DECISION SCIENCES INSTITUTE

Towards a Theory of Dynamic Information Security Behaviors

Canchu Lin
Carroll University
Email: clin@carrollu.edu

Anand Kunnathur
University of Toledo
Email: Anand.Kunnathur@utoledo.edu

ABSTRACT

As a theory paper, this study builds a framework that draws on the conceptual gist of organizational sensemaking to show the dynamic nature of information security behavior. It then situates the development of such dynamic information security behaviors in the context of organizational culture and proposes how organizational culture shapes these behaviors.

KEYWORDS: Dynamic information security behavior, Sensemaking, Organizational culture, Information security diagnosing behavior, Information security solving behavior, and Information security performing behavior

INTRODUCTION

A large number of information security incidents that incurred huge financial losses are reportedly due to ignorance, errors, and even deliberate computer abuse behaviors of employees in organizations (Lee & Lee, 2002; Lee et al., 2004; Willison & Warkentin, 2013). Sharing this concern, empirical research has mostly explored individual factors that lead to information security behaviors (ISB) (e.g., see Anderson & Agarwal, 2010; Banerjee, Cronan, & Jones, 1998; Bulgurcu, Cavusoglu, & Benbasat, 2010; Chatterjee, Sarker, & Valacich, 2015; D'Arcy & Herath, 2011; Lee & Kozar, 2005; Vance, Siponen, & Pahnila, 2012; Wright & Marett, 2010). Although ISBs are performed by individual employees, they occur in an organizational setting and therefore take on an organizational identity. Both the materiality and sociality of the organizational context determine individual employees' ISBs and their development patterns. Yet, despite the critical role of the organizational context, a theoretical lens that informs and enables analysis of individual ISBs from an organizational perspective is seriously missing in past and current research.

To fill this research gap, this study attempts to articulate a theory of dynamic information security behaviors (TDISB). Enlightened by the dynamic capabilities perspective (Teece, Pisano, & Shuen, 1997), the TDISB asserts that as tasks, information needs, and technology use in organizations change over time, organizations must develop dynamic capabilities to address the implications on information security that these changes generate. Such dynamic capabilities are mostly performed in their employees' behaviors regarding information security. Thus, viewed from this perspective, ISBs are dynamic in nature. As information security concerns stem from adoption, implementation, and use of technology, which triggers sensemaking (Griffith, 1999), ISBs can be perceived as outcomes of sensemaking. Thus, the TDISB maintains that sensemaking about information security at different phases predicts that different ISBs are required at these different phases of technology use.

Addressing information security in organizations is similar to action-oriented problem solving in some “high-velocity” or “high-hazard”, and “high-reliability” situations such as firefighting, manufacturing or computer programming troubleshooting, (Carroll, Rudolph, & Hatakenaka, 2002; Eisenhardt, 1989; Klein, Pliske, Crandall, & Woods, 2005; Repenning & Sterman, 2002; Weick, 1987; 1993), whose characteristics have been examined and well explained from the sensemaking perspective (Rudolph, Morrison, & Carroll, 2009; Weick, 1987). But little has been known about information security sensemaking.

Further, drawing on the research literature of organizational culture, the TDISB explicates how these dynamic ISBs are shaped by organizational culture. The benefit of applying the sensemaking perspective to the study of ISBs stems from its particular strength in analyzing individual behaviors by examining both individual cognition and organizational dynamics. At the individual level, sensemaking involves cognition, which is greatly shaped by organizational culture (Harris, 1994). In this sense, ISBs can be perceived as a site where sensemaking interacts with organizational culture as reinforcing forces. Thus, examining both sensemaking and organizational culture simultaneously holds promise for a deep understanding of the development of ISBs. The importance of organizational culture to the development of ISBs has been highlighted in previous research (e.g., see Da Veiga & Eloff, 2010; Kraemer & Carayon, 2005; Ruighaver, Maynard, & Chang, 2007; Van Niekerk & Von Solms, 2010). Further, organizational culture was sporadically examined as a factor influencing information security policy compliance (e.g., see Hu, Dinev, Hart, & Cooke, 2012). But there has been no theoretical attempt for integrating sensemaking and organizational culture to guide the investigation of ISBs. This study aims to articulate this new approach comprehensively and further develops it as a theoretical framework that constitutes TDISB.

While fulfilling this goal, this study attempts to make the following contributions. First, this study will extend and enhance our understanding of ISBs by conceptualizing some new categories of ISBs. Past research, relying on the deterrence theory, which originated in criminology, mostly focused on exploring negative ISBs and their drivers. Consequently, few ISBs especially positive ones were identified (Posey, Roberts, Lowry, Bennett, & Courtney, 2013). Drawing on the perspective of organizational sensemaking (Weick, 1979, 1995), this study will develop a taxonomy of ISBs based on the characteristics of sensemaking in different phases. The newly developed taxonomy will constitute a rich repertoire of ISBs that represent a heightened and extended understanding of ISBs. Second, this study will provide further insight into the development of ISBs. Past research mostly examined some individual factors that contribute to the development of negative ISBs and information security policy compliance. By nesting sensemaking on information security within the context of organizational culture, this study offers a theoretical framework that helps to examine ISBs from an organizational perspective. Although there are individual differences in ISB, organizational-specific schema shaped by organizational culture would determine the basic character of sensemaking about information security in the workplace and thus common features of individual ISBs. Third, as past research overwhelmingly focused on negative ISBs, an undesirable outcome was that individual employees have not been perceived as being able to positively contribute to information security management in their organizations. In delineating the various ISBs included in the new taxonomy, this study will show that individual employees can be a solution to information security issues (Stanton & Stam, 2006). Thus, this study will help to transform the image of individual employees as possible computer abusers or information security culprit into one of beneficial contributors to information security management.

The rest of the paper is organized as follows. First, we will review the current literature on ISB to provide an overview of major theories used in this area of research and the major findings regarding ISBs. Such a brief review will help us to identify areas of improvement in this field of research and, more importantly, look for directions for future research. We will provide a rationale for why the TDISB that nests sensemaking within organizational culture can help to overcome the limitations of the theoretical approaches currently used in the empirical research. Next, in developing the TDISB, we will draw on Weick's (1979, 1995) theory of organizational sensemaking to analyze information security management in organizations as a process of sensemaking. Analysis of this process of sensemaking will lead to the development of a taxonomy of ISBs. Then, to further the development of TDISB, we will integrate the review of ISB research and a brief review of organizational culture in order to show how organizational culture serves as both a platform and an effective control mechanism for information security management in organizations. Following that, we will focus on showing how different cultures help to promote a variety of ISBs. Lastly, we will discuss contributions of our framework, its possible implications for organizational practice, and future research directions.

INFORMATION SECURITY BEHAVIOR

As employees are deemed as the weakest link in organizations' efforts in addressing information security (Warkentin &Willison, 2009), IS researchers have made efforts to gain a deep understanding of this issue. They examined possible factors that influence employees' ISB and searched for effective means to control ISB. A review of the ISB research literature shows that two major approaches have been developed to the study of ISB. As early studies on ISB mostly used the deterrence theory, the deterrence approach has substantially shaped the research landscape in this area. There are already two literature reviews of the deterrence research on ISB (D'Arcy & Herath, 2011; Siponen, Willison, & Baskerville, 2008). This is enough evidence of the research productivity and also popularity of the deterrence approach. Borrowing the theory from criminology, the deterrence approach researchers applied the concepts of certainty, severity, and celerity of sanctions against illicit behaviors (Gibbs, 1975) in their empirical research. Although behaviors such as misuse or abuse of IS resources were examined, the key concern of the empirical studies of this approach is compliance or noncompliance of organizational information security policies and their antecedents (D'Arcy & Herath, 2011).

Besides the deterrence theory, information security researchers have also utilized behavior theories to examine ISB. These behavior theories have helped us to understand individual employees' cognitive behaviors regarding information security from a social perspective. The approach that represents these empirical studies is hereby named as the social cognitive approach. The social cognitive approach mainly used the theories of ethical/moral behavior (e.g., Banerjee et al. 1998; Culnan & Williams, 2009; Harrington, 1996; Myyry, Siponen, Pahnila, Vartiainen, & Vance, 2009), rational choice (e.g., Bulgurcu et al, 2010; Li, Zhang, & Sarathy, 2010), reasoned action (e.g., Guo, Yuan, Archer, & Connelly, 2011), planned behavior (e.g., Bulgurce et al., 2010; Guo et al., 2011), protection motivation (Ng, Kankanhalli, & Xu, 2009; Herath & Rao, 2009a; Pahnila, Siponen, & Mahmood, 2007), and technology acceptance model (Johnston & Warkentin, 2010; Ng & Rahim, 2005). Similar to the deterrence studies, a large number of empirical studies taking the social cognitive approach treated information security policy compliance as the dependent variable receiving influence from antecedent variables. Such an approach is still popular in recent studies (see, for example, D'Arcy, Herath, & Shoss, 2014; Hu, West, & Smarandescu, 2015; Johnston, Warkentin, & Siponen, 2015, and Vance,

Lowry, & Eggett, 2015). Yet, regrettably, prior research taking those two approaches discovered few ISBs other than policy compliance. More ISBs are yet to be identified.

