A Conceptual Framework of Empowering Knowledge-Workers to Enact Security Practices[1]

Xiaodong Deng, Oakland University

Abstract

With the requirements of security laws and/or the increasingly revealed number of information security incidents, many organizations have developed and implemented security policy to comply with legal requirements and to promote security practices to knowledge-workers who legitimately use the organizations' information systems to analyze or interpret data. However, non-compliance behavior of these knowledge-workers or insiders were still listed as a most likely source of security attack.

Based on information security management and psychological empowerment literatures, this study proposed a framework that linked knowledge-workers' environment to their psychological empowerment, security practices, and to security outcomes. The framework viewed knowledge-workers' enactment of security practices as an experiential learning process that followed an observe-assess-design-implement (OADI) cycle of individual learning. The study argued that organizations should nurture an environment where knowledge-workers could be intrinsically motivated to enact security practices to their work. Psychological empowerment played a critical role in this process.

Keywords: psychological empowerment, security environment, security practices, information security outcomes, knowledge worker

INTRODUCTION

More and more organizations have been convinced to develop their security policy to counter against potential information security incidents such as data breaches or to comply with security laws or acts. They implement security education, training, and awareness (SETA) programs to promote security practices to their insiders or knowledge-workers (Gregory, 2015; Whitman and Mattord, 2017). Organizations

[1] An earlier version of this manuscript received the best paper award of 2016 International Academy of Business's Conference on Education, Business and Information Technology Issues, October 13-15, 2016, Arlington, VA. It was with the author for one revision.

must maintain the confidentiality, integrity, and availability of their information assets for business survival and sustainability.

Technologies play a critical role in securing an organization's information assets. However, technological solutions alone are not enough (Posey, Roberts, and Lowry, 2015). Human beings in general have been suggested as the weakest link in security management (Workman, Phelps, and Gathegi, 2013). While external threats increase and outside hackers' skills have become much more sophisticated than ever before (Whitman and Mattord, 2017), organizations' insiders are still regarded by many industrial surveys as the major concern about cyber security incidents. EY global information security survey 2017-18 reported that about 77% of the survey respondents considered a careless member of staff as the most likely source of attack (Ernst & Young, 2018).

These insiders or employees are knowledge workers who analyze or interpret organization's data or information (Baltzan, 2016). They are knowledgeable in their functional areas and are excellent users of the organization's information technologies or systems. However, to many of them, security practices are new, require special expertise to deal with, and, thus, are normally viewed as the knowledge domain of IT/IS staff. The knowledge workers themselves should focus on their own specialty area and contribute to organization's business.

These individuals may be unaware that information security today is the responsibility of the whole community of the organization (Whitman and Mattord, 2017). They may not know that the moment they ignore their organization's security procedures or omit information security practices, hackers may obtain needed information or gain an opportunity to access the organization' system through the vulnerabilities created by the ignorance or omissions. It is these knowledge workers' security practices that ultimately determines the success of the organization's information security initiatives (Da Veiga and Eloff, 2010).

Extensive studies have explored how to increase organizational insiders' intentions to comply with security behavior with deterrent theory (Straub and Welke, 1998; Siponen and Vance, 2010; Willison and Warkentin, 2013), coping theory (D'Arcy, Herath, and Shoss, 2014), protection motivation theory (Posey, Roberts, and Lowry, 2015; Spears and Barki, 2010; Boss, Galletta, Lowry, Moody, and Polak, 2015). However, the results are not conclusive. This study views knowledge-workers' enactment of security practices as an experiential learning process (Kim, 1993; Eisenhardt and Tabrizi, 1995) where individuals observe or experience the information security elements in their environments, assess or reflect on how the observed or experienced are related to their work, design or form their own cognitions about their security responses, and implement the design or take security actions.

The research question of this study is: how could an organization empower their knowledge workers to enact information security practices to their work? The proposed research framework intends to extend but complement existing literatures. The model argues that organizations should nurture an empowering environment where knowledge-workers would be intrinsically energized to enact security practices to their work. Psychological empowerment plays a critical role in this enactment process.

LITERATURE REVIEW

Research on how to enhance security policy compliance or security practices can be roughly categorized into two main streams: control-based and motivation-based. Originated from criminology, the control-based studies emphasized on deterring the violations by demonstrating the severe consequence(s) of not following security procedures or violating security policy. The theories on which the studies are based include deterrence theory, neutralization theory, and coping theory.

Deterrence theory posits that individuals weigh costs (or sanctions) and benefits when deciding whether to follow a security policy or practice or not, and they choose not to when it pays (Siponen and Vance, 2010). Sanctions include performance loss, legal cost, the disapproval of peers for given actions (Paternoster and Simpson, 1996), or shame (Siponen and Vance, 2010). While research found that shame functioned as a deterrent and decreased individuals' motivation to perform unwanted behaviors (Nagin and Paternoster, 1993), Siponen and Vance (2010) contended that, overall, employees' non-compliance of IS security policy or practices were poorly explained by the sanctions. Neutralization techniques (Sykes and Matza, 1957) could weaken the restraints imposed by the sanctions (Akers and Sellers, 2004).

