2014

UNDERSTANDING ORGANIZATION EMPLOYEE`S INFORMATION SECURITY OMISSION BEHAVIOR: AN INTEGRATED MODEL OF SOCIAL NORM AND DETERRENCE

Hao Chen
Dalian University of Technology, ch9569@126.com

Wenli Li
Dalian University of Technology, wlli@dlut.edu.cn

UNDERSTANDING ORGANIZATION EMPLOYEE`S INFORMATION SECURITY OMISSION BEHAVIOR: AN INTEGRATED MODEL OF SOCIAL NORM AND DETERRENCE

Hao Chen, Faculty of Management and Economics, Dalian University of Technology, China, ch9569@126.com

Wenli Li, Faculty of Management and Economics, Dalian University of Technology, China, wlli@dlut.edu.cn

Abstract

Employee`s information security behavior is critical to ensure the security of organization`s information assets. Countermeasures, such as information security policies, are helpful to reduce computer abuse and information systems misuse. However, employees in practice tend to engage in these violation behaviors, although they know policies and countermeasures. Undoubtedly, these omission behaviors will bring big loss or other potential risks to information assets security. The current study try to make clear on the influence factors of information security omission behaviors and how these drive factors work. From organization control perspective, we integrate deterrence theory and social norm theory to construct research model. We expect deterrence (as normal control) will effectively decrease omission behavioral intention. Besides, colleague`s security omission behaviors may mislead some employee`s behaviors more or less, which is easy to form error code of conduct and induce to the similar omission behaviors. To date, social norms of misperception (as informal control) has not been sufficiently concerned in IS security literature and we believe that may provide a new perceptive to understand the formation mechanism of security omission behaviors.

Keywords: Social Norms of Misperception; Punishment; Information Security Omission Behavior; Organization Control

1 INTRODUCTION

One of the big challenge for enterprises in information asserts management is try to avoid information security incidents in workplace. Surveys suggest that 25% of organizations suffer from the Internet abuse caused by employees, and 13% of organizations report the unauthorized access attempts sourced from insiders (Park et al. 2012). More increasing researchers and practitioners have reached a consensus that internal employees pose a major threat to IS security rather than external attacks (Guo et al. 2011; Warkentin & Willison 2009). In order to minimize security breaches, organizations pin their hopes on security education, training and awareness (SETA) programs and information security policies (ISPs) (Bulgurcu et al. 2010; Puhakainen & Siponen 2010; Whitman 2003). In practice, nearly 90% of large-size enterprises and 67% of small-size enterprises in UK have established information security policies (Furnell & Rajendran 2012). These policies provide some standards to demarcate what behaviors are permitted or prohibited for employees in information security practice, as well as the consequent sanctions if the forbidden behaviors are happened. However, employees often use some tricks to rationalize their violation behaviors, such as neutralization techniques (Siponen & Vance 2010). Besides, employees` benefit-cost calculate or rational choice processes may also lead to the ineffectiveness of sanctions (Hu et al. 2011). Many employees in enterprises always "do not do what they are supposed to do" (Furnell & Rajendran 2012; Guo et al. 2011). When employees "who are aware of IS security threats and countermeasures but fail to implement those measures", information security omission behavior will be happen, this phenomenon also be called as knowing-doing gap (Workman et al. 2008) .

Assisting information security management practices to avoid these knowing-doing gap depends on the ability to determine why and how these omission behavior happened. Workman et al. (2008) construct a threat control model based on protection motivation theory to explain this knowing-doing gap. The model concerns personal response to fear appeals and social influences. Besides, Cox (2012) develops a model of knowing-doing gap based on the theory of planned behavior to examine the information assurance understanding and security awareness. The conclusion reveals that subjective norms play a significant role in understanding the omission behavior. Subjective norm captures one`s perception about "what those who are important think he should do in a given situation" (Bobek et al. 2013). As one of social norm constructs, subjective norm is promoting employee`s ISPs compliance and decreasing their misbehaviors (Al-Omari et al. 2012; Herath & Rao 2009; Hu et al. 2012). On the contrary, Dugo (2007) confirms the positive correlation relationship between employees` subject norm for committing an information security violation and their intention to commit violation. That reveals that incorrect norms may lead to deviation behaviors during employee`s organizational information security practices. Furthermore, both Li et al. (2010) and Zhang et al. (2009) conjecture the exists of incorrect norms (such as Internet abuse norms) and the negative impact on employees intention to information security policy compliance. Unquestionably, this incorrect norm is beyond the expectations of organization and must be avoided.