The social cognitive approach examined antecedents to ISB, including ethics/moral judgment, security-related perceptions (regarding security risk, severity, vulnerability, and susceptibility), coping perceptions (response efficacy, effectiveness and benefits), security-related attitudes and norms, information security awareness, and self-efficacy. These antecedents were examined as predictors of ISB, mostly information security policy compliance. Based on their definitions, these antecedents can be grouped into three categories: ethics and morality, perceptions and attitudes, and knowledge and skills. As a major antecedent, ethics influences an individual's perception of information risk or threat, which then determines his or her behavior toward the risk or threat such as adoption of anti-spyware software (Lee & Kozar, 2005). Similarly, employees with strong moral beliefs are found to be restrained from misuse or abuse behavior (D'Arcy & Herth, 2011). In addition to ethics and moral judgment, perceptions and attitudes are found to be important precursors to ISBs (see, for example, Anderson & Agarwal, 2010; Guo et al. 2011; Johnston & Warkentin, 2010; Ng et al., 2009). Information security related perceptions include those of security risk (see Guo et al., 2011; Wright & Marett, 2010; and Xu, Wang, & Teo, 2005), risk or threat severity, computer or information systems' vulnerability and susceptibility to risks and threats (LaRose, Rifon, & Enbody, 2008; Lee & Larsen, 2009; Ng et al., 2009; Workman, Bommer, & Straub, 2008), possible benefits of coping behavior such as response efficacy (Johnston & Warkentin, 2010; LaRose et al., 2008; Lee & Larsen, 2009; Woon, Tan, & Low, 2005), and security behavior effectiveness (Anderson & Agarwal, 2010; Culnan, Foxman, & Ray, 2008; Ng et al., 2009). These perceptions are positively related to attitude toward security-related behavior (Anderson & Agarwal, 2010), which then leads to security behavior (Guo et al, 2011; Lee & Kozar, 2005). Lastly, knowledge and skills provide employees confidence and expertise needed for positive ISB (Wright & Marett, 2010). Knowledge and skills include information security awareness, more specifically, awareness of risks or threats, and awareness of measures available for coping with risks and threats (Aytes & Connolly, 2004; Bulgurcu at al., 2010; Furnell, 2008; Hu, Hart, & Cooke, 2006; Whitman, 2004), and self-efficacy (Anderson & Agarwal, 2010; Bulgurcu at al., 2010; Lee & Kozar, 2005; Lee & Larsen, 2009; Ng et al., 2009; Woon et al., 2005; Wright & Marett, 2010).

To sum up, the deterrence approach and the social cognitive approach helped to advance our knowledge of negative ISBs and factors influencing information security policy compliance. However, limited progress was made in previous research using those two approaches in extending our understanding to multiple especially positive ISBs. To address this research gap, a different theoretical approach is needed. An ideal theoretical perspective is one that can provide insight into both negative and positive ISBs (Posey et al., 2013) and, more importantly, explain the underpinnings of those behaviors. We argue that the TDISB that integrates sensemaking and organizational culture to provide a systematic examination of ISBs is such an ideal perspective. Our rationale is provided next.

THEORY OF DYNAMIC INFORMATION SECURITY BEHAVIORS

The TDISB provides a new lens for us to examine ISBs by integrating the essentials of sensemaking and organizational culture. Information security management is similar to issues of crisis and safety management in that that they all involve coping with uncertainty and making decisions. Sensemaking and organizational culture have been demonstrably relevant to management of these high-reliability or high-hazard issues (e.g., see Weick, 1987, 1993). However, both have been overlooked in the literature of ISBs.

Sensemaking has been rarely addressed in this thread of literature. But for organizational culture, its role in shaping ISBs was slightly suggested in previous research. Indeed, previous research with the social cognitive approach sporadically showed the impact of organizational culture on the precursors of ISBs. But, organizational culture was mainly examined as one independent variable (in addition to others) (e.g., Bulgurcu et al. 2010; Guo et al. 2011; Herath & Rao, 2009b) or a contingency variable that moderates the relationship between the precursor variables and ISB (e.g., Dinev, Goo, Hu, & Nam, 2009; Hovav & D'Arcy, 2012). Examining organizational culture together with other antecedent factors only aimed to show how organizational culture may contribute to the development of ISB of individuals, but did not reveal any organizational pattern in ISBs. With that approach, our understanding of organizational-level ISBs is still lacking. As their focus was not on organizational culture, previous research did not show the full potential of organizational culture on cultivating and developing different ISBs. Additionally, previous research articulated a view that it is important to develop a specific information security culture in organizations to help to manage information security (see, e.g., Da Veiga & Eloff, 2010; Kraemer & Carayon, 2005; Ruighaver et al., 2007; van Niekerk & von Solms, 2010; Vroom & von Solms, 2004). This view was mostly prescriptive in that it offered culture as a solution to information security problems, but did not explain how culture can play that role. Besides, arguing for establishing an information security culture in organizations deviates from a widely shared view that culture is emergent and complicated, but not imposed (Detert, Schroeder, & Mauriel, 2000). To sum up, previous research, while rarely touched on sensemaking, because of its inadequate design and biased view toward organizational culture, showed us little evidence of organizational culture's role in shaping ISBs.

Yet, both sensemaking and organizational culture are highly relevant to ISBs. Sensemaking links cognition and action (Weick, 1979, 1995) and therefore can explain how individual employees perceive risks and threats to information security by interpreting informational cues and then act to cope with such risks and threats. Similarly, culture is an effective mechanism for behavior control (O'Reilly & Chatman, 1996; Ouchi, 1980; Ray, 1986; Schein, 1985). In this sense, the perspective of organizational culture holds promise for providing insightful explanations for how organizational culture shapes ISBs. Additionally, it can offer insight into the development of multiple such behaviors, as it holds that there is much multiplicity and diversity in organizational culture (Martin, 2002; Van Maanen & Barley, 1984). Overcoming the weaknesses of the deterrence theory and the social cognitive theories, the TDISB can potentially explain how different cultures cultivate and shape different ISBs. Before we show how sensemaking and organizational culture contribute to the development of ISBs, we deem it important to explain how sensemaking and organizational culture are linked together and interactively generate and shape different ISBs. In doing this, we show the gist of the TDISB.

The first main point of this TDISB is that organizational culture facilitates sensemaking, as "shared, relatively coherent interrelated sets of emotionally charged beliefs, values and norms that bind some people together and help them to make sense of their worlds" (Trice & Beyer, 1993, p. 33). Sensemaking refers to a gradual development of a loose agreement among organizational members about how to interpret an event and take action to address it (Orton, 2000). The event is new, unexpected, confusing, and involves a lot of uncertainties (Maitlis & Christianson, 2014). It requires organizational members to use systematic rules to make judgement about causal relationships (Einhorn & Hogarth, 1986). When coping with an event, different organizational members scan different cues of the event, display different beliefs in making judgement, and prefer different actions. Yet over time, these fragmentations among the individual employees are transformed into an organizational consensus, which Weick (1979)

termed as “workable version of reality”, which serves as the basis of decision making by organizational members. The final decision culminates the organizational sensemaking process regarding the treatment of that event. The transformational process of integrating individual differences into an organizational agreement and then decision choice is made possible by organizational culture. Organizational culture serves as a “dominant perceptual filter that shapes and biases sensemaking” (Abolafia, 2010, p. 357). When articulating, discussing, and then evaluating various interpretations, preferences, and decision alternatives from individual employees, they draw on beliefs, norms, values, and rules that are supposedly sensible and binding to organizational members (Bowman & Hurry, 1993). Their organizational culture may well be the most readily available source that supplies them with such beliefs, norms, values, and rules. Cultural values such as individualism, hierarchy, egalitarianism, and fatalism provide framing assumptions that influence sensemaking (Malsch, Tremblay, & Gendron, 2012).