Neutralization theory suggests that both policy-abiding and policy-violating individuals believe in the norms and values of secure information processing in general (Siponen and Vance, 2010). Individuals psychologically enable themselves to violate security policy by applying techniques of neutralization such as denial of responsibility, denial of injury, or appeal to higher loyalties (Sykes and Matza, 1957). Denial of responsibility refers to an individual's tendency to ascribe responsibility to him- or herself or to other irresistible situational factors. Denial of responsibility, for example, was found to be highly correlated with individuals' computer abuse judgment and intention (Harrington, 1996). By neutralizing their behavior, individuals can maintain their image and drift back and forth between policy-violating and policy-abiding behaviors (Piquero, Tibbetts, and Blankenship, 2005).

Coping theory describes cognitive and behavioral processes to manage psychological stress such as security related stress (D'Arcy et al., 2014).

According to coping theory, individuals go through two interrelated appraisals in determining whether following security policy is stressful. First, individuals evaluate the relevance of an espoused security behavior and the extent whether the behavior is stressful. Second, the individuals assess their control over the stressful situation, if any. The combination of two appraisals gives rise to the individuals' coping efforts that aim to alleviate the felt stress (Lazarus and Folkman, 1984).

The control-based approach may be effective, to certain extent, for those who attempt to contravene organization's security policy. With the security policy and related controls implemented, they now need to weigh seriously the loss and the gain of policy-violating behaviors. This approach helps reduce rule-breaking practices. Motivation-based studies, on the other hand, employ protection motivation theory and buy-in theory to motivate individuals to follow the advocated security practices.

Protection motivation theory (PMT) intends to explain individuals' actions regarding any security threat (Posey et al., 2015). A threat refers to a potential risk to an information asset (Whitman and Mattord, 2017). The protection motivation involves creating an effective intention to safeguard an information asset against the threat facing the individuals (Floyd, Prentice-Dunn, and Rogers, 2000). When a threat is perceived, fear may be invoked (Posey et al., 2015). The focus of PMT studies is to identify and prove the effectiveness of an approach to communicate the threat and invoke the fear that will persuade individuals to follow intended actions (Floyd et al., 2000). While the fear may frighten the individuals, PMT studies contend that it motivates adaptive, protective behaviors of the individuals (Tanner, Day, and Crask, 1989). The theory presents a cognitive process that individuals undergo when faced with threats. This process motivates the individuals to engage in either adaptive or maladaptive responses (Rogers, 1983). The adaptive response is the control of the threat while the maladaptive response is the control of the invoked fear from the threat. The outcome is a motivational force that drives individuals' behavioral change (Rogers and Prentice-Dunn, 1997).

The buy-in theory in the context of information system development (ISD) focuses on users' participation in the system development process and relates users' acceptance of the resultant system to their psychological involvement that was developed during their participation (Spears and Barki, 2010). Following this theory, if individuals participate actively in developing security policy for their organization, they may view the policy more relevant to their respective business processes and, thus, are more likely to embrace the behaviors elaborated in the policy than they would otherwise be.

Motivation-based approaches seem to be appropriate for those individuals who may omit security requirements unintentionally or who are actively engaged in security initiatives. However, for knowledge workers who may skip some security

measures in order to fulfill their job requirements such as meeting project deadlines, they may not elect to involve in those activities. They have to be internally motivated to enact security behaviors. Psychological empowerment theory may be a good alternative that helps provide such motivation.

Psychological empowerment is an intrinsic motivation reflecting an individual's cognitive assessment about a task along four dimensions: meaningfulness, self-efficacy, autonomy, and impact (Thomas and Velthouse, 1990; Spreitzer, 1995; Doll and Deng, 2010). Meaningfulness is the intrinsic value of a work goal or purpose, judged in relation to an individual's own ideals or standards (Spreitzer, 1995). Self-efficacy is an individual's belief in his or her ability to perform activities with skill (Bandura, 1989). Autonomy is an individual's sense of having choice in initiating and regulating work behaviors and processes (Spector, 1986). Impact is the degree to which an individual can influence strategic, administrative, or operating outcomes at work (Spreitzer, 1995). These four cognitive task assessments have been suggested as a nearly complete or sufficient set of cognitions for the concept of psychological empowerment (Spreitzer, 1995; Thomas and Velthouse, 1990).

