SENSEMAKING AND INFORMATION SECURITY BEHAVIORS

ABSTRACT

Past research overwhelmingly focused on examining negative information security behaviors but overlooked employees' potential in positively contributing to information security. To fill this research gap, this study attempts to build a framework that draws on the conceptual gist of organizational sensemaking to show the dynamic nature of information security behavior. This study then situates the development of such dynamic information security behaviors in the context of organizational culture and proposes how organizational culture shapes these behaviors. Possible contributions of this framework and future research directions are also discussed.

Keywords: Sensemaking, Information security behavior, Information security diagnosing behavior, Information security forming behavior, 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). Internal employees are therefore viewed as the weakest link for information security in organizations (Mitnick & Simon, 2002; Warkentin & Wilson, 2009). It is mandatory for organizations to take measures to curb such negative behaviors (Chen, Ramanurthy, & Wen, 2013). One such organizational measure is to develop and enforce organizational information security policies (ISPs) that help to govern employees' information security behavior (ISB) (Bulgurcu, Cavusoglu, & Benbasat, 2010; Siponen & Vance, 2010). In most cases, these policies define the roles and responsibilities for their employees regarding access and use of organizational information and technology resources (Bulgurcu et al., 2010). These roles and responsibilities are usually performed by employees via their behaviors. In this sense, employees' compliance with their organizational ISPs can help to reduce significantly the number of negative behaviors (Hu, Dinev, Hart, & Cooke, 2012).

While using policies to execute prevention of negative behaviors, organizations should not overlook a possibility that their employees are resources for information security (Posey et al., 2013; Spears & Barki, 2010). Employees have a great potential in contributing to organizational success via their positive behaviors (Brief & Motowidlo, 1986; George & Brief, 1992; Graham, 1991; Organ, 1988). These positive behaviors can emerge in any contextual domain (Parker, Williams, & Turner, 2006), which would certainly include information security management. For example, employees can participate in generating ideas about how to enhance information security and seeking solutions to security problems (Posey et al., 2013). Even in the area of prevention of negative behaviors, employees can play an important role. More specifically, organizational ISPs define employees' roles and responsibilities mostly based on employees' past and current use of information and technology assets (Orlikowski, 2000). In other words, employees' experiences with the use of organizational information and technology assets provide a site for the development of those roles and responsibilities. As a process of learning, employees' assess to and use of newly adopted and implemented information and technology resources are experiential and exploratory in nature (Gallivan, Spitler, & Koufaris, 2005). Some practices in the exploratory process may not be perceived as negative until employees become aware of, understand, and realize their negativity such as risk, danger, and threat to information security in their interactions with technology (Bulgurcu et al., 2010;

D'Arcy & Herath, 2011). Only when agreement among employees is reached about their negativity such practices would be defined in the policies as negative behaviors that should be prevented. In this sense, formulating information security rules and policies relies on employees' collective perception and interpretation about information security management in the context of technology adoption and implementation (Stahl, Doherty, & Shaw, 2012). Technology adoption and implementation is a dynamic process, which consists of identifiable phases where employees perceive and interpret their technologies differently (Hsiao, Wu, & Hou, 2008). Thus, diverse behaviors may develop, consistent with their different perceptions and interpretations of technology at the phases.

In this study, we attempt to open up new fronts in ISB research by taking an integrative theoretical approach to exploring employees' diverse behaviors in managing information security. We use one research question to guide our exploration: 1). What behaviors do employees exhibit in managing information security at different phases of their interactions with information and technology resources? To answer this question, we draw on the dynamic capabilities perspective (Teece, Pisano, & Shuen, 1997) and organizational sensemaking literature to articulate a theory of dynamic information security behaviors (TDISB). In doing that, we plan to contribute to the ISB literature by proposing a new theoretical framework that enables investigation of organizational dynamics as a central force cultivating and shaping ISBs, and understanding employees as contributors to information security management. This major contribution is reflected in the following objectives.

First, this study aims to extend and enrich our understanding of ISBs by conceptualizing some new categories of ISBs. 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, thus representing a heightened and extended understanding of ISBs. Second, this study seeks to provide further insight into the development of ISBs. Past research mostly examined some individual factors that contribute to the development of negative ISBs and ISP compliance. Seond, as past research overwhelmingly focused on negative ISBs, an undesirable outcome was that individual employees' potential in positively contributing to information security management in their organizations has not been well explored. In delineating the various ISBs included in the new taxonomy, this study hopes to 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 is based on sensemaking 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. Lastly, we will discuss contributions of our framework, its possible implications for organizational practice, and future research directions.

