norms define how things should be done (Scott 2013). Professionalization is the members of an occupation attempt to specify work conditions and procedures to create an occupational autonomy (DiMaggio and Powell 1983). Formal education and professional networks create an environment that supports shared social values and norms (Guler et al. 2002) leading to professionalization. Normative mechanisms may have positive impacts (e.g. value creation and opportunities to gain reputation) as well as negative impacts (e.g. deviations from goals and standards) on organizations (Staw and Epstein 2000). *Mimetic mechanism*s occur when organizations mimic the actions of other organizations due to uncertainly of the organizational environment, lack of understanding of organizational technologies, or ambiguous organizational goals (DiMaggio and Powell 1983; Liang et al. 2007). There is a high probability that the organizations mimic other organizations when they have boundary spanning ties (Mizruchi and Fein 1999). Mimetic mechanisms minimize the cost of finding viable solutions when organizations encounter similar issues (Hu et al. 2007). *Coercive mechanisms* are generated by the formal and informal pressures of external organizations, such as government and other powerful organizations upon which they are dependent (DiMaggio and Powell 1983; Guler et al. 2002). The cultural expectations of the environment within which the organization functions also play a role in generating coercive mechanisms. The formal and informal pressures can range from establishing rules, monitoring other organizations to identify whether they adhere to rules, and implementing rewards and punishments accordingly (Scott 2013).

Research Model and Hypotheses

Based on the previous theoretical discussion, this study proposes the research model in Figure 1. Normative and mimetic mechanisms are hypothesized as the antecedents of top management belief in ISKS practices, while coercive mechanisms are considered a direct antecedent of ISKS practices. Absorptive capacity is positioned as a moderator of the relationship between top management belief in ISKS practices and the ISKS practices themselves. Security compliance and security culture are positioned as two potential outcomes of ISKS practices.

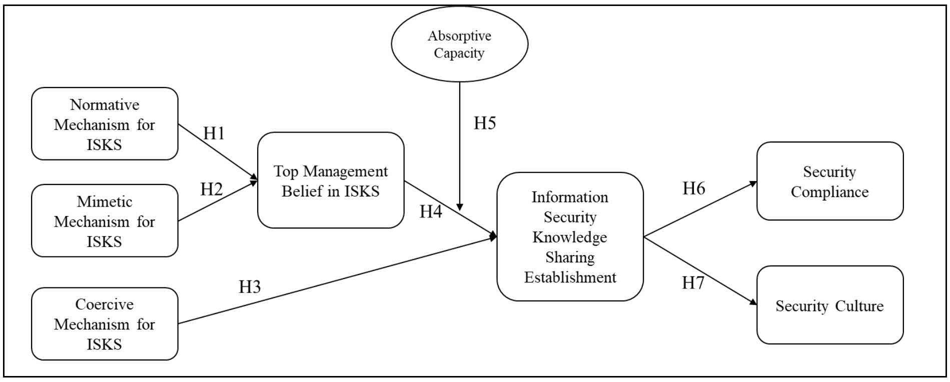
Absorptive Capacity
Normative Mechanism for ISKS
Mimetic Mechanism for ISKS
Coercive Mechanism for ISKS
Top Management Belief in ISKS
Information Security Knowledge Sharing Establishment
Security Compliance
Security Culture
H1
H2
H3
H4
H5
H6
H7

Figure 1. Proposed Research Model

The members of an industry such as suppliers, customers, and other stakeholders collectively evaluate and promote ISKS practices within their industry. Such normative mechanisms established by the members of the industry through social values, social norms and professionalization have the ability to influence top management beliefs on establishing new practices and procedures (Barton et al. 2016) such as ISKS practices. A person's beliefs are shaped by the subjective culture of their social networks and the interpersonal agreements the person has developed with social networks in specific social situations (Johnston and Warkentin 2010). For example, top managers' decisions to implement InfoSec policies and procedures is often influenced by normative mechanisms followed by suppliers, customers, and stakeholders (Cavusoglu et al. 2015). This is mainly because the firm can learn about the benefits and costs associated with the InfoSec practices from its business partners (Teo et al. 2003b). When organizations share InfoSec practices through organizational networks, those practices become stronger and better able to influence the beliefs of their managers (Teo et al. 2003b). Since universities, companies, and professional associations, such as ISACA, highlight the importance of InfoSec mechanisms, professionalism in the InfoSec industry has been increased. This strong sense of professionalism influences managers' beliefs about the importance of ISKS. When ISKS practices are a socially accepted norm, the managers have a tendency to believe that ISKS will provide benefits to the organizations. Thus, we hypothesize:

H1: Normative mechanisms are positively associated with top management beliefs in ISKS practices.

