# Toward Developing a Theory of End User Information Security Competence

**Canchu Lin**
University of Toledo
Canchu.lin@rockets.toledo.edu

**Anand S. Kunnathur**
University of Toledo
anand.kunnathur@utoledo.edu

## ABSTRACT

In this paper we attempt to synthesize the behavioral information security research literature to construct a theory of end-user information security competence. The theory has three components: ethics and perceptions, knowledge and skills, and behavior. Additionally, we also propose that organizations can play an important role in the development of the information security competence. Contributions to both theory and practice are discussed.

Keywords
End-user information security competence, ethics and perceptions, knowledge and skills, behavior.

## INTRODUCTION

Realizing that end-users represent the weakest link in security (Warkentin & Willison, 2009), information systems (IS) researchers have examined factors that contribute to end-user security behavior. Because of their varying concerns and foci, previous information security studies identified a variety of factors that are perceived to be influential on security behavior. What is lacking in the literature is a systematic and comprehensive review of basic attributes of a competent end-user with respect to information security. Indeed, among the factors examined in prior and current information security studies, some can be deemed as positive. Prior research did not further explore the relationships among those factors. What remains to be done is to build a framework that can hold these factors together, indicate their interrelationships, and theoretically account for their contributions to positive security behaviors. Thus, the purpose of this study is to construct an end-user information security competence (EUISC) theory. We draw on the following theories to construct the theory of end-user information security competence: theories of reasoned action (Fishbein & Ajzen, 1975) and planned behavior (Ajzen, 1991), protection motivation theory (Rogers, 1975, 1983), organizational culture, participation, and the human relations and resources perspectives on management (see Figure 2). The theoretical framework of EUISC consists of three dimensions: perceptions and attitude, knowledge and skills, and security behavior (see Figure 1). We argue that development of information security competence is a process in which individuals gain perceptions about information security risks and effectiveness, and formulate attitudes, which influence knowledge and skill acquisition, which then fosters information security behavior. The paper is organized as follows: First, we will trace the theories underlying the components of the theory. Next, we will address each of the components of the theory. Finally, we will conclude the paper with some discussions on contributions from this theory and directions for future research.

## PERCEPTIONS

### Ethics and Moral Judgment

IS research has increasingly noted the importance of ethics in shaping individual perceptions toward information security. To some extent, the process of perceiving information security related issues is also one of moral judgment or reasoning. Moral reasoning positively relates to actual behavior (Blasi, 1980; King & Mayhew, 2002). Moral reasoning is relevant to information security behavior because the decision surrounding the behavior is a process of assessing whether the behavior is morally right. For example, before one violates an information security policy, one experiences a moral conflict and then morally justifies it or reduces its moral effect (Myyry, Siponen, Pahnila, & Vance, 2009). Puhakainen (2006) found that employees lightly discharged their ethical burden of failing to comply with IS security policies by arguing that their workload was too high and following the policies would slow them down in their work performance. These examples arguably showed that ethics matter so much to information security behavior.

Ethics can guide individuals to perceive information risk or threat as malicious. As Lee and Kozar (2005) demonstrated, individuals must perceive spyware as immoral and unethical, and at least not to perceive it as beneficial before they are able to successfully cope with it. As information security behavior is an outcome of moral reasoning, it is critical for employees to have a moral basis or ethics that promotes positive information security behavior and curbs negative behavior. Research findings underscored the importance of this view. For example, IS employees' intention to behave ethically/unethically relates to their personal moral judgment toward the behavior (Banerjee, Cronan, & Jones, 1998). Thus, persons with such personal ethics can be expected to comply with organizational information security policy regarding privacy control and commit themselves to protecting confidential information from unauthorized people, for example.

### Risk and Threat Perceptions

*Perceived security risk* Perceived security risk refers to end users' assessment of the security risk that may be caused by a behavior such as violation of security policies and rules. Similar to the ability to ethically assess information security issues and situations that individual employees should develop, they must develop competency in perceiving risks appropriately. Research has shown a connection between inability to perceive risk or threat and negative information security behavior. For example, inadequate perception of risks to information systems will lead to violation of information security policies (D'Arcy & Herath, 2011). With inadequate risk perception, employees have a tendency to prioritize performance and productivity over adherence to information security policies and thereby ignore or even violate security policies (Predd, Pfleefer, Hunker, & Bulford, 2008). According to Guo, Yuan, Archer, and Connelly (2011), individual employees are likely to have a favorable attitude toward and ultimately engage in non-malicious security policy violations if they perceive a lower security risk.