INFORMATION SECURITY BEHAVIOR

As internal employees' misbehaviors constitute a great threat to organizational information security (D'Arcy et al., 2009; Warkentin &Willison, 2009), IS researchers have examined possible factors that influence employees' ISB and searched for effective means to control it. A review of the ISB research literature shows that, to date, a significant number of behavior theories have been adopted to study ISBs (see Appendix A). 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. Besides the deterrence theory, the deterrence approach also uses other theories such as fear appeal (Johnston &

Appendix A: Major Information Security Behaviors and Theories in IS Research

Behavior	Theory	Representative Studies
Negative behaviors:		
• Misuse or abuse of IS resources	Deterrence	Reviewed in D'Arcy & Herath, 2011; Siponen, Willison, & Baskerville, 2008
• Security policy violation, policy noncompliance, and/or policy compliance	Deterrence, rational choice, reasoned action, planned behavior, neutralization, coping, moral disengagement, self-control, personal and situational factors, fear appeal, control and reactance, moral reasoning, accountability, norm activation	Bulgurcu et al., 2010; D'Arcy, Herath, & Shoss, 2014; Guo et al., 2011; Herath & Rao, 2009; Hu, West, & Smarandescu, 2015; Johnston et al., 2016; Johnston, Warkentin, & Siponen, 2015; Lowry & Moody, 2015; Myyry et al., 2009; Siponen & Vance, 2010; Tsohou, Karyda, & Kokolakis, 2015; Vance et al., 2012; Vance, Lowry, & Eggett, 2015; Willison & Warkentin, 2013; and Yazdanmehr & Wang, 2016
Positive behaviors:		
• Intent to use anti-spyware software	Fear appeal, planned behavior	Johnston & Warkentin 2010; Lee & Kozar, 2005
• Adopting and updating protective technologies	Protection motivation, reasoned action	Boss et al., 2015; Lee & Larsen, 2009; Shropshire, Warkentin, & Sharma, 2015
• Coping with phishing	Channel expansion, disposition	Wright & Marett, 2010
• Habitual information or computer protection behavior	Control, fear appeal, protection motivation, protection motivation, elaboration likelihood, and	Boss et al., 2009; Boss et al., 2015; Larose, Rifon, & Enbody, 2008; Ng et al., 2009

	social cognitive, expectancy-value	
• Protection-motivated behaviors	Protection motivation	Posey et al., 2013; Warkentin et al., 2016
• Extra-role behaviors	Social control, formal control	Hsu et al., 2015

Warkentin, 2010; Warkentin et al., 2016), opportunities (Padayachee, 2016), and routine activity theories (Wang, Gupta, & Rao, 2015). 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. The deterrence studies highlighted some negative behaviors such as misuse or abuse of IS resources (e.g., see D'Arcy et al., 2009, and Straub, 1990). Further, these negative behaviors were attributed to neutralization (Siponen & Vance, 2010), subjective norms and perceived behavioral control (Djajadikerta, Roni, & Trireksani, 2015), weak ethics and moral beliefs (Banerjee et al., 1998), and weak organizational trust and ineffective organizational communication (Lowry et al., 2015). Most importantly, however, these deterrence studies tended to treat noncompliance of organizational ISPs as a root cause of these negative behaviors, and therefore began to be concerned with how to effectively enhance policy compliance (D'Arcy & Herath, 2011).

This major concern was then quickly taken over by numerous studies that used other behavior theories to examine information security. These other behavior theories include, but not limited to, the theories of ethical/moral behavior (e.g., Banerjee et al. 1998; Culnan & Williams, 2009; Harrington, 1996; Myyry et al., 2009), reactance (Lowry & Moody, 2015; Lowry et al., 2015), coping (D'Arcy, Herath, & Shoss, 2014), 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), and protection motivation (Boss et al., 2015; Ng, Kankanhalli, & Xu, 2009; Herath & Rao, 2009a; Pahnila, Siponen, & Mahmood, 2007; Warkentin et al., 2016). The empirical studies that used the other behavior theories then sought to explore antecedents that can help to enhance organizational ISPC. Antecedents that were examined in these studies include 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 (see Appendix B). These antecedents were investigated as predictors of ISB, mostly ISPC.