Mimetic mechanisms occur when organizations mimic the InfoSec policies and procedures of competitors without proper consideration. Organizations can mimic other organization's security policies in two ways (Teo et al. 2003b): following the security mechanisms which are successfully implemented by the other organizations in the industry or following the general practice of the industry. With a compliance perspective, the managers may adopt ISKS mechanisms which are aligned with the industry norms (Appari et al. 2009). The strength of mimetic mechanisms can be highlighted by the fact that the organizations follow the security policies and procedures of leading companies with the intention to gain a reputation. Managers mimic other organizations to minimize search costs of security solutions and to reduce the risk by not being the first to invent security policies. When the organization operates in an environment with unpredictable security threats, managers may attempt to mimic other organizations' InfoSec practices (Lun et al. 2008). Moreover, since the establishment of ISKS requires innovation which is risky, the organizations tend to mimic the security policies and practices of other organizations (Hwang and Choi 2017). Formal benchmarking and availability of security policies and procedures may contribute to these types of mimicking activities. Thus, we hypothesize:

H2: *Mimetic mechanisms are positively associated with top management beliefs in ISKS practices.*

Coercive mechanisms occur as a result of formal and informal pressures exerted on organizations by other organizations (DiMaggio and Powell 1983). InfoSec rules, policies and procedures established by the government and other powerful organizations (Kondra and Hurst 2009; Shi et al. 2008) can be considered as coercive mechanisms. Pressures arise from regulations may include legal requirements, health and safety requirements as well as contractual agreements with other organizations (Ashworth et al. 2007). Coercive mechanisms may have a direct or indirect influence on ISKS practices. For example, regulatory agencies such as international organization for standardization (i.e. ISO) have a direct influence on organizations as they are expected to follow the rules established by the regulatory agencies (e.g. ISO270001 standard). Even without a direct impact, the ISKS strategies followed by dominant organizations in an industry can originate an indirect pressure on the other organizations in the same industry (Cavusoglu et al. 2015). For example, when the dominant organizations in an industry equipped with integrated ISKS practices, it motivates other organizations to follow similar ISKS practices in order to achieve competitive advantages.

H3: Coercive mechanisms are positively associated with the organization's ISKS practices.

Top management identify and prioritize the organizations' strategic issues, which will receive organizational commitment and resources (Tejay and Barton 2013). Top management beliefs guide the actions, decisions and behaviors of the top managers (Liang et al. 2007). Therefore, when top management believe that there are InfoSec threats to the organization and it is important to take necessary actions to mitigate these security threats, they tend to commit to implementing InfoSec mechanisms (Barton et al. 2016). Beliefs of top managers about the benefits of InfoSec can signal the rest of managers and other employees about the importance of establishing InfoSec mechanisms (Chatterjee et al. 2002). When top managers believe that ISKS practices are not necessary for the organization, they do not invest their time and energy to explore about the ISKS practices. In contrast, when they believe that ISKS can provide benefits, they are likely support and participate in establishing ISKS practices in their organizations. We therefore hypothesize:

H4: Top management belief in ISKS is positively associated with establishing ISKS practices.

Absorptive capacity focuses on the acquisition of external knowledge as well as the organizations' ability to transform and exploit external knowledge (Rothaermel and Alexandre 2009). The organization's prior knowledge on the IS security mechanisms supports the assimilation of external knowledge about the IS security mechanisms and application of the InfoSec knowledge for commercial purposes (Liang et al. 2007). Providing security training for the employees and establishing InfoSec support teams serve as the bases of the organizations' ability to adopt and implement IS security mechanisms (Teo et al. 2003a). Firms with greater absorptive capacity would nurture the management belief in establishing ISKS. For example, the organization's prior related knowledge is useful for managers in identifying organizational benefits of ISKS practices. Although top managers are aware of the benefits of ISKS, the ability to establish ISKS practices also depends on organizations' absorptive capacity. For instance, ISKS cannot be established when employees are not ready to follow the security policies and procedures. Thus, we hypothesize:

H5: A firm's absorptive capacity positively moderates the impact of top management belief in ISKS on the establishment of ISKS practices.