### Coping Perceptions

*Perceived effectiveness and perceived benefits* These perceptions are integral to the concept of information security competence. Perceived effectiveness refers to the end users' belief that their security behaviors will make their organizations informationally safe or simply will benefit their organizations (Ng, Kankanhalli, & Xu, 2009). In other words, employees believe that their security behaviors will make a difference to the overall organizational security environment. For example, when employees believe that their behaviors (complying with organizational information security policies) will make a difference and positively impact their organizations' overall information security, they will most likely comply with the policies (Herath & Rao, 2009). These perceptions are consistent with the human resources view of management in that self-actualization motivates employees to exhibit behaviors that are positive to their organizations. When employees believe that their behaviors are positive to their organizations, they will behave that way. The perception that their security actions will make a difference to their organizations motivates employees to undertake those positive information security behaviors.

## KNOWLEDGE AND SKILSS

Knowledge and skills constitute the second dimension of the end user information security competence concept. While perception and attitude provide end users a mental scheme for understanding the importance and seriousness of information security, knowledge and skills prepare them for practicing information security. Knowledge and skills provide end users confidence and expertise needed for positive information security behavior. As Wright and Marett (2010) showed, security knowledge is critical to detecting deception (phishing). Security knowledge and skills are developmental, meaning end users acquire them over time. The following constructs developed and used in information security research constitute information security knowledge and skills.

### Information Security Awareness

Information security awareness is a key component of the knowledge and skills dimension of the end user information security competence concept. It refers to an end user's overall knowledge about information security. It covers both awareness of risks or threats and, maybe more importantly, awareness of measures that are available for coping with risks/threats. The former can be labeled as *awareness knowledge* and the latter as *how-to knowledge* (Bulgurcu, Cavusoglu, & Benbasat, 2010). Information security awareness is widely believed to be critical to effective information security behavior (Goodhue & Straub 1991; Siponen 2000a, 2000b; Straub and Welke 1998; Whitman 2004). Information security awareness is deemed as a prerequisite for adequate security protection (Goodhue & Straub, 1991). Most empirical studies confirmed the link between information security awareness and security behavior (which varies from study to study, although it was mainly operationalized as policy compliance in most studies).

Information security awareness can be built from direct life experiences such as computer crash and loss of data resulted from a virus attack, and/or can be gained from external sources such as media report, security training workshops, and security documents (Bulgurcu et al., 2010). These sources especially the external sources open up opportunities for end users to acquire information security awareness. For organizations, several authors have already recommended information security awareness training programs and campaigns. For example, Straub and Welke (1998) addressed managerial information security planning including security awareness training, and proposed that such training be extended to employees as well. D'Arcy, Hovav, and Galletta (2009) recommended that information security awareness training and education be used as a security countermeasure to reduce information systems misuse in organizations. Siponen (2000a) drew on several motivation, persuasion, and behavior theories to provide conceptual insight into information security awareness campaigns and training. He addressed specific methods and how they should be used to effectively educate end users so as to increase their information security awareness. Most of the information security studies recommended information security policy awareness as a targeted goal for information security awareness training programs. If security policy concerns about specific security issues and procedures local to the organization, information security policy awareness may not cover general information security awareness (Bulgurcu et al., 2010). Thus, security awareness training should cover content that helps end users to increase their general information security awareness as well.

### Self-Efficacy

Self-efficacy is another core component of the knowledge/skill dimension of the end-user information security competence concept. It is defined as one's confidence or ability to perform a behavior based on one's skill, knowledge, and/or expertise. Self-efficacy is contextually adaptive. As empirical research studies were concerned with different aspects of information security behavior such as compliance with information security policies (Bulgurcu et al., 2010) and adoption of anti-malware software (Lee & Larsen, 2009), self-efficacy was usually tied to those aspects of information security behavior. Self-efficacy significantly influences information security behavior. It was found to be a significant predictor of security behavior (Woon, Tan, & Low, 2005). Its positive relationship to security behavior has been confirmed in empirical research. For example, self-efficacy was found to have positive influence on intent of information security policy compliance (Bulgurcu et al., 2010; Vance, Siponen, & Pahnila, 2012), intentions to adopt anti-spyware software (Lee & Kozar, 2005), intentions to adopt anti-malware software (Lee & Larsen, 2009), taking security precautions (Workman, Bommer, & Straub, 2008), attitude toward security-related behavior (Anderson & Agarwal, 2010), positive email behavior (Ng et al., 2009), and ability to detect computer deception (Wright & Marett, 2010). Self-efficacy's positive relationship to security behavior was supported in the majority of empirical research studies on information security except one (Pahnila, Siponen, & Mahmood, 2007).