Appendix B: Antecedents of Information Security Behaviors in IS Research

Antecedent	Representative Studies
Ethics/morality	Lee & Kozar, 2005; D'Arcy & Herath, 2011
Perceptions and Attitudes	
• Information security related perceptions of:	
• security risk	Guo et al., 2011; Wang, Xiao, & Rao, 2015; Wright & Marett, 2010; and Xu, Wang, & Teo, 2005
• risk or threat severity, computer or information systems' vulnerability	LaRose, Rifon, & Enbody, 2008; Lee & Larsen, 2009; Ng et al., 2009; Workman, Bommer, & Straub, 2008

and susceptibility to risks and threats	
• possible benefits of coping behavior such as response efficacy	Johnston & Warkentin, 2010; LaRose et al., 2008; Lee & Larsen, 2009; Woon, Tan, & Low, 2005
• control of information	Hajli & Lin, 2016
• security behavior effectiveness	Anderson & Agarwal, 2010; Culnan, Foxman, & Ray, 2008; Ng et al., 2009
• Attitude toward security-related behavior	Anderson & Agarwal, 2010; Johnston et al. 2016
Knowledge and skills	
• 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
• 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

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 & Herath, 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; Chiu, Chau, & So, 2015; 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; Wang, Xiao, & Rao, 2015; 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), control of information (Hajli & Lin, 2016), 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; Johnston et al. 2016), which then leads to security behavior (Guo et al, 2011; Lee & Kozar, 2005). Further, dispositional factors such as personality traits and situational factors such as organizational sanctions shape these perceptions' impact on behavior intention (Johnston et al. 2016; Shropshire, Warkentin, & Sharma, 2015).

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).

As consistently shown in the above reviewed antecedent studies, the concern with effective policy compliance has gained popularity in most recent studies (see, for example, D'Arcy, Herath, & Shoss, 2014; Hu, West, & Smarandescu, 2015; Johnston et al., 2016; Johnston, Warkentin, & Siponen, 2015; Lowry & Moody, 2015; Tsohou, Karyda, & Kokolakis, 2015; Vance, Lowry, & Eggett, 2015; and Yazdanmehr & Wang, 2016). Despite its importance in reducing negative behaviors, policy compliance seems to be a minimum organizational requirement for employees. Overly emphasizing policy compliance would restrain organizations in properly recognizing their employees' potential in positively contributing to information security management. This is because security policies usually cannot cover numerous impromptu beneficial behaviors expected of their employees (Hsu et al., 2015). Indeed, research has already showcased positive ISBs from employees, such as exerting caution in treating email attachments (Ng et al., 2009), adopting using, and updating protective technologies such as anti-virus software (Boss et al., 2015; Culnan et al., 2008; Johnston & Warkentin, 2010; Lee & Kozar, 2005; Lee & Larsen, 2009; Shropshire, Warkentin, & Sharma, 2015), properly creating and safeguarding passwords, backing up data, encrypting sensitive information before transmitting it, using a firewall on computers (Boss et al., 2015; Culnan et al., 2009), coping with phishing (Wright & Marett, 2010), and security precaution taking behavior (Boss et al., 2009). Recent examples of positive behaviors include protection-motivated behaviors (Posey et al., 2013; Warkentin et al., 2016), and extra-role behaviors (Hsu et al., 2015). However, in the field of ISB research, compared to the negative behavior and policy compliance, positive behaviors have been seriously under explored.

Further, as Posey et al. (2013) and Hsu et al. (2015) showed, positive behaviors are mostly spontaneous in nature. The strength of the behavior theories used in past studies lies in showing what factors help to enhance or hinder a certain behavior. For example, Warkentin et al. (2016) showed that perceptions of threat severity, and susceptibility, response efficacy, and self-efficacy determine protective security behavior continuance. Those studies are, however, less helpful for us to identify or capture spontaneous ISBs that emerge over time. Thus, a new theory is needed, one that offers insight into multiple and diverse ISBs but also helps to explain the underpinnings of those behaviors. We attempt to offer the TDISB as such a new theoretical perspective.

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, as it generates uncertainty for an organization (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. All these three phases are identifiable in technology especially information security sensemaking, as employees face uncertainty about information security in their interactions with technology and information resources. They have to seek information, make interpretations about what their interactions with those resources mean to information security, and take actions to address their interpretation results.

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. After these three phases, organizational members begin to execute their sensemaking outcomes. This is known as enacting (Weick, 1977, 1995). Although it is not originally included in the sequential model of sensemaking, enacting is an important element of Weick's (1977, 1995) overall organizational sensemaking theory, as it particularly occurs in the organizational context. In the spirit of the sequential view of sensemaking, since enacting follows the previous three phases, it can be also deemed as another phase in organizational sensemaking. Below, to develop the TDISB, we further explain how these four phases/activities occur in the context of information security sensemaking. In doing that, we show how distinct behaviors occur in the phases of scanning and interpreting, responding, and enacting of information security sensemaking, and name them as information security diagnosing, solving, and performing behaviors, in correspondence with the phases.

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 (Katos & Adams, 2005). 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 explore numerous questions regarding what changes (for example in job security and identity (Barrett & Walsham, 1999)) including those in information security such as privacy and data security. In the ramification of information security sensemaking, they may seek to find out whether this new technology will bring risks or dangers such as loss of privacy, data security, or 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, after email has been extensively used, employees may notice that large numbers of useless emails accumulate in their boxes, and then tend to believe that these useless emails may block and slow down email communication. Eventually, the email spam issue is therefore identified (Caliendo, Clement, Papies, & Scheel-Kopeinig, 2012). This process involves scanning or cuing (noticing the issue), interpreting (tending to believe that an issue may occur), and developing knowledge (email spam).