Ensuring employee compliance towards InfoSec policies has been a major issue faced by organizations (Nasir et al. 2017). When the employees do not comply with security policies, organizations cannot gain the intended results from their security solutions (Puhakainen and Siponen 2010). Organizations can conduct trainings and awareness programs to improve employee understanding of the InfoSec threats and the importance of complying with the security policies and procedures established by the organizations (Rocha Flores and Antonsen 2013). When employees are aware of the danger of InfoSec threats, they tend to comply with the InfoSec policies and procedures. Moreover, the organizations can shape employees' attitudes to comply with security policies by establishing technology platforms which support the InfoSec knowledge sharing. Without InfoSec awareness, the organizations cannot ensure that the employees will comply with the security policies and procedures. InfoSec knowledge sharing is a sign of InfoSec involvement, where the employees are willing to share their knowledge with their fellow colleagues, leading to security compliance of the organization (Safa et al. 2016a). It is important that the organizations establish security policies and procedures to support ISKS, so that security compliance in the organizations can be strengthen (Daud et al. 2018). We therefore hypothesize;

H6: ISKS practices are positively associated with security compliance in an organization.

Lack of InfoSec awareness needs to be addressed to develop a security culture within the organizations (Martins and Elofe 2002). Conducting awareness programs on InfoSec can be considered as an initial step to shape the security culture. It is important that the organizations incorporate security behaviors into the routines of employees (Vroom and Von Solms 2004), so that the employees can follow security practices on a daily basis. This can be achieved by educating employees about security policies and procedures of the organizations as well as by ensuring that the employees interpret and understand security policies accurately (Chen et al. 2015). InfoSec culture emerges from awareness of the employees about acceptable security behaviors. When employees are aware of the importance of InfoSec policies, they tend to promote good security and privacy practices within the organizations (Whitman 2003). Implementing technologies for creating an integrated platform to provide necessary InfoSec-related knowledge and assist InfoSec knowledge sharing leads to an organizational environment that supports security minded thinking. We argue that establishing security awareness programs can help to form a security culture, where InfoSec is considered as an important organizational value. Thus, we hypothesize,

H7: ISKS practices are positively associated with the security culture of an organization.

Research Design

This study empirically evaluates the research model based on the perceptions of managers who are aware of InfoSec procedures, policies, and regulations in their organizations. We use measurement items that have been validated in previous studies. The measurement items on neo-institutional mechanisms, top management belief in ISKS, and absorptive capacity were adopted from Liang et al.

(2007). For ISKS practices, we adopted items from Rocha Flores et al. (2014). The six items measuring security culture were adopted from Chen et al. (2015). For security compliance, we adopted items from Siponen et al. (2010). 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. This cross-sectional study used online surveys distributed to professional managers through the Qualtrics platform. The sampling frame for this research was composed of 403 managers (after removing incomplete responses) across a broad range of roles and company sizes in Australia and New Zealand.

Data Analysis

We used Partial Least Squares – Structural Equation Modeling (PLS-SEM) SmartPLS 3.0 software to evaluate the measurement and structural model. PLS has been adopted as the most common approach in quantitative studies to evaluate the relationships between variables in human information security behaviors (e.g., Bulgurcu et al. 2010; Rocha Flores et al. 2014; Warkentin et al. 2016) and is recommended for exploratory research (Gefen et al. 2011) as well as for testing models that contain formative constructs (Petter et al. 2007). This research is exploratory and uses a model with formative construct (e.g., ISKS establishment), therefore PLS is a suitable tool for this study. To test for common method bias (CMB), we followed an approach proposed by Kock (2015) to conduct a full collinearity assessment. When a variance inflation factor (VIF) reaches a value greater than 3.3, it is considered as the pathological collinearity that indicates the model is infected by CMB (Kock 2015). We used the approach suggested by 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 1.42 to the highest value of 2.71, thus inferring no cause for concern with respect to CMB.

Measurement Model Assessment

According to Hair and colleagues (2019), 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. In the proposed research model, we assessed normative and mimetic mechanisms influencing the top management belief in ISKS. We also tested the impact of coercive mechanisms for ISKS and top management belief in ISKS on the establishment of ISKS practices. We then evaluated the influence of the establishment of ISKS practices on security culture and InfoSec policy compliance in organizations. In this study, all of the constructs are measured using first-order reflective measures except the establishment of ISKS practices which was assessed as a second-order formative construct with two reflective first-order constructs: formal knowledge sharing awareness and support for knowledge transfer.