Second, the TDISB maintains that organizational culture constitutes a social context for sensemaking. As a macro context or institutional factor, organizational culture serves as three mechanisms – priming (source of social cues), editing (accomplished through social feedback), and triggering (ambiguity and confusion inherent in organizational culture causing interpretations), through which substance of organizational culture such as beliefs, norms, values, and rules is woven into sensemaking (Weber & Glynn, 2006). Further, organizational culture provides the cultural identity for sensemaking by individual employees, which makes their sensemaking as organizational not just individual (Weber & Glynn, 2006). Examples of interactions of sensemaking and organizational culture are already supplied in the literature. For example, the ‘mechanism’ role of institution (culture) enables sensemaking in the context of interorganizational relationships (Vlaar, Van den Bosch, & Volberda, 2006). Similarly, culture’s interaction with sensemaking also occurs in the organizational process of constructing and negotiating compensation policies (Malsch et al., 2012). In the context of ISBs, we will show that sensemaking and organizational culture interact in such a way that sensemaking helps to develop ISBs and then organizational culture facilitates and shapes the development of ISBs by influencing sensemaking.

ORGANIZATIONAL SENSEMAKING AND INFORMATION SECURITY BEHAVIORS

In developing the TDISB, we argue that information security management in organizations is a sensemaking process. Managing information security involves interpretation and choice, a process of sensemaking and decision making, just as many other action-oriented problem solving situations (Rudolph, Morrison, & Carroll, 2009). Technology triggers sensemaking (Griffith, 1999). Organizational members’ social interactions impact how they interact with IT (Agarwal and Prasad, 1998; Moore & Benbasat, 1991; Vaast & Walsham, 2005; Walsham, 1998), leading to social constructions of information security emanated from IT. When a new technology or practice is introduced in an organization, it will trigger much uncertainty, or in Weick’s (1979) term, equivocality. This uncertainty includes unsureness about information security associated with the new technology or practice. What ensues uncertainty or equivocality is sensemaking by organizational members (Weick, 1979; 1995). Organizational members are expected to exhibit multiple behaviors in their information security sensemaking process. Thus, examining this particular sensemaking process helps to reveal possible behaviors of managing information security by organizational members.

Sensemaking is a sequential process and consists of three activities: scanning, interpreting, and responding (Daft & Weick, 1984; Thomas, Clark, & Gioia, 1993). Scanning is about information gathering (Thomas et al., 1993). In this phase of sensemaking, organizational members seek

informational cues from their environment to reduce the amount and complexity of information and notice different aspects of a situation such as technology adoption and use. Interpreting refers to the act of making meaning out of ambiguous cues (Porac & Thomas, 2002). In the interpreting phase, organizational members perceive certain issues as relevant or irrelevant to the situation (Barr & Huff, 1997). Lastly, responding is the action based on the interpreting outcomes (Hahn, Preuss, Pinkse, & Figge, 2015). In the responding phase, organizational members seek solutions to address the situation. Although scanning and interpreting are two distinct phases, both involve cognition. In the context of managing information security, organizational members in these two phases of sensemaking tend to behave in a similar manner, i.e., seeking information and making meaning out of it. So, these two phases can be treated as one of perception and understanding. Unlike perception, responding is real action. In the responding phase, managing information security actually involves seeking solutions for information security problems such as risks and threats. From this perspective, we argue that managing information security behaviors in the two phases of scanning and interpreting is similar but very distinct in the phase of responding. As an extension of the sequential view of sensemaking, enactment is regarded as what follows sensemaking (Weick, 1977, 1995). In the enactment phase, organizational members execute their sensemaking outcomes such as decisions. Below, to develop the TDISB, we elaborate three types of ISBs developed in the phases of scanning and interpreting, responding, and enactment.

Information Security Diagnosing Behavior

As technology is equivocal (Weick, 1990), among others, information security implications of technology can trigger intense sensemaking among internal employees. According to Weick (1995), sensemaking is also noticing, gathering facts and opinions. Sensemaking involves individuals' reactions to what they notice in their environment. When involved in technology sensemaking, in the phases of scanning and interpreting, organizational members gather various kinds of information about the technology and its possible impacts from their peers and other social contacts (Fulk, 1993; Gopal & Prasad, 2000). When a technology is just adopted, the uncertainty around it should also involve diverse concerns about information security it may generate. So, at the initial phase of technology implementation, organizational members' sensemaking about the technology may involve finding out the benefits as well as downsides of implementing the technology including possible loopholes in information security that this newly adopted technology may create to the organization. For example, cloud computing provides promises in storing and transferring huge amounts of data. When a technology company decides to adopt it, its employees would throw in numerous questions regarding information security. Specifically, they would identify and discover risks of data breach (Sen & Borle, 2015).

Further, the ongoing nature of organizational sensemaking suggests that employees' discoveries of potential information security issues inherent in the use of this same technology are continuous. They will discover other information security problems which will emerge at subsequent phases of using this same technology. For example, when companies adopted wireless systems, they kept exploring potential security issues and threats of this new adoption until wireless security reached to the level of wired security, but by that time, the wired world may have developed to a level where new security challenges occur, which require addressing different security needs (Katos & Adams, 2005). Similarly, as email is extensively used, large numbers of useless emails may block and slow down email communication. The email spam issue is therefore identified (Caliendo, Clement, Papies, & Scheel-Kopeinig, 2012).

More importantly, employees are motivated to *voice* their concerns and comments regarding information security when they realize that doing that ultimately helps their organization in addressing information security (Hsu, Shih, Hunng, & Lowry, 2015). Thus, to a large extent, internal employees often engage themselves in sensing about technology's possible risks, threats, as well as dangers to information security. Such behaviors aim at discovering potential information security issues and problems, and thus can then be categorized as information security ***diagnosing*** behaviors. ***Information security diagnosing behavior*** is hereby defined as an activity in which employees are engaged in finding out possible risks, dangers, and threats of a technology with regard to information security. One such diagnosing behavior is finding and reporting a potential information-security problem or loophole (Posey et al. 2013).

In line with the social nature of sensemaking, information security diagnosing behaviors pertain to various groups of employees. It may not always be the IT staff of a company that are engaged in such diagnosing behaviors. For example, in a healthcare organization, physicians, nurses, IT professionals, and other groups of employees perceived different information security issues about the same information systems (Vaast, 2007). As non-IT employees ultimately use a newly adopted technology to perform their work duties, they are more likely than IT staff to discover substantial and concrete issues and threats regarding information security.

Information Security Solving Behavior

Although organizational sensemaking is ongoing, it may take on different phases, thus triggering different actions or behaviors (Weick, 1995) toward information security. In the responding phase, organizational members mainly seek methods to solve problems (Hahn et al., 2015). This suggests that even though discovering information security issues and problems is continuous, at a time when such issues and problems have triggered enough organizational awareness, sensemaking may start to move from discovering problems, issues, risks, and threats that the new technology poses to generating solutions to them. For example, for an organization that has suffered from computer crashes caused by malware, the urgent need to stop such crashes may motivate employees to develop anti-malware software (Kim & Kim, 2015).

Accompanying the emerging information security concerns are efforts and motives to search for measures that address the information security concerns. Such measures can be technological as well as behavioral. While IT staff can take a leading role in developing technical measures to address information security concerns inherent in the adoption of a new technology, non-IT employees can make sense of how they can cope with these issues and problems behaviorally (Vaast, 2007). For example, in Vaast's (2007) study, IS professionals reported their continuous development of aggressive tools to detect virus and intrusions from outside, whereas non-IT employees learned to be more sensitive to inquiries about patients' personal information and develop a standard way to reject such inquiries. In the case of implementing cloud computing, while IT professionals may develop technical solutions such as enhancing their IT infrastructure's capability of speedily identifying and alerting about potential hacking activities, non-IT employees may brainstorm about secure ways of sharing sensitive information with their company's external stakeholders, and accumulate their successful experiences and promote them to more employees.

In sensemaking, human agents draw on not only local/organizational but also institutional rules and resources (Weber & Glynn, 2006). Institutions also function to contextualize sensemaking by imposing cognitive constraints on the actors in their sensemaking (Weber & Glynn, 2006;

Weick et al., 2005). To conform to institutional requirements, organizational members may engage themselves in information systems security innovations (Hsu et al., 2012). Besides their own experiences, employees may develop measures to safeguard company information through external learning, an important source of knowledge acquisition (March, 1991). For example, for a company dealing with wireless security issues, employees can turn to Wireless Location Industry Association for more resources, which has developed a set of self-regulation policies for dealing with security implications of wireless systems (Katos & Adams, 2005). Other external learning sites such as professional conferences sponsored and organized by professional organizations helped companies to develop procedures and policies to deal with information security (Hu et al., 2007). Employees' personal as well as professional external networks enable them to learn solutions developed elsewhere. Regardless of the sources, solutions to information security concerns are developed. Thus, behaviors engaged in seeking solutions can be defined as ***information security solving behaviors***. Further examples of such information security exploring behaviors include developing anti-virus software, standard steps in sending and receiving email attachments, and effective anti-phishing methods (Abbasi et al., 2015).