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 et al., 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. Diagnosing behaviors lead to knowledge and understanding of information security issues, which is known as information security awareness in the literature (see the definition in Bulgurcu et al., 2010). 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. 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 ISPs 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.

DISCUSSION

Although past research examined a number of information security behaviors, a consistent focus has been directed on how to facilitate information security policy compliance. However, ISPs mostly prescribe in-role behaviors but rarely suggest extra-role behaviors, which contribute to organizational information security management more than the former (Hsu et al., 2015). Such a myopia in information security research is largely due to stagnant theorizing about information security behavior. While a variety of behavior theories helped past research to identify factors facilitating or inhibiting information security behaviors especially ISPC, they could not explain how extra-role behaviors could possibly emerge. To fill this research gap, this study proposed a new theoretical perspective in the hope of offering insight in emergent information security behaviors from employees. Thus, this study contributes to information security behavior research with the development of the theory of dynamic information security behaviors that aims to explain how organizational dynamics helps to stimulate emergence of both in-role and extra-role behaviors in the organizational context. This contribution is shown in several ways.

First, this study helps to reveal the dynamic nature of information security behaviors in the sense that employees perform diverse and multiple behaviors as they move from phase to phase in information security sensemaking. Specifically, this study shows that the emergence of these behaviors is due to organizational dynamics, which is revealed in the integration of organizational culture and sensemaking in the site of information security management. Drawing on Weick's (1979, 1995) organizational sensemaking theory, this study holds the view that while sensemaking is mainly performed by individual employees, organizational context provides a common value base that binds employees together in their sensemaking process. Dominated by the common core cultural values, employees tend to behave collectively in the scanning, interpreting, responding, and enacting activities of sensemaking, a process of organizational sensemaking (Weick, 1979, 1995). The integration of organizational context and sensemaking helps to explain how employees may perform diagnosing, solving, and performing behaviors while engaged in the scanning and interpreting, responding, and enacting sensemaking activities. Our theorizing suggests that these behaviors are spontaneous, and dynamic, as they emerge in the process of employees coping with uncertainty about information security they face in their interactions with technology and information resources.

Viewed from this perspective, this study contributes to the literature with this dynamic view of information security behaviors that suggests how positive, especially extra-role information security behaviors that are not covered in information security policies can possibly emerge, and more importantly, how they can be examined, i.e. by exploring the information security sensemaking process. This suggested direction in research represents an active response to the call for studying diverse and, more importantly, positive, behaviors (Posey et al., 2013). Moreover, this study also shows the process in which extra-role behaviors become in-role behaviors, as it has explained that after diagnosing and solving behaviors emerge and get normalized, they can be documented into information security policies for employees to perform.

Further, the presentation of diagnosing, solving, and performing behaviors represents a comprehensive categorization of information security behaviors in the organizational setting, as it captures most behaviors in organizational information security management. This organizational context-sensemaking view applies to information security management in most organizations. Thus, most behaviors can fall under these categories. This suggests that the taxonomy of information security behaviors developed in this study has significant generalizability.

Second, this study contributes to information security behavior research by suggesting a shift in focus from studying individual behaviors to examining collective behaviors. Past research, although occasionally examined organizational efforts such as training (Puhakainen & Siponen, 2010) in improving employees' ISBs, mostly focused on investigating individual factors affecting behaviors, such as cognition (e.g., see Bulgurcu et al., 2010) and ethics (Siponen & Vance, 2010). Although employees behave individually, their individual information security behaviors may demonstrate some commonality in the organizational setting. From a managerial point of view, collective information security behaviors matter more to information security management. To understand collective information security behaviors, our theorizing should help to reveal what contributes to development of collective behaviors. This study suggests and demonstrates a treatment of organizational context as a binding force promoting collective information security behaviors. Drawing on the literature, it articulates the view that organizational context facilitates as well as constrains individual sensemaking by employees and transforms it into an organizational sensemaking, which provides both form and substance to collective information security behaviors in organizations.

A third contribution of this study is that it challenged an important assumption underlying 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 helps to re-image the role of employees in organizational information management. While they may intentionally or unintentionally behave in a way that threatens information security, as reported in the literature, this study reveals that employees can be beneficial contributors to information security management in their organizations. Thus, this study generates an important implication that employees can be looked at not just as a problem, but more importantly, a solution to problems 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 context (for example, 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

References available upon request from ... (list an author's name and contact information)