Psychological empowerment theory assumes that an individual's interpretive styles are developed habits and, thus, can be changed through making the individual aware of the ongoing interpretations and their consequences (Thomas and Velthouse, 1990; Spreitzer, 1995). Interpretive styles are tendencies regarding an individual's interpretive processing of tasks (Thomas and Velthouse, 1990). This processing adds subjective information regarding evaluation, attribution, and envisioning. Specific styles of performing each process are asserted to have direct effects on an individual's task assessments. These interpretive styles identify a significant way in which the individual may empower him- or herself. The theory further assumes that individual differences in interpretive styles create diverse motivational cognitions about situational attributes (Thomas and Velthouse, 1990). Therefore, the theory posits that management practices that enhance the situational or contextual attributes of work will enhance individuals' effort and innovation only if the individuals develop empowering cognitive task assessments (Thomas and Velthouse, 1990).

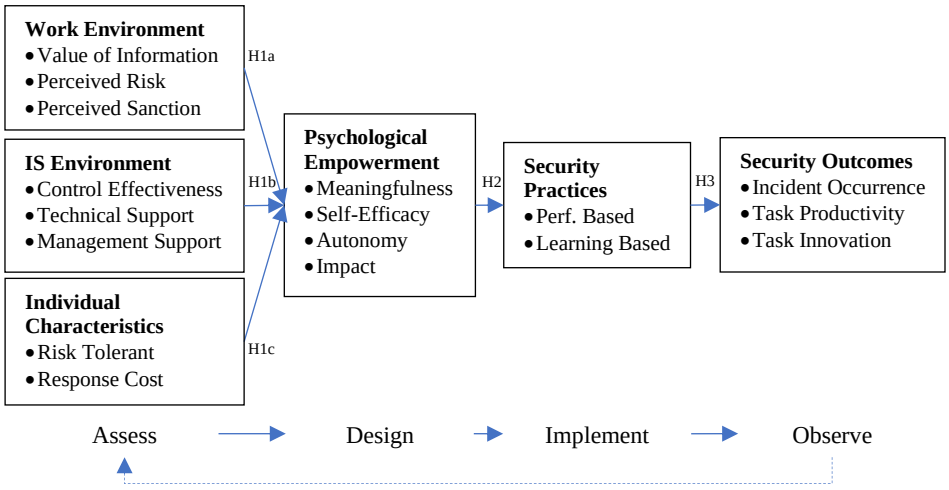
Psychological empowerment concept has been adapted to a team level to explore how team-based change initiatives be implemented effectively in a global competitive environment (Kirkman and Rosen, 1999). In information system literature, engineering knowledge workers' psychological empowerment has been found to be invoked by software capabilities and peer support and, in turn, motivates the individuals' problem solving/decision support efforts and work process innovations (Doll and Deng, 2010). Talib and Dhillon (2015) applied the concept to investigate its role in predicting an individual's intention of complying an organization's information security policy (ISP). Their study found that security education, training, and awareness (SETA), access to information security strategy

and goals, and participation in information security decision-making positively impacted on the level of an individual's psychological empowerment. Just like that of many PMT studies, the outcome is individuals' ISP compliant intention rather than their security actions.

RESEARCH MODEL

A research framework (see Figure 1) is proposed that links the task situational variables of a knowledge-worker to his or her psychological empowerment, to security practices, and, then, to security outcomes. Consistent with Spreitzer's (1995; 1996) studies, the framework/model includes situational factors, psychological empowerment, and security efforts along a nomological network. The model extends Spreitzer's nomological network by including security outcomes, which would help security managers justify their security investment and efforts. Borrowing the framework of Straub and Welke (1998), this model categorizes situational factors into work environment, IS environment, and individual characteristics. The variables in each category are closely related to individuals' security context.

FIGURE 1
Research Framework



This framework views the knowledge-workers' security practices as an experiential learning process (Eisenhardt and Tabrizi, 1995) that follows an observe-assess-design-implement (OADI) cycle of individual learning (Kim, 1993). Knowledge workers assess their work environment, information systems (IS) environment, and individual characteristics by reflecting on their observations or prior experiences. The assessments help form their own cognition (i.e., psychological empowerment) as a response to their environment. The cognition

will, then, lead to the implementation of security practices, which, in turn, create security outcomes. These concrete experiences, together with the observations from their environments commence another cycle of experiential learning (Kim, 1993; Eisenhardt and Tabrizi, 1995).

This framework suggests that organizations should nurture an environment where knowledge workers would be intrinsically energized to practice information security behaviors. Knowledge workers' psychological empowerment (through individuals' interpretive styles) plays a key role in enhancing or debilitating the experiential learning process.

Psychological Empowerment in Securing Information Assets

Psychological empowerment in this study is adapted as the intrinsic motivation invoked by an individual's cognitive assessment about a security task along four dimensions: meaningfulness, self-efficacy, autonomy, and impact. The task is to secure information assets at the individual's work. The information assets can be the data that the individual is processing or the information systems that the individual uses to process the data. The task includes a purpose and the activities that are directed to it (Thomas and Velthouse, 1990). The task can be required by the organization or chosen by the individual. The individual assesses the task based on his or her interpretation of the immediate vicinity (Spreitzer, 1996), which are characterized by work environment, IS environment, and individual characteristics (Straub and Welke, 1998).