Information Security Performing Behaviors

Finally, the outcome of organizational sensemaking is characterized by the process of enactment (Weick 1995). In Weick's theory of sensemaking, sensemaking and organizing are interconnected and mutually enmeshed (Weick et al., 2005). After numerous communication cycles (Weick, 1979), organizational members will develop a sense about the new phenomenon toward which sensemaking is focused. That newly developed sense will then be saved as an organizational routine that will be used to guide future organizational action toward dealing with such a phenomenon. Weick (1979) named this process as enactment. In the case of sensemaking about information security, when information security issues, problems, and threats have been carefully examined, and reliable measures have been developed to address these issues, problems, and threats, such reliable measures would be saved as organizational procedures or standard practices to deal with information security. In many cases, these procedures and practices would be documented as organizational information security policies to guide action. During the enactment phase, individual behaviors expected from employees would be mostly to follow the prescribed practices and abide by organizational regulations and policies regarding information security. In this sense, ISBs are mostly performing in nature. Thus, such behaviors are defined as ***information security performing behaviors***, which are prescribed in information security policies. For example, once techniques are proposed and developed for ensuring safe and concurrent execution of database transactions (Croker, 1987), they would be covered in organizational information security policies. Employees would be trained to apply those techniques in their work.

TDISB - LINKING ORGANIZATIONAL SENSEMAKING ABOUT INFORMATION SECURITY TO ORGANIZATIONAL CULTURE

Weick's sensemaking theory is a general characterization of the process of organizational sensemaking. Special attention should be paid to sensemaking by diverse groups of organizational members (Maitlis, 2005). As they engage in sensemaking from a variety of organizational positions and subcultures (Dutton & Dukerich, 1991; Gephart, 1993; Weick, 1995), their sensemaking processes unfold in different patterns or forms that lead to different outcomes (Maitlis, 2005). Depending on the sensemaking process characteristics (levels of animation and control) (Maitlis, 2005), organizational sensemaking outcomes in terms of the

accounts generated can be unitary and convergent or multiple and divergent (Balogun & Johnson, 2004, 2005). Unity and divergence may very well be manifested in information security sensemaking. The outcome is that shared beliefs and perceptions about information security are developed among organizational members but multiple and different behaviors also emerge among groups of organizational members. This is the role of organizational culture in achieving both centralization and decentralization (Weick, 1987), here in information security management. As organizational culture is about meaning making (Weick, 1987), it cultivates similar and uniformed perceptions and actions toward information security. Thus, common or standard behaviors are developed among organizational members. Yet, organizational culture also enables autonomy in interpretation, improvisation, and different actions (Weick, 1987), thereby leading to multiple but different ISBs.

Organizational culture is complicated. On the one hand, organizational culture represents a common set of beliefs and values shared by organizational members. Such a shared set of beliefs and values indicate that organizational members have reached a consensus on certain core values, which help to unify the whole organization. In this sense, organizational culture plays an important function of integrating various units or departments of an organization. This is the main idea of Martin's (2002) integration perspective on organizational culture. However, the common set of beliefs and values may not be shared equally among individual organizational members, groups, units, and departments in the organization. Further, despite the existence of an integrating organizational culture, subcultures are developed in various units, layers of organizational structure, and interest groups such as unions and management (Saffold, 1988). Development of multiple subcultures appears to be more the rule than an exception in organizations (Van Maanen & Barley, 1984). This differentiation view of organizational culture (Martin, 2002) suggests that organizational culture is not unitary (Saffold, 1988).

Both the integration and differentiation views are implicit in the competing values framework (CVF) of organizational culture (Cameron & Quinn, 2005; Quinn, 1988; Quinn & Rohrbaugh, 1983; Quinn & Spreitzer,1991). Further, the CVF recognizes both the complicated and diverse nature of organizational culture (Denison & Spreitzer, 1991). Moreover, the CVF has been used to enlighten empirical research on the relationship between organizational culture and effectiveness (Denison & Mishra 1995), including effectiveness in organizational control (Hartnell et al., 2011). Because of this, the CVF emerges to be an overarching framework for explaining the possible relationships between organizational culture and behavior control with regard to information security in organizations. The CVF consists of two dimensions---internal vs. external focus, and flexibility and discretion vs. stability and control. Along these two dimensions, four cultures are identified: group, hierarchical, developmental, and rational cultures, although the labels used to describe them differ from study to study. Group culture is an organization or a unit that emphasizes such values as positive working relationships, esprit de corps at work, social support, high morale, growth and development for individual members. Hierarchical culture refers to a place where values of rule control, formalization, efficiency, order, and productivity are highlighted. Developmental culture is one that promotes such values of creativity, exploration, learning, and knowledge generation. Lastly, rational culture is a place where values of customer service, productivity, and competitiveness are highlighted. We draw on the CVF framework to account for culture's role in ISB development.

ROLE OF ORGANIZATIONAL CULTURE IN ISB DEVELOPMENT

Group Culture

Group culture is internally oriented, but it emphasizes flexibility and discretion (Denison & Spreitzer, 1991). Highly endorsed group cultural values include cohesion, open communication, participation, and empowerment (Quinn & Kimberly, 1984). Sharing information, and praising performance are further characteristics of a group culture (O'Reilly, Chatman, & Caldwell, 1991). All these values tend to cultivate positive employee morale (Cameron & Ettington, 1988).

Flexibility and discretion suggest that organizations with a group culture favor measures that are highly adapted to situations with respect to information security. Further, in a group culture, employees feel empowered, and empowerment, compared to directive leadership, more likely stimulates task proficiency, and more importantly, proactivity (Martin, Liao, & Campbell, 2013). In the context of information security in organizations, given the difficulty for a security policy to cover exhaustively all areas of information security, such proactivity from employees is greatly needed, as that means that employees will proactively identify and report security concerns and issues and brainstorm for methods to address them. This helps to promote both information security diagnosing and solving behaviors. For example, in a cooperative cultural context, employees most likely exhibit positive ISBs such as *helping* and *voicing* behaviors (Hsu et al., 2015). Group cultural values also help to create a sense of collective ownership and responsibility among employees (Denison & Mishra, 1995), which are important drivers of uniformity in action towards what is commonly regarded. This suggests that employees in a group culture take it as their own responsibility and obligation to enact what they have already agreed on in information security issues. This will be reflected in uniformity in abiding by information security policies.

Group culture also has the potential in facilitating the antecedents of ISB. Organizationally desired ethics and moral foundations surrounding information security are more likely to be developed and promoted in a group culture than in any of the three other cultures. Such organizationally desired ethics and moral foundations are usually outcomes of employee social interactions facilitated by a group culture. Employees are most likely to identify with and internalize those ethics and moral foundations that they have participated in developing. Further, positive perceptions and attitudes among employees are also more likely to develop in a group culture. For example, voluntary participation, a central feature of group culture, positively links to perceptions and attitudes (Leana, Ahlbrandt, & Murrell, 1992). Empowerment, another main feature of group culture, leads to high level of employee commitment, and citizenship behaviors (Seibert, Wang, & Courtright, 2011; Spreitzer, 2008; Thomas & Velthouse, 1990), which help to cultivate those perceptions and attitudes among employees. Additionally, it can be argued that group culture helps to enhance acquisition of information security related knowledge and skills. From an information processing perspective, employees in a group culture are able to gather and use more information for their work (Turner & Makhija, 2012). An important outcome of active participation is increased practices in decision making, problem solving, and goal setting (Sashkin, 1976), which arguably help to build employees' knowledge and skills including information security awareness knowledge and how-to knowledge. Participation also results in learning through behavioral practice, which leads to skill enhancement (Sashkin, 1976).

The above discussion of how group culture would influence ISBs, especially the review of prior research showing how antecedents contribute to effective ISBs naturally lead to the following propositions:

Proposition 1-a: Group culture promotes information security diagnosing behaviors among employees more than any of the other three cultures.

Proposition 1-b: Group culture promotes information security solving behaviors.

Proposition 1-c: Group culture promotes information security performing behaviors.

Proposition 1-d: Group culture positively contributes to the development of all the three categories of ISB antecedents: ethics and morality, perceptions and attitudes, and knowledge and skills, more than any of the other three cultures.

Hierarchical Culture

Hierarchical culture is internally oriented and has a strong control mechanism in its organizational structure (Denison & Spreitzer, 1991). This culture emphasizes the following values: formal communication, routinization, and consistency (Quinn & Kimberly, 1984). These values stimulate rule compliance, process control, measurement, efficiency, timeliness, and smooth functioning (Hartnell et al., 2011). Employees from a hierarchical culture would be expected to follow rules and their roles would be clearly defined. They would value precise communication, task and process routinization, formalization of work and process, and consistency across units (Quinn & Kimberly, 1984).