Although self-efficacy mostly predicts or proceeds information security behavior, it influences the first dimension—perception and attitude, as well. It is believed that self-efficacy influences end-users' perceptions of avoidability of a threat to information technology (Liang & Yue, 2009). Similarly, Anderson and Agarwal (2010) found that self-efficacy positively influences attitude toward security-related behavior. Developing a positive ethical judgment on information security behavior, an end-user would be highly motivated to acquire necessary knowledge and skill required by the information security behavior. In this sense, perception and skill influences knowledge and skill such as self-efficacy. However, it can go the other way around. End-users with good security knowledge and skills most likely will perceive information security as important and develop a positive attitude toward security behavior. Thus, self-efficacy can also influence perception and attitude. Just as information security awareness, self-efficacy facilitates persuasion. In other words, self-efficacy facilitates the process of organizations persuading employees to take security actions. For example, Boss and Kirsch (2007) found that general computer self-efficacy is effective in helping organizations to convince employees that security policies are mandatory.

## SECURITY BEHAVIOR

Although we have shown that perceptions and knowledge and skills are prerequisites to information security behavior, there is still a perceiving/knowing-doing gap (Workman, Bommer, & Straub, 2008). Only when behavior is undertaken is the information security competence completely exhibited. Thus, security behavior is the third and last dimension of the end user information security competence concept. Commonly regarded security behaviors include exerting caution in treating email attachments (Ng et al., 2009), adopting using, and updating protective technologies such as anti-virus software (Culnan et al., 2008; Johnston & Warkentin, 2010; Lee & Kozar, 2005; Lee & Larsen, 2009), properly creating and safeguarding passwords, backing up data, encrypting sensitive information before transmitting it, using a firewall on computers (Culnan et al., 2009), coping with phishing (Wright & Marett, 2010), and security precaution taking behavior (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009). However, it is impossible to list and describe all specific security behaviors when elaborating on the behavior dimension of the information security competence concept.

### Information Security Policy Compliance

Information security behavior varies from organization to organization and from context to context. Given the highly contextualized nature, no specific information security behavior 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 security policies established in organizations usually tailor to their specific needs and requirements. In most cases, organizational information security policies define the roles and responsibilities for their employees regarding access and use of organizational information and technology resources (Bulgurcu et al., 2010). As it is assumed that information security behaviors are documented in detail in the policies, positive end user information security behavior is reduced to compliance with the policies. From the organization’s perspective, if their employees do not adhere to their security policies, their security measures will fail. Because of these two reasons, organizational information security policies have been deemed extremely important. Because of its perceived importance to organizations, prior research directed a significant amount of attention on inquiring what factors facilitate end users’ compliance with organizational information security policies (for a few examples, see Bulgurcu et al., 2010; Herath & Rao, 2009; Myyry et al., 2009; Siponen & Vance, 2010; Son, 2011.) Thus, from the organization’s perspective, it is clear that information security policy compliance is a core component of the behavior dimension of the information security competence concept.

### Participation in Security Decision Making

The perspective of participative decision making provides theoretical rigor to the argument for employee participation in information design. Security design is an organizational process that also involves decision making regarding security issues. Participation will provide extra motivation for employees to care about information security and voluntarily seek solutions to security problems or needs. Further, they will be better motivated to comply with organizational information security policies if they participate in making these security policies. Participation contributes to employees’ accountability. Participation will also enable employees to thoroughly understand the importance and relevance of information security measures that the organizations take. In the field of IS research, efforts have already been made to provide a theoretical foundation for user participation in information systems design which includes information security design.