To check if a construct explains more than 50 percent of the item's variance, the loading should be greater than 0.708. Therefore, non-contributing items need to be removed from the measurement model (Hair et al. 2019). All the items reported a loading greater than 0.708 except SUKS1, ABSC1 and ABSC2 (see table 1), which were subsequently removed from the research model. 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 indicated that all of the constructs were within acceptable thresholds. Convergent validity can be assessed 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 showed that all were above the cut-off value of 0.5, as shown in Table 1.

Table 1. Convergent Validity Testing

Construct	Item	Std. loading of each item	Cronbach's Alpha (α)	Composite Reliability (CR)	Average Variance Extracted (AVE)
Normative mechanism	NORM1	0.892	0.842	0.905	0.76
	NORM2	0.863			
	NORM3	0.859			
Mimetic mechanism	MIM1	0.822	0.836	0.902	0.754
	MIM2	0.9			
	MIM3	0.881			

Coercive mechanism	COER1	0.848	0.824	0.895	0.74
	COER2	0.879			
	COER3	0.853			
Top management belief in ISKS	TOPB1	0.884	0.836	0.901	0.752
	TOPB2	0.884			
	TOPB3-R	0.833			
Formal knowledge sharing awareness	FOKS1	0.939	0.87	0.939	0.885
	FOKS2	0.943			
Support for knowledge transfer	SUKS1	0.701	0.856	0.897	0.637
	SUKS2	0.788			
	SUKS3	0.791			
	SUKS4	0.837			
	SUKS5	0.772			
Security compliance	SCOM1	0.836	0.899	0.923	0.665
	SCOM2	0.816			
	SCOM3	0.839			
	SCOM4	0.832			
	SCOM5	0.741			
	SCOM6	0.826			
Security culture	SECU1	0.764	0.88	0.909	0.624
	SECU2	0.819			
	SECU3	0.767			
	SECU4	0.81			
	SECU5	0.789			
	SECU6	0.79			
Absorptive capacity	ABSC1	0.682	0.73	0.826	0.547
	ABSC2	0.605			
	ABSC3	0.798			
	ABSC4	0.848			

The discriminant validity of the constructs was tested by evaluating 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. For distinct constructs, HTMT values lower than 0.85 indicate discriminants validity (Henseler et al. 2015). In our study, the results show an acceptable level of discriminant validity based on the HTMT criterion with the values ranging from 0.293 to 0.74.

Assessment of Structural Model and Hypothesis Testing

Structural model evaluation involves assessing collinearity among the exogenous constructs, testing the significance and relevance of path coefficients, and examining the model's predictive accuracy and relevance model (Hair et al. 2019). To evaluate collinearity among the constructs, the Variance Inflation Factor (VIF) for each exogenous construct of the model was assessed. While VIF values should not be greater than 5, values less than 3 are seen as ideal values (Hair et al. 2019). The examination of VIF values showed that all the values were less than 2.71, indicating no cause for concern with respect to collinearity issues. To determine the statistical significance of the path coefficients, we ran the bootstrapping method using the number of samples as 2,000 and the number of cases as 300.

H1 and H2, which hypothesized the positive relationships between normative and mimetic mechanisms for ISKS, and top management belief in ISKS, were supported with path coefficients = 0.29, 0.39, $p < 0.001$, respectively. Hypotheses H1 and H2, infer that institutional norms coming from organizations' suppliers and customers about establishment of ISKS practice, as well as impersonating actions of successful peers or competitors would guide top managers' perceptions in making decisions to mitigate uncertain outcomes of InfoSec threats.

H3, which hypothesized a positive relationship between the coercive mechanism for ISKS and the establishment of ISKS practices, was supported (path coefficient = 0.22, $p < 0.001$). Thus, the policies and regulations imposed by the regulatory or government agencies would encourage the top management team as the focal point of these coercive mechanisms to take structuring actions for establishing the ISKS platform. In these circumstances, top management does not need to cognitively believe in the benefits of the establishment of ISKS. Therefore, coercive mechanisms and pressures directly simulate the actions aimed at the establishment of ISKS practices in organizations. H4, which hypothesized a positive association between top management belief in ISKS and establishment of ISKS in the organization, was supported (path coefficient = 0.14, $p < 0.001$). It indicates that top management beliefs about InfoSec threats and effectiveness of implementing the InfoSec procedures and policies positively influence the decisions on the establishment of ISKS in order to integrate all these procedures in one unified platform to better mitigate the InfoSec risks.