The purpose of the current study is try to understand employee`s information security omission behaviors from organization control perspective. Research questions center on: 1) Recognizing the role of punishment with mandatoriness. Through neutralization techniques and rational calculate processes may cause the failure of deterrence, we still believe punishment is indispensable for reducing employee`s omission behaviors. 2) Exploring the role of social norms with misperception. Social norms theory states that personal behavior is impacted by some incorrect perceptions of how other social group

members think and act (Berkowitz 2004). And these incorrect perceptions stem form misperception, namely, the gap between perceived norms and actual norms. However, these negative norms are little attracted in IS security researches. We believe social norm theory may provide a new perspective to understand the formation of the security omission behavior. 3) Excavating the potential relationships between these formal control (punishment) and informal control (social norms). We are interested in whether the punishment will go to ineffectiveness in this misperception norms context. We also interested in whether the punishment positively moderate the relationship between social norm of misperception and behavior intention. The conclusion will be provide an interesting perspective that counters deterrence theory. (4) Designing the effective intervention mechanism based on social norm approach, and then promoting employee`s actual compliance to ISPs.

2 THEORY BACKGROUND

2.1 Organization Control

Control is defined as a process in which organizations of people affect what other people, group, or organization will do (Jaeger & Baliga 1985). From organizational information security perspective, control is a mandatory mechanism established to ensure employees` actions in line with an agreed-upon strategy and then achieve desired security goals. Two types of organization control mechanisms are concerned: formal control and information control (Narayanaswamy & Henry 2005; Nieminen & Lehtonen 2008). Formal control is a process of performance evaluation in organization, where the senior leaders (as the controllers) observe employees behaviors or states desired outcomes; while informal control focus more on social or people self-regulation (Kirsch 1997). At the formal control level, written documents in terms of rules, goals, procedures, and regulations are in place to specify desirable behaviors, while at the informal control level, organizational values, norms, and cultures are emphasized to influence compliance behaviors (Das & Teng 1998). In current study, we are interested in understanding whether security omission behavior will be affected by these control mechanisms and how they work.

2.1.1 Formal Control: Punishment

Deterrence is widely adopted in IS security literatures (D'Arcy et al. 2009; Kankanhalli et al. 2003; Straub Jr & Nance 1990), which consists of two dimensions: punishment certainty and punishment severity (Liao et al. 2009; Tittle 1980). Deterrence theory predicts violation or infringement behaviors can be controlled well through sanctions which are certainty and/or severity. Namely, people will abandon undesirable behaviors and turn to act recommendations when they believe the probability of capture is high (punishment certainty) and/or the power of penalty is strong (punishment severity). However, not all the researches recognize the effective of punishment (Hu et al. 2011; Pahnila et al. 2007; Siponen & Vance 2010). Bulgurcu et al. (2010) believe that punishment is only a part of external motivation for users ISPs adherence behavior, intrinsic desires also play important roles simultaneously. Besides, Siponen and Vance (2010) find that neutralization technologies usage is an important factor to explain deterrence efforts failure in employee`s ISPs violation behaviors. Despite the inconsistent of research conclusions, deterrent theory still an effective and highly recognized criminal theory. Finding the reasons why deterrent security policies do not work is important (Guo et al. 2011). This study focus on the general deterrence theory and take punishment as critical measure in organization formal control. Formal control uses codified policies with mandatoriness, which including the explicit sanction, to

guide and regulate employees behaviors (Liang et al. 2013).

2.1.2 Informal Control: Social Norms

Informal control (i.e. clan control) relates to social strategies to bridge gaps among peers and guide their behaviors into recommendations (Liang et al. 2013). In this paper, we focus on social norms, which can be viewed as standards of behaviors well acknowledged by employees in information security circumstance. Social norm is established based on normative beliefs, which promotes employee`s ISPs compliance behavior and against violation or abuse behaviors (Al-Omari et al. 2012; Herath & Rao 2009; Hu et al. 2012). In these studies, social norms are defaulted as beliefs in accordance with organization expectations. However, Zhang et al. (2009) fail to confirm the analogous relationship between subjective norms (one construct of social norms) and intention to comply with policy. They give a potential reason that the effect of subjective norms are highly associated with personal experience, while the long-term accumulated ill beliefs may occupy the dominance and then lead employees to the contrary of recommendation behaviors. Not all the norms in organization are in line with organizational expectations, there exist quite a few of misperception norms which deviate from organizational identification. And the greater employees` subjective norm for committing information security violation behavior, the greater their intention to commit it (Dugo 2007). Yet, these norms are not taken too much consideration in prior studies.