Instead of looking at end users as the weak link in security (Mitnick & Simon, 2002; Warkentin & Willison, 2009), organizations should treat them as resources benefiting information security (Spears & Barki, 2010). Although employees may cause problems, they can provide solutions as well (Stanton & Stam, 2006; Whitman, 2008). Siponen (2005) noted that employees can play a valuable role in security design. Spears and Barki (2010) has already affirmed the benefits of user participation in organizational information security management. They showed that user participation helps to increase organizational identification and awareness of security risks and threats and organizational search for effective control measures to tackle security risks and threats in their business processes. User participation also enables employees to align security risk management with their organization’s business values, objectives, and needs. Subsequently, organizational information security control performance substantially improves.

## ORGANIZATIONAL ENHANCEMENT

In the development of end-user information security competence, an organization can play a critical role. Organizational support and involvement can influence each of the three dimensions in a way that it enhances their development. Based on prior research findings, here we will mainly elaborate on the role of two organizational interventions in the development of end-user information security competence: organizational culture and security education, training, and awareness (SETA) programs (D'Arcy et al., 2009).

### Organizational Culture

Prior research on information security strongly indicates that social influence shapes security behavior such as adoption and use of security protection software (Johnston & Warkentin, 2010; Lee & Kozark, 2005, Lee & Larsen, 2009), and compliance with security policies (Herath & Rao, 2009). Similarly, normative beliefs positively contribute to security policy compliance intention (Bulgurce et al., 2010). Likewise, subjective norms positively relate to policy compliance as well (Liao et al., 2009). Further, workgroup norms also influence non-malicious security violation intention (Guo et al., 2011). Social influence, normative beliefs, subjective norms, and workgroup norms work  in influencing information security behaviors through exerting social pressure that approves or disapproves security behaviors (Guo et al., 2011; D'Arcy & Herath, 2011). Social influence, normative beliefs, subjective norms, and workgroup norms constitute organizational culture. We thus argue that organizational culture shapes almost every aspect of information security competence including ethical reasoning, risk/threat perception, response efficacy, coping effectiveness perception, information security awareness, self-efficacy, security behaviors including policy compliance, and participation in information security design. Organizational culture that encourages social participation highly motivates employees to participate in information security activities of their organizations. It cultivates a climate of trust, feeling of shared ownership of security, and collaboration with respect to information security. Employees in such a culture are motivated to take proactive approaches to security rather than just react to security incidents after they have emerged, and develop a broader perspective on and an extended focus of security, and collaborative relationship with IS professionals.

### Education, Training, and Awareness

Organizational enhancement can also be accomplished through security education, training, and awareness (SETA) programs. These programs can curb or deter negative security behaviors such as IS misuse intention (D'Arcy et al., 2009). More importantly, education and training was deemed as more effective than punitive strategies such as sanctions in promoting positive security behavior, e.g., security policy compliance (Puhakainen & Siponen, 2010). In the information security literature a number of studies provided specific recommendations on how to conduct training programs for employees to improve security. The theoretically underscored SETA programs aim at motivating employees to increase their information security awareness by appealing to their rationality, emotionality, and moral principles or ethics (Siponen, 2000a). Such SETA programs can fulfill the need of training employees to be competent in security perceptions, knowledge and skills, and behavior. For example, organizations can educate their employees about the importance of security behaviors (security is no less important than productivity) and ethicality of security behaviors and unethicality of security violations. A higher objective for such programs is to train employees to be able to not just to follow security policies but more importantly to foresee possible security concerns associated with their work and task processes. Thus, consistent with the thrust of participative decision making, SETA programs should be designed and conducted to transform employees to be participative in organizational information security design. More specifically, they should promote employee interaction and participation in security related decision making activities (Siponen, 2000a).

## CONCLUSION

In this paper we have developed the end-user information security competence theory by synthesizing multiple theories and the literature on behavioral information security research. This has been the first attempt to theoretically address how end-users develop a competence in dealing with information security. Thus, our main contribution is that we have provided a roadmap showing how end users can develop a competence in addressing information security in organizations. We have shown that this competence is developmental in that acquiring the elements in the first two dimensions is crucial to behaving competently in dealing with information security. A second contribution is that we have theoretically demonstrated the organizational role in helping end users to develop the information security competence. As this information security competence is contextualized in the organizational setting, clarifying the organizational role in its development is helpful to both employees and organizations. To employees, this shows what resources they can seek from their organizations to help them to develop their security competence. To organizations, organizational enhancement implies that they should provide an infrastructure conducive to the development of the end-user information security competence, mainly a participative organizational culture. Thirdly, this study further contributes to organizations in their efforts to educate and train their employees about information security. The theory informs organizations on how to design educational and training programs especially what content should be covered in such programs. An important message this theory sends to organizations is that it is more important to motivate employees to participate in information security activities rather than passively comply with current security rules and policies.