H5, which hypothesized a positive moderation effect of absorptive capacity on the relationship between top management belief in ISKS and establishment of ISKS, was not supported (path coefficient = -0.007, $p = 0.78$). This infers that top management team may not believe or be interested in developing the organizations' capabilities to provide responses, guidelines and policies to minimize InfoSec risks, and instead they may rely on the best practices developed by other organizations. H6, which hypothesized a positive association between establishment of ISKS practices and security compliance, was supported (path coefficient = 0.50, $p < 0.001$). Therefore, in order to improve compliance with InfoSec requirements, having an integrated platform for InfoSec processes that aims to detect and mitigate InfoSec risks is essential. H7 hypothesized a positive relationship between establishment of ISKS practices and security culture (path coefficient = 0.52, $p < 0.001$). This infers organizations equipped with an integrated platform for InfoSec awareness training, procedures and policies would be an initial step to shape the security culture in an organization. The normative and mimetic mechanisms explain 36% of the variance in top management belief in ISKS. Coercive mechanism and top management belief in ISKS explain 60% of the variance in the establishment of the ISKS construct. Moreover, the establishment of ISKS practices explains 25% and 27% of the variances in security compliance and security culture respectively.

Discussion

With organizations taking a more holistic approach to InfoSec that takes into account the organizational, technological, and social dynamics of the enterprise, the pressure to engage employees more closely in InfoSec planning and activities is greater than ever. For many organizations, however, the structures and procedures needed to effectively transform InfoSec knowledge from external resources into ISKS practices that support their InfoSec strategies are limited or under-developed. Much of this under-development may be associated with how the external InfoSec knowledge resources are made available to organizations as well as the value placed on them by top management. Unfortunately, there is lack of research which provide insights into this organizational phenomenon, with the majority of InfoSec research focused at the individual level. Little attention has been given to the issue of why organizations continue to struggle with developing ISKS practices that can help them improve both employee InfoSec policy compliance as well as their InfoSec culture.

Toward addressing this research gap, we leveraged neo-institutional theory to develop and test a research model that explains that external InfoSec resources are able to drive organizational ISKS practices. Test results of the model show that external InfoSec knowledge resources inform the development of ISKS practices directly by coercive means and indirectly by their normative and mimetic influence on top management ISKS beliefs. Of these, the strongest means by which external InfoSec knowledge resources are able to influence the development of ISKS practices is memetic. This suggests that firms continue to face uncertainty in their ISKS practices and find themselves simply mirroring the practices of their peers. While this is not a surprising outcome given the continued struggle among organizations to raise the profile of their InfoSec programs (Kam et al. 2019), the suggestion that the mimetic means of influence on ISKS practices is mediated by top management beliefs is interesting and can help explain why some InfoSec knowledge resources find their way into the organization, while others do not. Future research should examine how influential the eternal resources top management tap into are shaping ISKS practices.

The findings of our research also underscore the difficulties managers often face in implementing ISKS practices in their organizations. The fact that absorptive capacity was not found to moderate the relationship between top management belief in ISKS and ISKS practices may suggest that top managers give little consideration to the ability or preparedness of their organizations to implement ISKS practices, but rather feel compelled to push forward with them because others are doing so or because there are normative pressures for doing so. Either way, this suggests a disconnect between top management and organizational realities when it comes to ISKS practices; a disconnect that warrants further investigation. Finally, our findings also highlight the importance of ISKS practices for the sake of employee security compliance and the establishment and proliferation of an effective security culture. Prior research has shown that employees do not operate in a vacuum when it comes to interpreting and executing InfoSec policies, rather there is an element of collective security efficacy that helps drive individual behaviors (Johnston et al. 2019). The key to a well formed collective security efficacy is ISKS; wherein effective security responses are codified and distributed among an employee workforce or groups. Similarly, security cultures are reinforced through consistent successful patterns of behavior and outcomes. ISKS is paramount to this success.