In a hierarchical culture, information security policies would prescribe detailed rules, roles, and responsibilities for organizational members to follow, as that culture is rule, and control oriented. Hierarchical culture places priority on process control over human development and so would be more likely to implement technical procedures than to cultivate proactivity in employees to safeguard information security. However, because of formalization, organizations with a hierarchical culture would train their employees regarding their detailed information security policies. When undergoing the training sessions, employees are expected to be taught to have the same moral obligation, perceptions, and attitudes, and same level of knowledge and skills with regard to information security, as consistency and standardization require. Boss, Kirsch, Angermeier, Shingler, and Boss (2009) showed that mandatoriness mediates the relationship between organizational control measures for information security (specification of policies and rules, evaluation, and reward) and employees' ISB (taking precautions). Organizational control measures must be sufficient in hierarchical culture and mandatoriness is clearly communicated to employees.

ISB varies from organization to organization and from context to context. Given the highly contextualized nature, no specific ISB will be recommended as standard behavior. Instead, complying with information security policies will be deemed as a recommended behavior to end users. This is because organizational information security policies are formulated usually tailoring to their specific needs and requirements. In most cases, organizational information security policies define the roles and responsibilities for their employees regarding access to and use of organizational information and technology resources (Bulgurcu et al., 2010). These policies provide detailed descriptions of what employees can and cannot do with respect to accessing and using organizational information and technology resources (Whitman, 2008). The effectiveness of policy compliance by end users depends on how specific the organizational security policy is. This means that the policy's coverage of areas of information security and the corresponding security behaviors must be exhaustive. They have to cover all the areas of information security in the organization. It also means that the organizational policy has to specify each behavior for every area of information security. Specificity not only better informs employees of security behaviors but also enhances their belief that complying with organizational security policies is a must to them (Boss et al., 2009).

With respect to the antecedents of ISBs, hierarchical culture can positively contribute to the development of all the three categories. In a hierarchical culture, given top management's right assessment of the importance of information security to their company, together with their commitment to providing necessary resources, employees are likely to be trained or educated in a top-down manner to be ethically and morally alert to information security, heighten their perceptions and attitudes about information security, and enhance their information security knowledge and skills. In light of the above discussion, we propose the following propositions regarding the concepts of hierarchical culture and ISBs:

Proposition 2-a: Hierarchical culture promotes information security performing behaviors more than any of the other three cultures.

Proposition 2-b: Hierarchical culture positively contributes to the development of information security ethics and morality, perceptions and attitudes, and knowledge and skills.

Developmental Culture

The developmental culture is externally oriented and has a flexible organizational structure (Hartnell et al., 2011). They value growth, stimulation, variety, and autonomy (Quinn & Kimberly, 1984). More importantly, they encourage creativity and exploration. Their external orientation prepares them a sensitivity and keenness to external cues. When a new technology is developed and is demonstrating its potential, externally oriented developmental culture members would capture this new development and exhibit enthusiasm in importing this new technology to their own company. In a similar fashion, once a new method is developed outside their company to address information security issues associated with the new technology, employees with a strong external orientation are highly likely to adopt it. For the same reason, employees from a developmental culture have a strong readiness to interpret external cues occurring in the environment including updated solutions to information security problems. They are quick to take such newly introduced solutions to help to address their internal information security needs. For example, when an information security countermeasure portfolio was developed or updated (Kumar, Park, & Subramaniam, 2008), employees from a developmental culture would be very quick to recommend it to their organizations.

Developmental culture values a flexible organizational structure. When approaching technology, employees from this culture would focus on its technical function in terms of enhancing productivity, as opposed to those from a stability-oriented culture such as hierarchical and rational cultures who may like to explore its social and organizational functions of the technology such as facilitating coordination and control. For example, even though system development methodologies have production, coordination, and organizational control functions, IS developers from a developmental culture perceived them mainly as production technology, ignoring their coordination and organizational functions (Iivari & Huisman, 2007). Benefitted from their external learning inclination (Calantone, Cavusgil, & Zhao, 2002; Rauseo, 2001), employees are capable of seeking new ideas and information available in the external environment, and exploiting its internal resources to develop technical solutions to information security. Thus, employees from a developmental culture are more likely to display information security solving behaviors in coping with information security.

Indeed, among the four competing cultures, developmental culture has the strongest association with innovation (Buschgens, Bausch, & Balkin, 2013). In information security, their innovativeness would be highly likely to be reflected in developing new solutions to information security issues. Likewise, developmental culture cultivates proactiveness among its employees

(Brettel, Chomik, & Flatten, 2015). Their proactiveness would be demonstrated in foreseeing potential risks and threats to information security in technologies and other facilities adopted and used in their companies, and more importantly, in actively seeking measures to address such potential risks and threats. Developmental culture cultivates a risk-taking tendency in employees (Cooper, Edgett, & Kleinschmidt, 2004; McDonald, 2002; Miller & Friesen, 1982). Yet, this risk-taking spirit would be more shown in employees' experimenting with new measures for information security than in operating technology and equipment in their daily routine work processes.

With respect to the antecedents to ISBs, as developmental culture encourages its employees to engage in organizational learning and knowledge developing, it can be expected that they will constantly gain new knowledge and skills to deal with information security issues. Employees from this culture may be less likely to be bonded by moral obligation to try new things even though they may mean risks and threats to information security. And they are less likely to attach too much severity, vulnerability, and susceptibility in their perceptions to the possible risks and threats. However, given their pursuit of innovation and creative solutions to problems, they are more likely to acquire knowledge and skills needed to deal with risks and threats.

Thus, the following propositions can be posited:

Proposition 3-a: Developmental culture positively contributes to information security diagnosing behaviors.

Proposition 3-b: Developmental culture positively contributes to information security solving behaviors.

Proposition 3-c: Among the four cultures, developmental culture contributes to information security solving behaviors the most.

Proposition 3-d: Among the antecedents, developmental culture positively facilitates the knowledge and skill category.

Rational Culture

Similar to developmental culture, rational culture is also externally oriented (Denison & Spreitzer, 1991). Members from a rational culture also tend to develop a keen sensitivity to external cues. Rational culture also emphasizes such values as competitiveness, aggressiveness, productivity, achievement, and competence (Hartnell et al., 2011). When triggered by an external force, this achievement orientation may lead them to be highly concerned with information security. This external force is that their external customers raise such information security concerns about their products or services. To rational culture members, addressing customer needs and enhancing customer satisfaction with their products or services has a highest priority, as this translates into their achievement in the market (Cameron, Quinn, DeGraff, & Thakor, 2006). Because of this, members of a rational culture are sensitive to customers' information security concerns with their products or services. Moreover, they would speedily capture and send these customer feedback back to their companies. Doing this is comparable to identifying possible information security issues and problems inside the organization, i.e., diagnosing behaviors.

Further, rational culture is also positively related to innovativeness, proactiveness, and risk-taking (Brettel et al., 2015), cultural qualities that promote information security solving behaviors. Additionally, rational culture members are mostly result-oriented (Belassi, Kondra, & Tukel, 2007; Jaskyte, 2004). This orientation means an obsessive concern with present or direct results of an effort, which does not encourage exploration, a critical precedent to innovation. But their stability orientation favors a mechanism of organizational control, which is incompatible

with innovation. This suggests that employees of a rational culture may not exhibit as many information security solving behaviors as those of a developmental culture.

Rational culture's stability orientation translates into a preference of formal means of organizational control and adherence to existing rules and procedures (Buschgens et al., 2013). This suggests that employees of a rational culture agree with the practice of establishing rules, regulations, and policies to safeguard information security for their organizations. When risks, threats, and dangers of information security are well identified, and corresponding coping measures have been tested effective, employees of a rational culture would like to see them included in their organizational information security policies and regulations and exemplify themselves in abiding by these policies and regulations. Therefore, we can infer that rational culture promotes information security performing behaviors.

For the antecedents of ISBs, rational culture, as developmental culture does, may just promote the category of knowledge and skills. This is because rational culture does not take a strong stance on ethics and morality when it comes to information security. Rational culture, just as developmental culture, is more productivity and efficiency than sociality oriented. It may take a neutral position on ethics and morality. Neither does it encourage ethics and morality nor does it discourage them with respect to information security. As for the perceptions and attitude aspects of the antecedents, rational culture's role is subject to external influences, such as customers. Based on this discussion of rational culture's characteristics, the following propositions can be generated:

Proposition 4-a: Rational culture positively contributes to information security diagnosing behaviors.

Proposition 4-b: Rational culture positively contributes to information security solving behaviors.

Proposition 4-c: Rational culture is more positively related to information security diagnosing behaviors than solving behaviors.

Proposition 4-d: Rational culture positively contributes to information security performing behaviors.