This study also generates some implications for future research. This theory is mainly concerned with positive information security behaviors. Future research can follow this line to further seek possible factors that can contribute to positive security behaviors by end users. Research findings from this direction will help to strengthen this theory. For example, future research can investigate what individual and organizational factors can work together with this competence in contributing to end-user positive security behaviors. Another line of future research is to examine what outcomes this security competence will lead to. A possible research question is to ask whether developing this information security competence will bring down the number of security breaches in organizations.

## REFERENCES

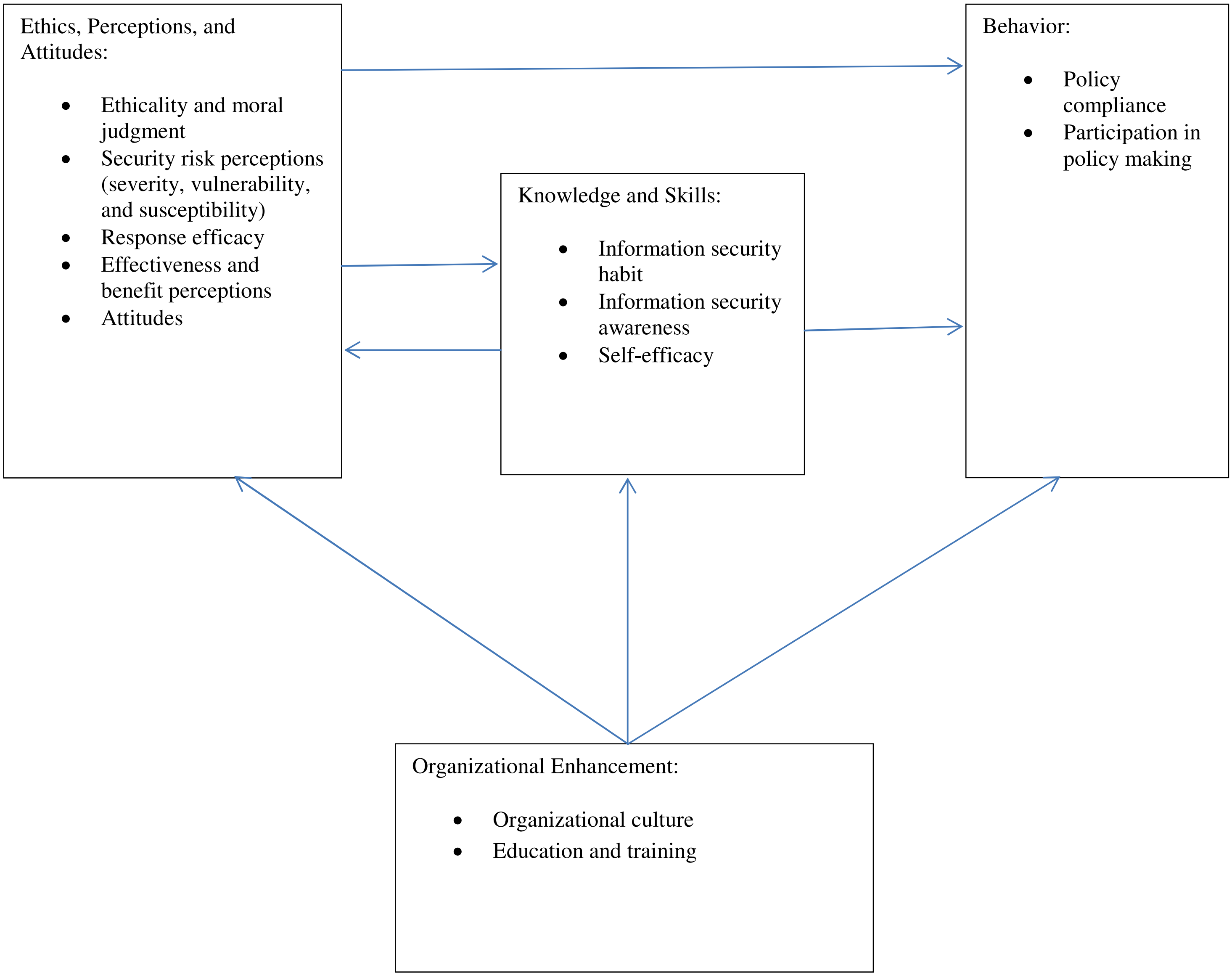
1. Ajzen, I. (1991) The theory of planned behavior. *Organizational Behavior and Human Decision Processes,* 50, 2, 179-211.
2. Anderson, C. and Agarwal, R. (2010) Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions, *MIS Quarterly*, 34, 3, 613-643.
3. Banerjee, D., Cronan, T. P. and Jones, T. W. (1998) Modeling IT ethics: A study in situational ethics, *MIS Quarterly*, 22, 1, 31-60.
4. Blasi, A. (1980) Bridging moral cognition and moral action: A critical review of the literature, *Psychological Bulletin*, 88, 1, 1-45.
5. Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A. and Boss, R. W. (2009) If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security, *European Journal of Information Systems, 18,* 151-164.
6. Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010) Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness, *MIS Quarterly,* 34, 3, 523-548.
7. Culnan, M. J., Foxman, E. R. and Ray, A. W. (2008) Why IT executives should help employees secure their home computers, *MIS Quarterly Executive*, 7,1, 49-56.
8. D'Arcy, J. and 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.
9. D'Arcy, J., Hovav, A. and Galletta, D. (2009) User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach, *Information Systems Research*, 20, 1, 79-98.
10. Fishbein, M. and Ajzen, I. (1975) Beliefs, attitude, intention and behavior: An introduction to theory and research, Addison-Wesley, Reading, MA.
11. Goodhue, D. L. and Straub, D. W. (1991) Security concerns of system users: A study of perceptions of the adequacy of security, *Information & Management,* 20, 13-27.
12. Guo, K. H., Yuan, Y., Archer, N. P. and Connelly, C. E. (2011) Understanding nonmalicious security violations in the workplace: A composite behavior model, *Journal of Management Information Systems*, 28, 2, 203-236.
13. Herath, T. and Rao, H. R. (2009) Protection motivation and deterrence: A framework for security policy compliance in organizations, *European Journal of Information Systems, 18,* 106-125.
14. Johnston, A. C. and Warkentin, M. (2010) Fear appeals and information security behaviors: An empirical study, *MIS Quarterly,* 34, 3, 548-566.