Implications for Research and Practice

We believe our research contributes to both research and practices in multiple ways. First, given the relative lack of InfoSec research at the organizational level, our study provides some needed insight that can help academics to understand how firm-level security-related outcomes are formed due to both external and internal dynamics. Second, our study is one of the early studies to examine how external InfoSec knowledge resources find their way into the organization and directly and indirectly shape ISKS practices, and ultimately, enhance compliance and culture-related outcomes. Our study contributes to the literature on ISKS by explaining the mediating role of top management beliefs in terms of how external ISKS knowledge resources are translated from normative and mimetic forces into ISKS practices. This has tremendous implications to both academia and practice because; a) the current range of organizational behavior models do not explicitly account for this mediating effect, and b) it is behoovant upon organizational insiders to understand, and perhaps inventory, the external knowledge sources to which their top management subscribes. Further research designed to explore the transformational nature of external resources into organizational security outcomes and the strategies and mechanisms by which this transformation occurs is needed.

Limitations and Future Research

As with all research, our study has its share of limitations. First, the study is limited by its sampling frame. While organizational managers across a range of roles and companies in Australia and New Zealand are appropriate for testing our research model, it’s important to note that the normative and coercive pressures felt by these managers are most likely unique to their region and should not be assumed to map cleanly to other global regions. An extension of this sampling frame to include European, Asian, and American managers, along with a multi-group analysis of the survey results could help improve the generalizability of this study’s findings. Due to the complexity of absorptive capacity construct, future studies should measure it through a set of well-developed dimensions in order to better examine a firm’s absorptive capacity. Further, this study also suffers from the same limitations as all cross-sectional surveys in that the results are time-sensitive and may over-inflate the influence of regional InfoSec events that were prevalent at the time of data collection. Data collection over multiple points in time could help to offset this limitation.

Conclusions

Given the critical importance of ISKS practices to an organization’s InfoSec outcomes, their ability to harness the InfoSec knowledge and expertise available to them from outside sources is critical. Yet, how these resources are tapped into and influence ISKS practices is not well understood. Our study provides some needed insight into this important question and suggests that these external resources do find their way into the organization by normative, mimetic, and coercive means, but much of their influence on ISKS practices is mediated by the ISKS beliefs held by top management. Based on our findings, it appears as though many firms continue to struggle with uncertainty in how to approach their

InfoSec practices and, as a result, mimic their peers without any real understanding of how that approach fits their organization's capacity for ISKS.

References

AlKalbani, A., Deng, H., and Kam, B. 2015. "Organisational Security Culture and Information Security Compliance for E-Government Development: The Moderating Effect of Social Pressure," *PACIS*, p. 65.

Appari, A., Johnson, M. E., and Anthony, D. L. 2009. "Hipaa Compliance in Home Health: A Neo-Institutional Theoretic Perspective," *Proceedings of the first ACM workshop on Security and privacy in medical and home-care systems*: ACM, pp. 13-20.

Ashworth, R., Boyne, G., and Delbridge, R. 2007. "Escape from the Iron Cage? Organizational Change and Isomorphic Pressures in the Public Sector," *Journal of public administration research and theory* (19:1), pp. 165-187.

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.

Bauer, S., Bernroider, E. W., and Chudzikowski, K. 2017. "Prevention Is Better Than Cure! Designing Information Security Awareness Programs to Overcome Users' Non-Compliance with Information Security Policies in Banks," *computers & security* (68), pp. 145-159.

Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., and Polak, P. 2015. "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors," *MIS Quarterly (MISQ)* (39:4), pp. 837-864.

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.

Cavusoglu, H., Cavusoglu, H., Son, J.-Y., and Benbasat, I. 2015. "Institutional Pressures in Security Management: Direct and Indirect Influences on Organizational Investment in Information Security Control Resources," *Information & Management* (52:4), pp. 385-400.

Chatterjee, D., Grewal, R., and Sambamurthy, V. 2002. "Shaping up for E-Commerce: Institutional Enablers of the Organizational Assimilation of Web Technologies," *MIS quarterly*), pp. 65-89.

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.

Cohen, W. M., and Levinthal, D. A. 1990. "Absorptive Capacity: A New Perspective on Learning and Innovation," *Administrative science quarterly* (35:1), pp. 128-152.

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.

Daud, M., Rasiah, R., George, M., Asirvatham, D., and Thangiah, G. 2018. "Bridging the Gap between Organisational Practices and Cyber Security Compliance: Can Cooperation Promote Compliance in Organisations?," *International Journal of Business and Society* (19:1), pp. 161-180.

DiMaggio, P. J., and Powell, W. W. 1983. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields," *American sociological review*), pp. 147-160.

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*), pp. iii-xiv.

Greenwood, R., and Suddaby, R. 2006. "Institutional Entrepreneurship in Mature Fields: The Big Five Accounting Firms," *Academy of Management journal* (49:1), pp. 27-48.