Meaningfulness is the intrinsic value of the security task purpose, judged in relation to the individual's own standards (Spreitzer, 1995; Guo, Yuan, Archer, and Conelly, 2011). Self-efficacy is the individual's belief in his or her ability to secure information assets with skill (Maddux and Rogers, 1983; Bandura, 1989). Autonomy is the individual's sense of having choice in initiating and regulating security behaviors and practices (Spector, 1986; Chatterjee, Sarker, and Valacich, 2015). Impact is the degree to which the individual's security behaviors can generate intended outcomes at work (Thomas and Velthouse, 1990; Chatterjee et al., 2015). The assessments along these four dimensions could create a sufficient set of empowering cognitions about the security task.

Work Environment

As a dimension that characterizes an individual knowledge worker's immediate vicinity, work environment includes the individual's assessment about the value of information assets, perceived security risks, and perceived sanctions of not practicing securely. A challenging work environment is interpreted when the individual perceives high value of information assets to his or her work and to the organization, high risks from the security threats to the information assets, and severe sanctions that the exploited vulnerability will bring.

Value of Information. The value of information refers to an individual knowledge worker's perception about the importance of the information assets he or she is processing to the organization and the individual (Posey, Roberts, Lowry, Bennett, and Courtney, 2013).

The value of an information piece can be assessed in terms of the extent it has to be maintained as confidential, integral, or available (Dhillon, 2018). Different pieces or the same piece at different occasions can demonstrate different extents. For example, information about customer's order requires more attention on its integrity and availability while information about customer's personal, financial, or healthcare should be emphasized more on its confidentiality or privacy.

The value of an information piece can also be assessed by its importance to the organization's ongoing business along two correlated dimensions of criticality and sensitivity. Critical information assets can be those that the organization relies on to facilitate transactions or generate revenue while sensitive information assets those that could, if compromised, pose serious threats to the organization (Doll, Rai, and Granado, 2003).

The value assessment helps individuals perceive how the information assets contribute to the operations, mission, and vision of the organization and to the individual him- or herself. This perception then helps the individual appreciate the value of the work and the security task. This assessment thus helps invoke the individuals' meaningful cognition and perceived impact perception toward handling the information in a secure way.

Perceived Security Risk. Perceived security risk refers to knowledge workers' evaluation of damages that a materialized security threat may bring in (Liang and Xue, 2009; Guo et al., 2011). Perceived security risk (or perceived threat) can be derived from the assessment of perceived threat severity and perceived threat vulnerability in their work context (Liang and Xue, 2009). Perceived threat severity refers to the degree to which an individual believes that the threat will cause consequential harm (Rogers, 1983; Boss et al., 2015). Perceived threat vulnerability refers to the degree to which an individual believes the threat applies to his or her specific circumstances or the probability that the described threat will occur (Rogers, 1983; Boss et al., 2015).

Perceived Sanctions. Perceived sanctions are the punishments that are caused by not following or enacting security behaviors (Guo et al., 2011). The punishments can be the losses of data, productivity, or reputation. Perceived sanctions can be influenced by perceived certainty of sanctions and perceived severity of sanctions. Perceived certainty of sanctions refers to the probability that stated consequences or punishments will occur or be enforced. Perceived severity of sanctions refers to the degree of punishment associated with non-secure behaviors or non-compliant

behaviors with security policy. Deterrence theory posits that assured and severe sanctions deter individuals from targeted actions (Gibbs, 1975).

Perceived risk helps create the meaningfulness and perceived impact cognitions of information security practices. This assessment could be followed by self-efficacy and autonomy assessments. Perceived sanctions help form individuals' impact of following security practices. This assessment may invoke the assessments of self-efficacy and autonomy of practicing security behaviors. Thus,

> H1a: The more challenge of the work environment in securing information assets, the higher the level of the knowledge worker's psychological empowerment.

IS Environment

Information system (IS) environment includes the existing security control performance, organizational technical support to knowledge workers in handling security issues, and the managerial support and encouragement of enhancing security practices. A supportive IS environment is interpreted as having effective security controls in place, offering timely technical supports to individual knowledge workers, and providing related resources and encouragement to knowledge workers.

Control Effectiveness. Control effectiveness refers to the extent that the existing security controls can manage the identified security risks (Liang and Xue, 2009). Related concepts include response efficacy, which is the degree to which a person believes that the recommended response will be effective (Maddux and Rogers, 1983) and control performance, which is improved security with improvements in the system of controls in place to manage security risk to information systems (Spears and Barki, 2010). The performance of the existing security controls reflects the importance and efforts the organization puts on securing the information assets. It helps invoke meaningfulness, self-efficacy, and autonomy cognitions of knowledge workers regarding their information assets.

Technical Support. Technical support is defined as the extent that a knowledge worker can call upon the technical team for the proper handling of security issues (Zheng, Wang, Doll, Deng, and Williams, 2018). An effective support helps locate materials with easy and make related instructions or components available. It affects the individuals' perception of their impact, self-efficacy, and autonomy when enacting security practices.