Proposition 4-e: Rational culture positively promotes the knowledge and skills category of the ISB antecedents.

DISCUSSION

The landscape of past research on ISB was dominated by the deterrence approach, which focused its attention on examining negative behaviors such as computer abuse (Willison & Warkentin, 2013). Past research also utilized a number of social cognitive theories, including reasoned action (e.g., see Pahnila, Siponen, & Mahomood, 2007), protection motivation (e.g., see Herath & Rao, 2009; Johnston & Warketin, 2010; Lee & Larsen, 2009), planned behavior (e.g., see Bulgurcu et al., 2010; Herath & Rao, 2009), and moral judgment and ethics (e.g., see Banerjee et al., 1998; Myyry et al., 2009), to explore a series of precursors to ISB but mostly investigated their impact on information security policy compliance only. These two approaches led to an under-exploration of other types of, especially positive ISBs (Posey et al., 2013). To help information security research to navigate out of this impasse, this study proposed the TDISB that integrates sensemaking and organizational culture for studying ISBs. Offering this new theoretical framework, the current study generated significant contributions to ISB research.

The main contribution of this study is that it has extended and advanced our understanding and knowledge of ISBs. Drawing on the organizational sensemaking perspective (Weick, 1979, 1995), this study generated three new categories of ISBs – information security diagnosing behavior, information security solving behavior, and information security performing behavior. Past research explored a number of individual cognitive factors impacting ISB, but treated ISB mostly as a dependent variable. Because of this research design, previous research only shed light on just a few negative ISBs such as computer abuse. A large number of empirical studies conceptualized ISB only as information security policy compliance (e.g., see Bulgurcu et al., 2010; Herath & Rao, 2009; Myyry et al., 2009; Siponen & Vance, 2010; Son, 2011). By offering the three above mentioned categories of ISB, this study adds more specificity and granularity to our knowledge of ISBs. With the development of these three categories of ISB, this study provided benefits to organizations regarding how organizations can assess and influence such ISBs (Stanton, Stam, Mastrangelo, & Jolton, 2005).

Another contribution of this study is that it provided a theoretical lens for examining the organizational role in the development of ISBs. Past research, although occasionally examined organizational efforts such as training (Puhakainen & Siponen, 2010) in improving employees' ISBs, mostly focused on investigating individual factors such as cognition (e.g., see Bulgurcu et al., 2010) and ethics (Siponen & Vance, 2010). Yet, these individual factors are impacted by the organizational context and thus should be examined in this context. By offering the TDISB, this study provides an important direction for researchers to examine ISBs, i.e., to explore the organizational role in the development of these behaviors. This new theoretical framework helps to extend past research by showing how individual cognition (scanning and interpreting) operates in and thereby is constrained and conditioned by the organizational cultural context. This study showed that ISBs are outcomes of sensemaking that is both facilitated and constrained by organizational culture. More importantly, this study advanced our understanding of how culture shapes ISBs in that it offered detailed explanation as to why a same ISB may be positively developed in diverse organizational cultures. For example, the information security diagnosing behavior was shown to emerge in all the four types of culture but was promoted differently in those cultures. Further, incentives, resources, or approaches used in generating the information security solving behavior were shown to be different in, for example, developmental culture and rational culture. Given these benefits, this study helped to overcome limitations in past research that only showed that organizational culture may impact information security policy compliance by individuals.

A third contribution of this study is that it challenged an important underlying assumption of past research especially the deterrence approach. Excessively showing the negative ISBs in past research would help to cultivate a biased view that internal employees constitute a threat to information security. By offering the three categories of ISBs especially the diagnosing and solving behaviors, this study helped to re-image the role of employees as beneficial contributors to information security management in their organizations. It also generated an important implication that employees can be looked as the solution instead of the problem even in the area of information security management (Spears & Barki, 2010).

In addition to the theoretical contributions, this study generated important practical implications for organizations. When making decisions on what approaches to information security control, organizations should assess their cultures first and then adopt approaches that fit their cultures. From the integration and differentiation perspective of organizational culture (Martin, 2002), an organization may have several subcultures existing simultaneously within their organizational boundaries. In this case, adopting an organization wide one-fitting-all information security

approach may not be appropriate. Instead, multiple approaches with each fitting its subculture can be adopted. Even in organizations that are overwhelmingly hierarchical in culture, some small participative conclaves can develop among groups or units, which can serve positively their organizations in information security management, as those subcultures would help to promote different but beneficial types of ISBs. For research direction, future research can seek empirical evidence for the theoretical propositions outlined in this study.

REFERENCES

Abbasi, A., Zahedi, F. M., Zeng, D., Chen, Y., Chen, H., & Nunamaker, J. F. 2015. Enhancing predictive analytics for anti-phishing by exploiting website genre information. *Journal of Management Information Systems,* 31(4), 109-157.

Abolafia, M. Y. 2010. Narrative construction as sensemaking: How a central bank thinks. *Organization Studies*, 31, 349–367.

Agarwal, R., & Prasad, J. 1998. A conceptual and operational definition of personal innovativeness in the domain of information technology. *Information Systems Research,* 9(2), 204-215.

Anderson, C., & Agarwal, R. 2010. Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions, *MIS Quarterly*, 34(3): 613-643.

Aytes, K., & Connolly, T. 2004. Computer security and risky computing practices: A rational choice perspective. *Journal of Organizational and End User Computing,* 16(3): 22-40.

Balogun, J., & Johnson, G. 2004. Organizational restructuring and middle manager sensemaking. *Academy of Management Journal,* 47, 523-549.

Balogun, J., and Johnson, G. 2005. From intended strategies to unintended outcomes: The impact of change recipient sensemaking. *Organization Studies,* 26, 1573-1601.

Banerjee, D., Cronan, T. P., & Jones, T. W. 1998. Modeling IT ethics: A study in situational ethics. *MIS Quarterly*, 22(1): 31-60.

Barr, P. S., & Huff, A. S. 1997. Seeing isn't believing: Understanding diversity in the timing of strategic response. *Journal of Management Studies,* 34, 337–370.

Belassi,W.,A. Z. Kondra, & O. I. Tukel. 2007. New product development projects: The effect of organizational culture. *Project Management Journal,* 38(4), 12–24.

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

Bowman, E. H., & Hurry, D. 1993. Strategy through the option lens: An integrated view of resource investments and the incremental choice process. *Academy of Management Review,* 18(4), 760–782.

Brettel, M., Chomik, C., & Flatten, T. C. 2015. How organizational culture influences innovativeness, proactiveness, and risk-taking, fostering entrepreneurial orientation in SMEs. *Journal of Small Business Management,* 53(4), 868-885.

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

Buschgens, T., Bausch, A., & Balkin, D. B. 2013. Organizational culture and innovation: A meta-analytic review. *Journal of Product Innovation Management,* 30(4), 763-781.

Calantone, R. J., Cavusgil, S. T., & Zhao, Y. 2002. Learning orientation, firm innovation capability, and firm performance. *Industrial Marketing Management,* 31, 515–24.

Caliendo, M., Clement, M., Papies, D., & Scheel-Kopeinig, S. 2012. The cost impact of spam filters: Measuring the effect of information system technologies in organizations. *Information Systems Research,* 23, 1068-1080.

Cameron, K. S., & Ettington, D. R. 1988. The conceptual foundations of organizational culture. In J. Smart (Ed.), *Higher education handbook of theory and research:* 356–396. New York, NY: Agathon Press.

Cameron, K. S., & Quinn, R. E. 2005. *Diagnosing and changing organizational culture*. San Francisco, CA: Jossey-Bass.

Cameron, K. S., Quinn, R. E., DeGraff, J., & Thakor, A. V. 2006. *Competing values leadership: Creating value in organizations.* Northampton, MA: Elgar.

Carroll, J. S., Rudolph, J. W., & Hatakenaka, S. 2002. Learning from experience in high-hazard industries. *Research in Organizational Behavior,* 24, 87-137.

Chatterjee, S., Sarker, S., & Valacich, J. 2015. The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems,* 31(4), 49-87.

Cooper, R. G., S. J. Edgett, & E. J. Kleinschmidt. 2004. Benchmarking best NPD practices. *Research Technology Management,* 47(1), 31–43.

Croker, L. 1987. Improvements in database concurrency control with locking. *Journal of Management Information Systems,* 4(2), 74-92.

Culnan, M. J., Foxman, E. R., & Ray, A. W. 2008. Why IT executives should help employees secure their home computers. *MIS Quarterly Executive*, 7(1): 49-56.

Culnan, M., & Williams, C. C. 2009. How ethics can enhance organizational privacy: Lessons from the Choice Point and TJX data breaches. *MIS Quarterly,* 33(4): 673-687.

D'Arcy, J., & Herath, T. 2011. A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems,* 20: 643-658.