Guler, I., Guillén, M. F., and Macpherson, J. M. 2002. "Global Competition, Institutions, and the Diffusion of Organizational Practices: The International Spread of ISO 9000 Quality Certificates," *Administrative science quarterly* (47:2), pp. 207-232.

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*).

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

Harrington, S. J., and Guimaraes, T. 2005. "Corporate Culture, Absorptive Capacity and It Success," *Information and Organization* (15:1), pp. 39-63.

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.

Hsu, C., Lee, J.-N., and Straub, D. W. 2012. "Institutional Influences on Information Systems Security Innovations," *Information systems research* (23:3-part-2), pp. 918-939.

Hu, Q., Hart, P., and Cooke, D. 2007. "The Role of External and Internal Influences on Information Systems Security–a Neo-Institutional Perspective," *The Journal of Strategic Information Systems* (16:2), pp. 153-172.

Hwang, I., and Cha, O. 2018. "Examining Technostress Creators and Role Stress as Potential Threats to Employees' Information Security Compliance," *Computers in Human Behavior* (81), pp. 282-293.

Hwang, K., and Choi, M. 2017. "Effects of Innovation-Supportive Culture and Organizational Citizenship Behavior on E-Government Information System Security Stemming from Mimetic Isomorphism," *Government Information Quarterly* (34:2), pp. 183-198.

Ifinedo, P. 2012. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory," *Computers & Security* (31:1), pp. 83-95.

Jarvenpaa, S. L., and Ives, B. 1991. "Executive Involvement and Participation in the Management of Information Technology," *MIS quarterly*), pp. 205-227.

Johnston, A. C., Di Gangi, P. M., Howard, J., and Worrell, J. 2019. "It Takes a Village: Understanding the Collective Security Efficacy of Employee Groups," *Journal of the Association for Information Systems* (20:3), pp. 186-212.

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS quarterly*), pp. 549-566.

Kam, H.-J., Mattson, T., and Goel, S. 2019. "A Cross Industry Study of Institutional Pressures on Organizational Effort to Raise Information Security Awareness," *Information Systems Frontiers*), pp. 1-24.

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 (ijec)* (11:4), pp. 1-10.

Kondra, A. Z., and Hurst, D. C. 2009. "Institutional Processes of Organizational Culture," *Culture and organization* (15:1), pp. 39-58.

Kostova, T. 1999. "Transnational Transfer of Strategic Organizational Practices: A Contextual Perspective," *Academy of Management Review* (24:2), pp. 308-324.

Lane, P. J., Koka, B. R., and Pathak, S. 2006. "The Reification of Absorptive Capacity: A Critical Review and Rejuvenation of the Construct," *Academy of management review* (31:4), pp. 833-863.

Lane, P. J., and Lubatkin, M. 1998. "Relative Absorptive Capacity and Interorganizational Learning," *Strategic management journal* (19:5), pp. 461-477.

Leca, B., Lawrence, T. B., Suddaby, R., and Leca, B. 2009. "Introduction: Theorizing and Studying Institutional Work," *TB Lawrence, R. suddaby & B. Leca (eds.), Institutional Work: Actors and Agency in Institutional Studies of Organizations*), pp. 1-27.

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.

Lun, Y. V., Wong, C. W., Lai, K. H., and Cheng, T. 2008. "Institutional Perspective on the Adoption of Technology for the Security Enhancement of Container Transport," *Transport Reviews* (28:1), pp. 21-33.

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

Meyer, J. W., and Rowan, B. 1977. "Institutionalized Organizations: Formal Structure as Myth and Ceremony," *American journal of sociology* (83:2), pp. 340-363.

Mizruchi, M. S., and Fein, L. C. 1999. "The Social Construction of Organizational Knowledge: A Study of the Uses of Coercive, Mimetic, and Normative Isomorphism," *Administrative science quarterly* (44:4), pp. 653-683.

Nasir, A., Arshah, R. A., and Ab Hamid, M. R. 2017. "Information Security Policy Compliance Behavior Based on Comprehensive Dimensions of Information Security Culture: A Conceptual Framework," *Proceedings of the 2017 International Conference on Information System and Data Mining*, pp. 56-60.

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*.

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

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

Puhakainen, P., and Siponen, M. 2010. "Improving Employees' Compliance through Information Systems Security Training: An Action Research Study," *MIS quarterly*), pp. 757-778.