Management Support. Management support is defined as the extent to which a knowledge worker can rely on the expertise of co-workers or the encouragement from management in dealing with security issues (Zheng et al., 2018). It is ongoing in nature and helps keep the threat information and the instructions of how to guard

against the threat up to date. It complements to formal SETA training sessions by allowing individuals to judge whether the information covered in the SETA program is applicable to their current situation or to practice whatever covered in the program to solve a security related issue. It also helps form a security culture within the community of interests or community of knowing (Whitman and Mattord, 2017. The culture sometimes can function as social norms of the behavior a knowledge worker engages in. It influences the worker's impact perception of security practices, the self-efficacy of practicing the behaviors, and the meaningfulness of security behaviors.

Management support could be manifested in terms of resource allocations, encouragement, or training or awareness programs. Resource allocation and encourage from the management can enhance employees' perception that they have the choices of determine how, when, and where to secure the organization's information. The training programs may help enhance the employees' skills and knowledge about how to deal with all kind of security related issues, thus, enhancing employees' competency. The awareness programs could help employees understand the consequences of a security incident or see the impact of a security compliance practice. Both will help increase the perceived impact of compliance behaviors. Thus,

> H1b: The more supportive the IS environment in securing information assets, the higher the level of the individual's psychological empowerment.

Individual Characteristics

Individual characteristics include an individual's risk tolerant and perceived response costs of securing the information assets. A responsive individual characteristic is interpreted as low risk tolerant and low perceived response costs.

Risk Tolerance. Originated from financial decisions in risky situations, risk tolerance here is adapted as the maximum amount of loss that a knowledge worker is willing to accept for a particular information asset (Barsky, Juster, Kimball, and Shapiro, 1997; Grable 2000; Liang and Xue, 2009; Whitman and Mattord, 2017). Risk tolerance has been viewed as an individual trait related to demographic variables such as age, gender, marital status, race, religion, education, and income (Filbeck, Hatfield, and Horvath, 2005; Grable 2000; Hallahan, Faff, and McKenzie, 2004). The high risk tolerant may obviate certain type of security practices.

A more risk-tolerant knowledge worker would be able to endure more (objectively) threatening malicious IT than a less risk-tolerant one. Facing the same malicious IT or security threat, the former will perceive a lower degree of threat than the latter. Thus, knowledge workers' risk tolerance has a negative effect on their perceived threat.

Perceived Response Costs. Perceived response costs refer to any perceived efforts (e.g., time, money, skills, or trouble) required to secure information assets (Weinstein, 1993; Floyd et al., 2000; Boss et al., 2015). The perception tends to affect the perceived impact, self-efficacy, and autonomy cognitions. Together,

H1c: The more responsive the individual characteristic, the higher the level of the individual's psychological empowerment.

Information Security Practices

Information security practices are defined as the efforts that knowledge workers take to counter against perceived security risks. The practices can be performance based or learning based. An intensive information security practice includes both performance- and learning-based practices.

Performance-Based Security Practices. Performance-based security practices refer to the efforts that are oriented toward the results of security actions. Examples include backing up data files or not opening suspicious email attachments. They may be specified in the organization's information security policy, trained through SETA programs, or acquired through the individual's own community of practices. Normally, this type of practices has a well-defined goal and well-described steps and does not require too much individual efforts to complete. If an individual is psychologically empowered, the individual values the efforts, see the consequences of the efforts, has the capability to engage the effort, and has the freedom of deciding when, where, and how to fulfill the efforts. The individual will likely enact the efforts in his or her job.

In the situations where the work environment is stable, the threats are well understood and safe-guarded, or the individuals are well-trained and prepared to the security threats, this type of practices may be very popular and sufficient to protect individuals' information assets.

Learning-Based Security Practices. Learning-based security practices refer to the efforts that are oriented toward the enacting process of security actions. In general, this type of practices occurs more in the complex or uncertain situations where detailed steps are not intuitive or not specified, knowledge workers need to be innovative to figure out how to follow the security guidelines. Examples include managing a passcode for an important account. The general guideline is to make the passcode open to you and the system only but blind to anybody else. However, in terms of its process, first, you have to make it difficult to guess and also satisfying the length and format requirements such as "at least eight charters long" and "including at least one lower case or upper case character and a special character". Second, you are recommended not to write it down on a piece of paper or post-it. You have to remember it, which may be challenging as well as it intends

not to be guessed or memorized with easy. Third, you need to change it at specified time interval (e.g., three months) and the new one cannot be too close to the existing one. Once you forget it or confuse it with a previous version or another code, you have limited times to try before you need to call helpdesk for a retrieval of your passcode. Otherwise, the account may be locked down for certain hours (e.g., 24-hour or three days), affecting your task productivity. If you do not follow the guidelines and the code happens to be on the thirdhand, the impact of data breach might be disastrous, given the importance of the information assets. Individuals need to be innovative or learn how to enact the passcode management practice to their work.