Da Veiga, A., and Eloff, J. H. P. 2010. A framework and assessment instrument for information security culture. *Computers and Security,* 29, 196-207.

Daft, R. L., & Weick, K. E. 1984. Toward a model of organizations as interpretation systems. *Academy of Management Review,* 9, 284–295.

Denison, D. R., & Mishra, A. K. 1995. Toward a theory of organizational culture and effectiveness. *Organization Science,* 6(2): 204-223.

Denison, D. R., & Spreitzer, G. M. 1991. Organizational culture and organizational development: A competing values approach. In R. W. Woodman & W. A. Pasmore (Eds.), *Research in organizational change and development:* 1-21. Greenwich, CT: JAI Press.

Detert, J, Schroeder, R, and Mauriel J. 2000. A framework for linking culture and improvement initiatives in organisations. *Academy of Management Review,* 25, 850–63.

Dinev, T., Goo, J., Hu, Q., & Nam, K. 2009. User behaviour towards protective information technologies: The role of national cultural differences. *Information Systems Journal,* 9(4): 391–412.

Dutton, J. E., & Dukerich, J. M. 1991. Keeping an eye on the mirror: Image and identity in organizational adaptation. *Academy of Management Journal,* 34, 517-554.

Einhorn, H. J., & Hogarth, R. M. 1986. Judging probable cause. *Psychological Bulletin,* 99(1), 3-19.

Eisenhardt, K. M. 1989. Making fast strategic decisions in high-velocity environments. *Academy of Management Journal,* 32, 543-576.

Fulk, J. 1993. Social construction of communication technology. *Academy of Management Journal,* 36(5), 921-950.

Furnell, S. 2008. End-user security culture: A lesson that will never be learnt? *Computer Fraud & Security,* 4: 6-9.

Gephart, R. P. 1993. The textual approach: Risk and blame in disaster sensemaking. *Academy of Management Journal,* 36(6), 1465-1514.

Gibbs, J. P. 1975. *Crime, punishment, and deterrence.* NY: Elsevier.

Gopal, A., & Prasad, P. 2000. Understanding GDSS in symbolic context: Shifting the focus from technology to interaction. *MIS Quarterly,* 24, 509-546.

Griffith, T. L. 199). Technology features as triggers for sensemaking. *Academy of Management Review,* 24(3), 472-488.

Guo, K. H., Yuan, Y., Archer, N. P., Connelly, C. E. 2011. Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, 28(2): 203-236.

Hahn, T., Preuss, L., Pinkse, J., & Figge, F. 2015. Cognitive frames in corporate sustainability: Managerial sensemaking with paradoxical and business case frames. *Academy of Management Review,* 4015 (1), 18-42.

Harrington, S. 1996. The effects of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly,* 20(3): 257-278.

Harris, S. G. 1994. Organizational culture and individual sensemaking: A schema-based perspective. *Organization Science,* 5(3), 309-321.

Hartnell, C. A., Ou, A. Y., & Kinicki, A. 2011. Organizational culture and organizational effectiveness: A meta-analytic investigation of the competing values framework's theoretical suppositions. *Journal of Applied Psychology,* 96(4): 677-694.

Herath, T., & Rao, H. R. 2009a. Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems,* 18(2): 106–125.

Herath, T., & Rao, H. R. 2009b. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems,* 47(2): 154–165.

Hovav, A., & D'Arcy, J. 2012. Appling an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information & Management,* 49: 99-110.

Hsu, C., Lee, J-N., & Straub, D. W. 2012. Institutional influences on information systems security innovations. *Information Systems Research,* 23(3), 918-939.

Hsu, J. S., Shih, S., Hung, Y. W., & Lowry, P. B. 2015. The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research,* 26(2), 282-300.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. 2012. Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences,* 43(4): 615-659.

Hu, Q., Hart, P., & Cooke, D. 2006. The role of external influences on organizational information security practices: An institutional perspective. *Proceedings of the 39th Hawaii International Conference on System Sciences.* Los Alamitos, CA: IEEE Computer Society Press.

Hu, Q., Hart, P., & Cooke, D. 2007. The role of external and internal influences on information systems security – A neo-institutional perspective. *Journal of Strategic Information Systems,* 16, 153-172.

Iivari, J., & Huisman, M. 2007. The relationship between organizational culture and the deployment of systems development methodologies. *MIS Quarterly,* 31(1), 35-58.

Jaskyte, K. 2004. Transformational leadership, organizational culture, and innovativeness in nonprofit organizations. *Nonprofit Management and Leadership,* 15(2), 53–68.

Johnston, A. C., & Warkentin, M. 2010. Fear appeals and information security behaviors: An empirical study. *MIS Quarterly,* 34(3): 548-566.

Katos, V., & Adams, C. 2005. Modelling corporate wireless security and privacy. *Journal of Strategic Information Systems,* 14, 307-321.

Kim, S. H., & Kim, B. C. 2014. Differential effects of prior experience on the malware resolution process. *MIS Quarterly,* 38(3), 655-678.

Klein, G., Pliske, R., Crandall, B., & Woods, D. 2005. Problem detection. *Cognition, Technology and Work,* 7, 14-28.

Kraemer, S., & Carayon, P. 2005. Computer and information security culture: Findings from two studies. *Proceedings of the Human Factors and Ergonomics Society 49th Annual Meeting*. Computer Society Press.

Kumar, R. L., Park, S., & Subramaniam, C. 2008. Understanding the value of countermeasure portfolios in information systems security. *Journal of Management Information Systems,* 25(2), 241-279.

LaRose, R., Rifon, N. J., & Enbody, R. 2008. Promoting personal responsibility for Internet safety. *Communications of the ACM,* 51(3): 71-76.

Leana, C., Ahlbrandt, R. S., & Murrell, A. J. 1992. The effects of employee involvement programs on unionized workers' attitudes, perceptions, and preferences in decision making. *Academy of Management Journal,* 35(4): 861-873.

Lee, J., & Y. Lee. 2002. A holistic model of computer abuse within organizations. *Information Management Computer Security,* 10(2): 57–63.

Lee, S. M., Lee, S. G., & Yoo, S. 2004. An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management,* 41(6): 707–718.

Lee, Y., & Kozar, K. A. 2005. Investigating factors affecting the adoption of anti-spyware system. *Communications of the ACM*, 48(8): 72-77.

Lee, Y., & Larsen, K. R. 2009. Threat or coping appraisal: Determinants of SMB executives'decision to adopt anti-malware software. *European Journal of Information Systems,* 18: 177-187.

Li, H., Zhang, J., & Sarathy, R. 2010. Understanding compliance with Internet use policy from the perspective of rational choice theory. *Decision Support Systems,* 48: 635-645.

Maitlis, S. 2005. The social processes of organizational sensemaking. *Academy of Management Journal,* 48(1), 21-49.

Maitlis, S., & Christianson, M. 2014. Sensemaking in organizations: Taking stock and moving forward. *The Academy of Management Annals,* 8(1), 57-125.

Malsch, B., Tremblay, M. S., & Gendron, Y. 2012. Sense-making in compensation committees: A cultural theory perspective. *Organization Studies*, 33, 389–421.

March, J. G. 1991. Exploration and exploitation in organizational learning. *Organization Science,* 2(1), 71-87.

Martin, J. 2002. *Organizational culture: Mapping the terrain*. Thousand Oaks, CA: Sage Publications.

Martin, S., Liao, H., & Campbell, E. M. 2013. Directive versus empowering leadership: A field experiment comparing impacts on task proficiency and proactivity. *Academy of Management Journal,* 56(5): 1372-1395.

McDonald, R. E. 2002. *Knowledge entrepreneurship: Linking organizational learning and innovation*. Ann Arbor, MI: ProQuest Information and Learning.

Miller, D., & P. H. Friesen. 1982. Innovation in conservative and entrepreneurial firms: Two models of strategic momentum. *Strategic Management Journal,* 3, 1–25.

Moore, G. C., and Benbasat, I. 1991. Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research,* 2(3), 192-222.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance A. 2009. What levels of moral reasoning and values explain adherence to information security rules? An empirical study.

Ng, B. Y., Kankanhalli, A., & Xu, Y. 2009. Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, 46: 815-825.

O'Reilly, C. A., & Chatman, J. A. 1996. Culture as social control: Corporations, cults, and commitment. *Research in Organizational Behavior,* 18: 157-200.

O'Reilly, C. A., Chatman, J., & Caldwell, D. F. 1991. People and organizational culture: A profile comparison approach to assessing person-organization fit. *Academy of Management Journal,* 34(3): 487-516.

Orton, J. D. 2000. Enactment, sensemaking and decision making: Redesign processes in the 1076 reorganization of US Intelligence. *Journal of Management Studies,* 37(2), 213-234.