15. King, P. M. and Mayhew, M. J. (2002) Moral judgment development in higher education: Insights from the defining issues test, *Journal of Moral Education*, 31, 3, 247-270.
16. Lee, S. M., Lee, S. G. and Yoo, S. (2004) An integrative model of computer abuse based on social control and general deterrence theories, *Information & Management,* 41, 6, 707–718.
17. Lee, Y. and Kozar, K. A. (2005) Investigating factors affecting the adoption of anti-spyware system, *Communications of the ACM*, 48, 8, 72-77.
18. Lee, Y. and 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.
19. Liang, H. and Yue, Y. (2009) Avoidance of information technology threats: A theoretical perspective, *MIS Quarterly*, 33, 1, 71-90.
20. Liao, Q, Gurung, A., LUO, X. and Li, L. (2009) Workplace management and employee misuse: Does punishment matter? *Journal of Computer Information Systems,* 50, 2, 49–59.
21. 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, 469-479.
22. Mitnick, K. D. and Simon, W. L. (2002) The art of deception: Controlling the human element of security*,* Wiley Publishing, Inc., Indianapolis, IN.
23. Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T. and Vance A. (2009) What levels of moral reasoning and values explain adherence to information security rules? An empirical study, *European Journal of Information Systems, 18,* 126-139.
24. Ng, B. Y., Kankanhalli, A. and Xu, Y. (2009) Studying users' computer security behavior: A health belief perspective, *Decision Support Systems*, 46, 815-825.
25. Pahnila, S., Siponen, M. and Mahomood, A. (2007) Employees' behavior towards IS security policy compliance, in *Proceedings of the 40th Hawaii International Conference on System Sciences*, January 3-6, Los Alamitos, CA, IEEE Computer Society Press.
26. Predd, J., Pfleefer, S. L., Hunker, J. and Bulford, C. (2008) Insiders behaving badly, *IEEE Security & Privacy*, 6, 4, 66-70.
27. Puhakainen, P. (2006) A design theory for information security awareness, Oulu, Finland: University of Oulu.
28. Rogers, R. W. (1975) Protection motivation theory of fear appeals and attitude change, *The Journal of Psychology,* 91, 1, 93-114.
29. Rogers, R. W. (1983) Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation, in B. L. Cacioppo and L. L. Petty (Eds.), *Social Psychology: A Source Book*, Guildford Press, London, 153-176.
30. Siponen, M. and Vance, A. (2010) Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 34, 3, 487-502.
31. Siponen, M. T. (2000a) A conceptual foundation for organizational information security awareness, *Information Management & Computer Security,* 8, 1, 31-41.
32. Siponen, M. T. (2000b) Critical analysis of different approaches to minimizing user-related faults in information systems security: Implications for research and practice, *Information Management & Computer Security,* 8, 5, 197-210.
33. Siponen, M. T. (2005) Analysis of modern IS security development approaches: Towards the next generation of social and adaptable ISS methods, *Information and Organization,* 15, 1, 339-375.
34. 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.
35. Spears, J. L. and Barki, H. (2010) User participation in information systems security risk management, *MIS Quarterly*, 34, 3, 503-522.
36. Stanton, J. M. and Stam, K. R. (2006) The visible employee*,* Information Today, Inc., Medford, NJ.
37. Straub, D. and Welke, R. (1998) Coping with systems risk: Security planning models for management decision making, *MIS Quarterly.* 22, 4, 441-469.