When the requirements are vague or the situation is complex with many constraints, psychologically empowered individuals tend to be more innovative (Thomas and Velthouse, 1990; Spreitzer, 1995). Experiential learning environment provides a natural context for knowledge workers to try out new or customized approach, explore the possible consequences of the customized approach, and rapidly build intuitive insight for the next round of process and assessment. Knowledge workers who believe that they will be successful in enacting the innovated security procedure to their work will demonstrate more effort and persistence in these efforts. Knowledge workers who find the experiential cycle of working and learning more enjoyable will be more self-motivated to continue the cycles of observation, assessment, design, and implementation. When Knowledge workers see the impact of the innovated security procedure, they are more likely to innovate.

Without the psychological empowerment, a knowledge worker may take the action, but the learning will be minimum. The individual does not understand why the actions have to be taken and what the impact the actions may create. Without this understanding, once the fear or requirement is neutralized or removed, the individual may not take the action anymore.

> Hypothesis H2: The higher the level of the individual's psychological empowerment, the more intensively they enact security practices in their job activities.

Security Outcomes

Security outcomes include the number of security incidents, task productivity and task innovation brought about by enacting security practices to work. Satisfactory security outcome means low number of security incidents, high task productivity, and more task innovations.

Number of Security Incidents. The number of security incidents are the number of incidents occurred within certain time period, for example, last six months or a year. It could also be the number of incidents in comparison to other colleagues.

When security practices are enacted, the security incident number or rate will be reduced.

Task Productivity. Task productivity refers to the extent that the security practices improve a knowledge worker's output per unit of time (Torkzadeh and Doll, 1999). While enacting security behaviors may take some time out of his or her time that is supposed to be used in job activities, task productivity here can be increased in terms of it will not be affected by the security-related events.

Task Innovation. Task innovation refers to the extent that the security practices help knowledge workers create and try out new ideas in their work (Torkzadeh and Doll, 1999). As knowledge workers experientially build and refresh their individual own areas of process expertise, integrate security knowledge and practices into their process knowledge, develop their capability for securing their information assets, and thus process, analyze, and interpret their information assets more extensively in a security-sensitive work environment, they may create or try out new ways to complete the work while following security practices. These innovations potentially help increase task productivity as well. Therefore,

> H3: The more intensively knowledge workers enact security practices in their job activities, the more satisfactory the security outcomes.

RESEARCH DESIGN

To test the proposed framework, all the constructs have to be operationalized and measured. Measurement instruments need to be adapted from the current literature or developed. The instrument items will then be reviewed by selected scholars or practitioners for clarity and readability. The reviewed questionnaire will be piloted with a small sample to assess the reliability, convergent and discriminant validity, and predictability of the constructs (Nunnally, 1978). Items may be revised, added, or deleted based on the results of pilot test to make sure that the revised items capture the essence of each construct and each construct has sufficient measurement items.

The target population will be the knowledge workers who use IT to process, analyze, or interpret information in an organizational setting. Knowledge workers in financial and healthcare industries may be desired for the study as these industries manage financial and patient healthcare information and, thus, security practices will be a key issue in organizations. However, as the data breaches or security incidents expand to organizations in other industries such as manufacturing, pharmaceutical, retail, IT, or educational, the responses from those industries will also provide valuable insights.

Organizations in all of these industries will be approached and solicited for participation in the study. The agreed organizations will then help recruit participants. The participation to this study will be voluntary and the participants' identities will be kept anonymous. Survey will then be administrated either online or via paper form, if required. Participants will be asked for their perceptions about their work environment, IS environment, individual characteristics, psychological empowerment, security practices, and security outcomes in relation to a typical task or tasks that secure(s) their information assets.

Collected data will be coded and analyzed with structural equation modeling (SEM) technique. The sample size will be at least 100 and preferably 200 or more for a reliable conclusion (Harris and Schaubroeck, 1990). The data analysis will follow Anderson and Gerbing's (1988) two-step approach: the measurement model followed by the structured model if a satisfactory measurement model is obtained.

The means, standard deviations, Skewness value, and Kurtosis value of each construct will be assessed first for the normal distribution assumption (Ghiselli, Campbell, and Zedeck, 1981). Each construct will then be assessed for its reliability, convergent validity, and discriminant validity with other ones (Nunnally, 1978; Fornell and Larcker, 1981). The values of χ^2, NNFI, CFI, and RMSEA will be used to judge the model-data fit for both measurement model and structural model (Joreskog and Sorbom, 1989; Steiger and Lind, 1980).

A satisfactory model-data fit of the structural model allows an examination of the research hypotheses through the structural coefficients between exogenous variables and endogenous variables or the ones between two endogenous variables. The findings will help judge the contributions of the research model to security management literature or practitioners, respectively.