People are easily to feel cognitive pressures when their current behavior is different to peers or they engage in a dilemma to choose their actions. Just as the misperceptions of Internet abuse beliefs may be viewed as one kind of "common" norms accumulating and diffusing during a bit long period, which then are adopted and imitated by the majority. We believe this diffusion of misperceptions will cause the increase of information omission behaviors. And the social norms theory may provide an explanation on the misperception.

2.2 Social Norms Theory

Social norm is more related to the concept of peer influence, which refers to the pressure to perform or not perform a behavior that is determined by a person`s inclination to comply with people who are important to him or her (Lee & Larsen 2009). Social learning theory posits that people learn from one another via observation, imitation, and modeling. As a social being, what we have done is more or less effected by others or effecting others. However, people often confuse the boundaries between perceived norms (what we think peers believe and do) and actual norms (peers real beliefs and actions), which may cause the misperception (Berkowitz 2004). Actually, people exaggeratedly overestimate or drastically underestimate the effect of peer influence.

Social norms theory captures people`s express or inhibit behavior to comply with a perceived norm (Berkowitz 2003), which states that people`s behavior is impacted by some incorrect perceptions of how other social group members think and act (Berkowitz 2004). Prior studies have been confirmed the empirical effectiveness of social norms theory in predicting and intervening health-risk behaviors (Berkowitz 2010; Berkowitz 2004; Perkins 2002). Berkowitz (2003) clarifies that the social norms theory is also suitable to issues without changes or adjustments under the conditions of identical etiology and dynamics of these issues, and extends this theory to explain social justice. Halbesleben et al. (2007) try to theorize pluralistic ignorance (one type of social norm of misperception) in organization contexts. In information security fields, pluralistic ignorance is adopted to predict employee`s Internet

abuse and personal use of Internet and system monitoring (Kim et al. 2005; Lee et al. 2008).

Two types of misperceptions are adopted to contribute to our research: pluralistic ignorance and false consensus. The former describes the majority who engage in health behavior may incorrectly believe they are in minority; and the latter captures the minority who engage in health-risk behavior may incorrectly deem they are in majority (Berkowitz 2004). Based on prior studies, people are easily engage in unhealthy behavior or risk behavior rather than healthy behavior when they exaggerate peers misconduct actions and/or underestimate their good practices. The current study tries to adopt social norms theory to explain the formation processes of employee`s information security omission behavior.

3 RESEARCH MODEL AND PROPOSTIONS

3.1 Punishment and Behavioral Intention

Punishment, as one type of formal control mechanisms with mandatoriness, can effectively adjust employee`s future behavior to avoid the possible negative consequences. Generally, punishment includes verbal reprimands, fines, suspensions, and terminations (Liang et al. 2013). In line with prior studies, we take punishment certainty and punishment severity as the components of sanctions in this study. We define punishment certainty as employee's perception of probability to be caught or imposed penalties if they engage in omission behaviors. While punishment severity means that employees believe they will be severely penalized if they engage in omission behaviors. Punishment will increase the physical and/or mental costs, which lead to the withdrawal of positive consequences from employees, such as removing privileges, withholding pay raise, or delaying promotions (Liang et al. 2013). We believe these adverse outcomes will obstruct people`s behavioral decisions making. Thus, punishment can effectively inhibit the happen of omission behaviors. We thus hypothesize that:

Proposition1: Punishment certainty negatively impact on employee`s intention to information security omission behavior;
Proposition 2: Punishment severity negatively impact on employee`s intention to information security omission behavior;

3.2 Social Norms of Misperception and Behavioral Intention

Prior studies about social norms under information security context have a premise that the social norms are defaulted as some unwritten rules in line with organization interests and values (Bulgurcu et al. 2010; Hu et al. 2012). In practices, not all the people can able to accurately identify these positive social norms, and then translate them as their own guidelines, because the misperception caused by gaps between employee`s perceptive norms and actual norms is inevitable.