Ouchi, W. G. 1980. Markets, bureaucracies, and clans. *Administrative Science Quarterly,* 25, 129-141.

Pahnila, S., Siponen, M., & Mahmood, A. 2007. Employees' behavior towards IS security policy compliance. *Proceedings of the 40th Hawaii International Conference on System Sciences*, January 3-6, Los Alamitos, CA: IEEE Computer Society Press.

Porac, J. F., & Thomas, H. 2002. Managing cognition and strategy: Issues, trends and future directions. In A. M. Pettigrew, H. Thomas, & R. Whittington (Eds.), *Handbook of strategy and management:* 165–181. London & Thousand Oaks, CA: Sage.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. 2013. Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly,* 37(4): 1189-1210.

Puhakainen, P., & Siponen, M. 2010. Improving employees' compliance through information security training: An action research study. *MIS Quarterly,* 34(4), 757-778.

Quinn, R. E. 1988. *Beyond rational management*. San Francisco, CA: Jossey-Bass.

Quinn, R. E., & Kimberly, J. R. 1984. Paradox, planning, and perseverance: Guidelines for managerial practice. In J. R. Kimberly & R. E. Quinn (Eds.), *Managing organizational transitions:* 295–313. Homewood, IL: Dow Jones–Irwin.

Quinn, R. E., & Rohrbaugh, J. 1983. A spatial model of effectiveness criteria: Toward a competing values approach to organizational analysis. *Management Science,* 29: 363-377.

Quinn, R. E., & Spreitzer, G. M. 1991. The psychometrics of the competing values culture instrument and an analysis of the impact of organization culture on quality of life. *Research in Organizational Change and Development,* 5: 115-142.

Rauseo, N. A. 2001. *E-Business as a Radical Innovation: The effect of Organizational Capabilities on its Adoption in Brick and Mortar Companies*. Ann Arbor, MI: ProQuest Information and Learning.

Ray, C. A. 1986. Corporate culture: The last frontier of control. *Journal of Management Studies,* 23, 287-297.

Repenning, N. P., & Sterman, J. D. 2002. Capability traps and self-confirming attribution errors in the dynamics of process improvement. *Administrative Science Quarterly,* 47, 265-295.

Rudolph, J. W., Morrison, J. B., & Carroll, J. S. 2009. The dynamics of action-oriented problem solving: Linking interpretation and choice. *Academy of Management Review,* 34(4), 733-756.

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

Saffold, G. S. 1988. Culture traits, strength, and organizational performance: Moving beyond "strong" culture. *Academy of Management Review,* 13(4): 546-558.

Sashkin, M. 1976. Changing toward participative management approaches: A model and methods. *Academy of Management Review,* 1(3): 75-86.

Schein, E. H. 1985. *Organizational culture and leadership.* San Francisco: Jossey-Bass.

Seibert, S. E., Wang, G., & Courtright, S. H. 2011. Antecedents and consequences of psychological and team empowerment in organizations: A meta-analytic review. *Journal of Applied Psychology,* 96: 981-1003.

Sen, R., & Borle, S. 2015. Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems,* 32(1), 314-341.

Siponen, M., & Vance, A. 2010. Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly,* 34(3), 487-502.

Siponen, M., Willison, R, & Baskerville, R. 2008. Power and practice in information systems security research. In *Proceedings of the International Conference on Information Systems,* 14-17, Paris, France.

Son, J. 2011. Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management,* 48: 296-302.

Spears, J. L., & Barki, H. 2010. User participation in information systems security risk management. *MIS Quarterly*, 34(3), 503-522.

Spreitzer, G. M. 2008. Taking stock: A review of more than twenty years of research on empowerment at work. In J. Barling & C. L. Cooper (Eds.), *The Sage handbook of organizational behavior:* 73-88. Thousand Oaks, CA: Sage.

Stanton, J. M. and Stam, K. R. 2006. The visible employee. Medford, NJ: Information Today Inc.

Stanton, K. M., Stam, K. R., Mastrangelo, P., & Jolton, J. 2005. Analysis of end user security behaviors. *Computers & Security,* 24, 124-133.

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal, 18 (7)*, 509-533.

Thomas, J. B., Clark, S. M., and Gioia, D. A. 1993. Strategic sensemaking and organizational performance: Linkages among scanning, interpretation, action and outcomes. *Academy of Management Journal,* 36(2), 239-270.

Thomas, K. W., & Velthouse, B. A. 1990. Cognitive elements of empowerment: An "interpretive" model of intrinsic task motivation. *Academy of Management Review,* 15: 666-681.

Trice, H. M., & Beyer, J. M. 1993. *The cultures of work organizations.* Englewood Cliffs, NJ: Prentice-Hall.

Turner, K. L., & Makhija, M. V. 2012. The role of individuals in the information processing perspective. *Strategic Management Journal,* 33: 661-680.

Vaast, E. 2007. Danger in the eye of the beholders: Social representations of information systems security in healthcare. *Journal of Strategic Information Systems,* 16, 130-152.

Vaast, E., & Walsham, G. 2005. Representations and actions: The transformation of work practices with IT use. *Information and Organization,* 15, 65-89.

Van Maanen, J., & Barley, S. 1984. Occupational communities: Culture and control in Organizations, in B. M. Staw and L. L. Cummings (eds.), *Research in organizational behavior,* pp. 287-365, Greenwich, CT: JAI Press.

Van Niekerk, J. F., & Von Solms, R. 2010. Information security culture: A management perspective. *Computers & Security,* 29: 476-486.

Vance, A., Lowry, P. B., and Eggett, D. 2015. Increasing accountability through user-interface design artifacts: A New approach to addressing the problem of access-policy violations. *MIS Quarterly,* 39(2), 345-366.

Vance, A., Siponen, M., & Pahnila, S. 2012. Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, 49: 190-198.

Vlaar, P. W., Van den Bosch, F. A., & Volberda, H. W. 2006. Coping with problems of understanding in interorganizational relationships: Using formalization as a means to make sense. *Organization Studies*, 27, 1617–1638.

Vroom, C., and von Solms, R. 2004. Towards information security behavioral compliance. *Computers & Security,* 23, 191-198.

Walsham, G. 1998. IT and changing professional identity: Micro studies and macro theory. *Journal of the American Society for Information Science,* 49(12), 1081- 1089.

Warkentin, M., & Willison, R. 2009. Behavioral and policy issues in information systems security: The inside threat. *European Journal of Information Systems,* 18: 101-105.

Weber, K., and Glynn, M. A. 2006. Making sense with institutions: Context, thought and action in Karl Weick's Theory. *Organization Studies,* 27, 1639-1660.

Weick, K. 1979. *The social psychology of organizing*. Reading, MA: Addison-Wesley.

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

Weick, K. E. 1990. Technology as equivoque: Sensemaking in new technologies in P. S. Goodman & L. S. Sproull (Eds.), *Technology and organizations* (pp. 1-44). San Francisco: Josey Bass Publishers.

Weick, K. E. 1993. The collapse of sensemaking in organizations: The Mann Gulch disaster. *Administrative Science Quarterly,* 38*,* 628-652.

Weick, K. E. 1995. *Sensemaking in organizations*. Newbury Park, CA: Sage.

Weick, K. E., Sutcliffe, K. M., and Obstfeld, D. 2005. Organizing and the process of sensemaking. *Organization Science,* 16(4), 409-425.

Whitman, M. E. 2004. In defense of the realm: Understanding threats to information security. *International Journal of Information Management,* 24: 43-57.

Whitman, M. E. 2008. Security policy: From design to maintenance. In D. W. Straub, S. Goodman, & R. L. Baskerville (Eds.), *Information security: Policy, processes, and practices:* 123-151. Armonk, NY: M. E. Sharpe, Inc.

Willison, R., & Warkentin, M. 2013. Beyond D\deterrence: An expanded view of employee computer abuse. *MIS Quarterly,* 37(1), 1-20.

Woon, I. M. Y., Tan, G. W., & Low, R. T. 2005. A protection motivation theory approach to home wireless security. In D. Avison, D. Galletta, & J. I. DeGross (Eds.), *Proceedings of the 26th International Conference on Information Systems*: 367-380. December 11-14, Las Vegas, NV, USA.

Workman, M., Bommer, W., & Straub, D. 2008. Security lapses and the omission of information security measures: An empirical test of the threat control model. *Journal of Computers in Human Behavior*, 24(6): 2799-2816.

Wright, R., T., & Marett, K. 2010. The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems*, 27(1): 273-303.

Xu, H., Wang, H., & Teo, H.-H. 2005. Predicting the usage of P2P sharing software: The role of trust and perceived risk. In R.H. Sprague (Ed.), *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, Los Alamitos, CA: IEEE.