DISCUSSION AND CONCLUSION

This study presented a conceptual model to help empower knowledge-workers to enact security practices to address the increased concern of information security in organizations. The model viewed the knowledge-workers' enactment process of security behaviors as an experiential learning process that followed Kim's (1993) OADI cycle of individual learning. The study suggested that security managers should focus more on nurturing an environment where knowledge-workers could be intrinsically energized to secure their information assets.

This model complements to the existing literature by highlighting the motivational role of psychological empowerment in the employee's security practices and by exploring the antecedents to and the behavioral consequences of psychological empowerment.

A major limitation of this study is the lack of empirical findings the assess the research model. The next step of this study, thus, is to develop the survey instruments and collect data for the pilot and the large-scale studies to test the hypotheses derived from the model. The results will help complete the research cycle and better understand the role of psychological empowerment in empowering knowledge workers' information security practices.

REFERENCES

Akers, R.L., and Sellers, C.S. 2004. *Criminological Theories: Introduction, Evaluation, and Application (4th ed.)*, Roxbury Press, Los Angeles, CA.

Anderson, J.C., and Gerbing, D.W. 1988. Structural Equation Modeling in Practice: A Review and Recommended Two-Step Approach. *Psychological Bulletin* (103:3), 411-423.

Baltzan, P. 2016. *Business Driven Information Systems (5th ed.)*. McGraw Hill Education, New York, NY.

Bandura, A. 1989. Human Agency in Social Cognitive Theory. *American Psychologist* (44:9), 1175-1184.

Barsky, R.B., Juster, F.T., Kimball, M.S., and Shapiro, M.D. 1997. Preference Parameters and Behavioral Heterogeneity: An Experimental Approach in the Health and Retirement Study. *The Quarterly Journal of Economics* (72:3), 537-579.

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

Chatterjee, S., Sarker, S., and Valacich, J.S. 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.

D'Arcy, J., Herath, T., and Shoss, M.K. 2014. Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems* (31:2), 285-318.

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

Dhillon, G. 2018. *Information Security: Text & Cases (2nd ed.)*, Prospect Press, Burlington, VT.

Doll, M.W., Rai, S., and Granado, J. 2003. *Defending the Digital Frontier, A Security Agenda*, John Wiley & Sons, Hoboken, NJ.

Doll, W.J., and Deng, X. 2010. A Technology Empowerment Model for Engineering Work. *The Data Base for Advances in Information Systems* (41:4), 52-74.

Eisenhardt, K.M., and Tabrizi, B.N. 1995. Accelerating Adaptive Processes: Product Innovation in the Global Computer Industry. *Administrative Science Quarterly* (40:1), 84-110.

Ernst & Young. 2018. Cybersecurity Regained: Preparing to Face Cyber Attacks. *20th Global Information Security Survey 2017-2018*. (https://www.ey.com/Publication/vwLUAssets/GISS_report_2017/$FILE/REPORT%20-%20EY%20GISS%20Survey%202017-18.pdf; accessed September 7, 2018).

Filbeck, G., Hatfield, P., and Horvath, P. 2005. Risk Aversion and Personality Type. *Journal of Behavioral Finance* (6:4), 170-180.

Floyd, D.L., Prentice-Dunn, S., and Rogers, R.W. 2000. A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology* (30:2), 407-429.

Fornell, C., and Larcker, D.F. 1981. Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research* (18:1), 39-50.

Ghiselli, E.E., Campbell, J.P., and Zedeck, J.P. 1981. *Measurement Theory for the Behavioral Sciences*, Freeman, San Francisco, CA.

Gibbs, J.P. 1975. *Crime, Punishment, and Deterrence*, Elsevier, New York, NY.

Grable, J. 2000. Financial Risk Tolerance and Additional Factors That Affect Risk Taking in Everyday Money Matters. *Journal of Business and Psychology* (14:4), 625-630.

Gregory, P.H. 2015. *CISSP Guide to Security Essentials (2nd ed.)*, Cengage Learning, Boston, MA.

Guo, K.H., Yuan, Y., Archer, N.P., and Conelly, C.E. 2011. Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of Management Information Systems* (28:2), 203-236.

Hallahan, T.A., Faff, R.W., and McKenzie, M.D. 2004. An Empirical Investigation of Personal Financial Risk Tolerance. *Financial Service Review* (13:1), 57-78.

Harrington, S.J. 1996. The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions. *MIS Quarterly* (20:3), 257-278.

Harris, M.M., and Schaubroeck, J. 1990. Confirmatory Modeling in Organizational Behavior/Human Resource Management: Issues and Applications. *Journal of Management* (16:2), 337-360.

Joreskog, K.G., and Sorbom, D. 1989. *LISREL Analysis of Structural Relationships by the Method of Maximum Likelihood*, Scientific Software, Inc., Mooresville, IN.

Kim, D.H. 1993. The Link between Individual and Organizational Learning. *Sloan Management Review* (35:1), 37-50.