38. Vance, A., Siponen, M. and Pahnila, S. (2012) Motivating IS security compliance: Insights from habit and protection motivation theory, *Information & Management*, 49, 190-198.
39. Warkentin, M. and Willison, R. (2009) Behavioral and policy issues in information systems security: The inside threat, *European Journal of Information Systems, 18*, 101-105.
40. Whitman, M. E. (2004) In defense of the realm: Understanding threats to information security, *International Journal of Information Management,* 24, 43-57.
41. Woon, I. M. Y., Tan, G. W. and Low, R. T. (2005) A protection motivation theory approach to home wireless security," in D. Avison, D. Galletta and J. I. DeGross (Eds.) *Proceedings of the 26th International Conference on Information Systems*, December 11-14, , Las Vegas, NV, USA, 367-380.
42. Workman, M., Bommer, W. and 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.
43. Wright, R., T. and 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.

Appendix 1:

Figure 1: Components of the End-User Information Security Competence Framework and their Relationships


Ethics, Perceptions, and Attitudes:
• Ethicality and moral judgment
• Security risk perceptions (severity, vulnerability, and susceptibility)
• Response efficacy
• Effectiveness and benefit perceptions
• Attitudes
Knowledge and Skills:
• Information security habit
• Information security awareness
• Self-efficacy
Behavior:
• Policy compliance
• Participation in policy making
Organizational Enhancement:
• Organizational culture
• Education and training

Appendix 2:

Figure 2: End-User Information Security Competence Framework and its Underlying Theories

| End-User Information Security Competence Framework and Its Components | Underlying Theories |
|---|---|
| Entire framework | Human relations and human resources management perspectives |
| Dimension one—Ethics, perceptions, and attitudes | |
| • Ethicality and moral judgment | Theory of moral judgment and ethics |
| • Security risk perceptions (severity, vulnerability, and susceptibility) | Protection motivation theory |
| • Response efficacy | Protection motivation theory |
| • Effectiveness and benefit perceptions | Protection motivation theory |
| • Attitudes | Theory of moral judgment and ethics, theory of planned behavior, and theory of reasoned action |
| Dimension two—Knowledge and Skills | |
| • Information security habit | General health orientation construct in preventive healthcare behavior theory |
| • Information security awareness | Protection motivation theory, theory of planned behavior |
| • Self-efficacy | Protection motivation theory, theory of planned behavior |
| Dimension three—Behavior | |
| • Policy compliance | Theory of reasoned action |
| • Participation in information security design | Participative decision making construct |
| Organizational enhancement | |
| • Organizational culture | Theory of organizational culture |
| • Education and training | Participative decision making construct |