Rhodes, J., Hung, R., Lok, P., Lien, B. Y. H., and Wu, C. M. 2008. "Factors Influencing Organizational Knowledge Transfer: Implication for Corporate Performance," *Journal of Knowledge Management*).

Rocha Flores, W., and Antonsen, E. 2013. "The Development of an Instrument for Assessing Information Security in Organizations: Examining the Content Validity Using Quantitative Methods," *International Conference on Information Resources Management (CONF-IRM)*, p. 44.

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.

Rothaermel, F. T., and Alexandre, M. T. 2009. "Ambidexterity in Technology Sourcing: The Moderating Role of Absorptive Capacity," *Organization science* (20:4), pp. 759-780.

Safa, N. S., and Von Solms, R. 2016. "An Information Security Knowledge Sharing Model in Organizations," *Computers in Human Behavior* (57), pp. 442-451.

Safa, N. S., Von Solms, R., and Furnell, S. 2016a. "Information Security Policy Compliance Model in Organizations," *Computers & Security* (56), pp. 70-82.

Safa, N. S., Von Solms, R., and Futcher, L. 2016b. "Human Aspects of Information Security in Organisations," *Computer Fraud & Security* (2016:2), pp. 15-18.

Scott, W. R. 2013. *Institutions and Organizations: Ideas, Interests, and Identities*. Sage Publications.

Shi, W., Shambare, N., and Wang, J. 2008. "The Adoption of Internet Banking: An Institutional Theory Perspective," *Journal of Financial Services Marketing* (12:4), pp. 272-286.

Siponen, M., Pahnila, S., and Mahmood, M. A. 2010. "Compliance with Information Security Policies: An Empirical Investigation," *Computer* (43:2), pp. 64-71.

Staw, B. M., and Epstein, L. D. 2000. "What Bandwagons Bring: Effects of Popular Management Techniques on Corporate Performance, Reputation, and Ceo Pay," *Administrative Science Quarterly* (45:3), pp. 523-556.

Tejay, G. P., and Barton, K. A. 2013. "Information System Security Commitment: A Pilot Study of External Influences on Senior Management," *2013 46th Hawaii international conference on system sciences*: IEEE, pp. 3028-3037.

Teo, H. H., Wan, W., Wang, X.-W., and Wei, K.-K. 2003a. "Effects of Absorptive Capacity on Organizational Predisposition toward Information Systems," in: *International Conference on Information Systems (ICIS)*.

Teo, H. H., Wei, K. K., and Benbasat, I. 2003b. "Predicting Intention to Adopt Interorganizational Linkages: An Institutional Perspective," *MIS quarterly*), pp. 19-49.

Thomson, K.-L., Von Solms, R., and Louw, L. 2006. "Cultivating an Organizational Information Security Culture," *Computer fraud & security* (2006:10), pp. 7-11.

Todorova, G., and Durisin, B. 2007. "Absorptive Capacity: Valuing a Reconceptualization," *Academy of management review* (32:3), pp. 774-786.

Tolbert, P. S., and Zucker, L. G. 1983. "Institutional Sources of Change in the Formal Structure of Organizations: The Diffusion of Civil Service Reform, 1880-1935,").

Van Niekerk, J., and Von Solms, R. 2010. "Information Security Culture: A Management Perspective," *Computers & security* (29:4), pp. 476-486.

Von Solms, B. 2005. "Information Security Governance: Cobit or ISO 17799 or Both?," *Computers & Security* (24:2), pp. 99-104.

Vroom, C., and Von Solms, R. 2004. "Towards Information Security Behavioural Compliance," *Computers & security* (23:3), pp. 191-198.

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.

Whitman, M. E. 2003. "Enemy at the Gate: Threats to Information Security," *Communications of the ACM* (46:8), pp. 91-95.

Yoo, C. W., Sanders, G. L., and Cerveny, R. P. 2018. "Exploring the Influence of Flow and Psychological Ownership on Security Education, Training and Awareness Effectiveness and Security Compliance," *Decision Support Systems* (108), pp. 107-118.

Zahra, S. A., and George, G. 2002. "Absorptive Capacity: A Review, Reconceptualization, and Extension," *Academy of management review* (27:2), pp. 185-203.

Zakaria, O. 2006. "Internalisation of Information Security Culture Amongst Employees through Basic Security Knowledge," *IFIP International Information Security Conference*: Springer, pp. 437-441.