Kirkman, B.L., and Rosen, B. 1999. Beyond Self-Management: Antecedents and Consequences of Team Empowerment. *Academy of Management Journal* (42:1), 58-74.

Lazarus, R.S., and Folkman, S. 1984. *Stress, Appraisal, and Coping*, Springer, New York, NY.

Liang, H., and Xue, Y. 2009. Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly* (33:1), 71-90.

Maddux, J.E., and Rogers, R.W. 1983. Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change. *Journal of Experimental Social Psychology* (19:5), 469-479.

Nagin, D.S., and Paternoster, R. 1993. Enduring Individual Differences and Rational Choice Theories of Crime. *Law & Society Review* (27:3), 467-496.

Nunnally, J.C. 1978. *Psychometric Theory*, McGraw Hill, New York, NY.

Paternoster, R., and Simpson, S. 1996. Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime. *Law & Society Review* (30:3), 549-584.

Piquero, N.L., Tibbetts, S.G., and Blankenship, M.B. 2005. Examining the Role of Differential Association and Techniques of Neutralization in Explaining Corporate Crime. *Deviant Behavior* (26:2), 159-188.

Posey, C., Roberts, T.L., and Lowry, P.B. 2015. The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. *Journal of Management Information Systems* (32:4), 179-214.

Posey, C., Roberts, T.L., Lowry, P.B., Bennett, R.J., and 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.

Rogers, R.W. 1983. Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation. In J.T. Cacioppo and R.E. Petty (eds.), *Social Psychophysiology: A Sourcebook*, Guilford, New York, NY, 153-176.

Rogers, R.W., and Prentice-Dunn, S. 1997. Protection Motivation Theory. In D.S. Gochman (ed.), *Handbook of Health Behavior Research I: Personal and Social Determinants*, Plenum Press, New York, NY, 113–132.

Siponen, M.T., and Vance, A.O. 2010. Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly* (34:3), 487-502.

Spears, J.L., and Barki, H. 2010. User Participation in Information Systems Security Risk Management. *MIS Quarterly* (34:3), 503-522.

Spector, P.E. 1986. Perceived Control by Employees: A Meta-Analysis of Studies Concerning Autonomy and Participation at Work. *Human Relations* (39:11), 1005-1016.

Spreitzer, G.M. 1995. Psychological Empowerment in the Workplace: Dimensions, Measurement and Validation. *Academy of Management Journal* (38:5), 1442-1465.

Spreitzer, G.M. 1996. Social Structural Characteristics of Psychological Empowerment. *Academy of Management Journal* (39:2), 483-504.

Steiger, J.H., and Lind, J.C. 1980. Statistically Based Tests for the Number of Common Factors. In *Psychometric Society Annual Meeting*. Iowa City, IA.

Straub, D., and Welke, R. 1998. Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly* (22:4), 441-469.

Sykes, G., and Matza, D. 1957. Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review* (22:6), 664-670.

Talib, Y.Y.A., and Dhillon, G. 2015. Employee ISP Compliance Intentions: An Empirical Test of Empowerment. *Thirty-Sixth International Conference on Information Systems*, December 13-16, Fort Worth, TX

Tanner, J.F., Day, E., and Crask, M.R. 1989. Protection Motivation Theory: An Extension of Fear Appeals Theory in Communication. *Journal of Business Research* (19:4), 267-276.

Thomas, K.W., and Velthouse, B.A. 1990. Cognitive Elements of Empowerment: An Interpretive Model of Intrinsic Task Motivation. *Academy of Management Review* (15:4), 666-681.

Torkzadeh, G., and Doll, W.J. 1999. The Development of a Tool for Measuring the Perceived Impact of Information Technology on Work. *OMEGA* (27:7), 327-339.

Weinstein, N.D. 1993. Testing Four Competing Theories of Health-Protective Behavior. *Health Psychology* (12:4), 324-333.

Whitman, M.E., and Mattord, H.J. 2017. *Management of Information Security (5th ed.)*, Cengage Learning, Boston, MA.

Willison, R., and Warkentin, M. 2013. Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS Quarterly* (37:1), 1-20.

Workman, M., Phelps, D.C., and Gathegi, J.N. 2013. *Information Security for Managers*, Jones & Bartlett Learning, Burlington, MA.

Zheng, Y., Wang, J., Doll, W.J., Deng, X., and Williams, M. 2018. The Impact of Organisational Support, Technical Support, and Self-Efficacy on Faculty Perceived Benefits of Using Learning Management System. *Behaviour & Information Technology* (37:4), 311-319.

About the Author

Xiaodong Deng is a Professor of Management Information Systems at Oakland University. He received his Ph.D. in Manufacturing Management and Engineering from The University of Toledo. His research has appeared in Journal of Management Information Systems, Decision Sciences, Information and Management, Communications of the Association for Information Systems, and International Journal of Production Economics. His research interests are in post-implementation information technology learning, information technology acceptance and diffusion, and supply chain management.