Pluralistic ignorance is the majority who engage in information security behaviors may incorrectly believe they are in minority. In terms of ethical behavior, pluralistic ignorance is suitable to predict how inaccurate private perceptions of group norms can lead to an accepted environment of unethical behavior (Halbesleben et al. 2005). For example, anti-spyware installing is the behavior organization expected to ensure the safety of information assets. However, anti-spyware installing and updating is a troublesome business for individual employees, although related training on how to user it and the supports for helping them properly install it have been included in SETA programs. Once people find

their colleagues in twos and threes who do not install anti-spyware because of the inconvenience, they may mistakenly believe that only less proportion of colleagues select to install it and the most do the opposite. Then they are likely to discount their initial safety practices to cite to the "majority" peers behaviors. Thus, information security omission behaviors are diffused. Based on that, we posit that:

Proposition 3: Pluralistic ignorance positively impact on employee`s intention to information security omission behavior;

False consensus is the minority who engage in omission behaviors incorrectly deem they are in majority. This misperception is just the reverse of pluralistic ignorance. The retinal effects in psychology is helpful to understand false consensus misperception better. Retinal effects suggests that people will be more to notice the features or evens the same or similar with their own from others. We also take anti-spyware software installing as an example. If people find their colleagues in twos and threes who do not install anti-spyware for convenience, it is likely for them to mistakenly view this individual self-interested behavior as the common criteria for most peers. They immerse themselves in this "normal" norms and imitate this omission behaviors. However, they fail to clearly recognize the mainstream of policy compliance behaviors in majority. Thus, we posit that:

Proposition 4: False consensus positively impact on employee`s intention to information security omission behavior;

3.3 Punishment and Social Norms

The effect of subjective norm on employee`s behavioral intention is largely due to the ability of significant referent others to punish noncompliance (Venkatesh & Davis 2000), but the excessive of punishment is also easy to cause misperception. In organization, the success of information security practices are based on the power of security policies. Punishment is one of the critical contents, which impacts on employee`s information security behavior by force. However, the way of "punishment intimidation" exists the potential negative impact. Actually, warning to the negative behavior continually may give employees hints that more people are engaging in information risk behaviors than they thought. Thus, they may deem that so many peers around are acting beyond the accordance of the policies, and the risky behaviors may be viewed as the acceptable behavior by majority. Moreover, under the misperception norms, these security behaviors which in conformity with the specification originally may be replaced to the opposite in a long run, namely causing the risky behaviors. Similar view has been discussed in education field, such as study on intervention of Internet addiction. Yet, this misperception in information security field has not been sufficiently concerned. Thus, we posit that:

Proposition 5: Punishment acts as the positive moderator in the relationship between social norms and security omission behavior.

Based on the organization control framework, we integrate social norm theory and deterrence theory to construct research model in order to explain and predict organization employee`s intention to information security omission behavior. Major factors include punishment certainty, punishment severity, pluralistic ignorance, and false consensus. Additionally, intention to information security omission behavior is adopted as outcome variable. Besides, we also adopt scenario, gender, age, work experience, and the presence of security training as the control variables according to prior studies. The research model is shown in figure 1.

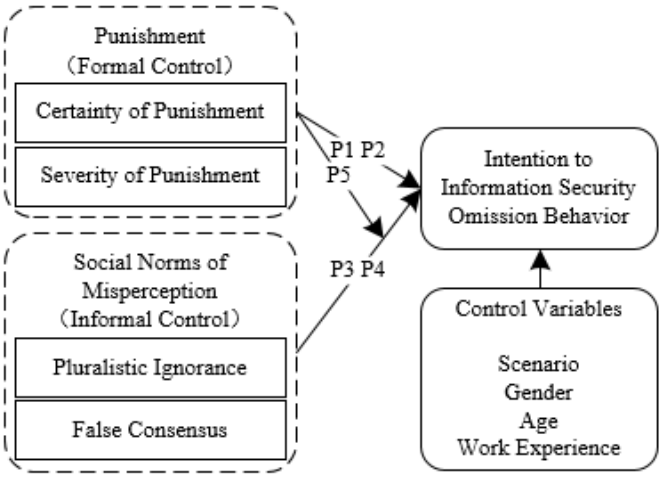

Figure 1. Research Model

4 DISCUSSION AND CONCLSION

Our work significantly contributions to the information security field by identifying potential determinants of employee's information security omission behavior intention from organizational control perspective. We construct research model by integrating deterrence theory and social norm theory. And we believe that employee`s omission behavior depends on the interaction of formal control and informal control. More in detail, we expect that punishment as one type of formal control mechanisms may effectively reduce employee`s omission behaviors, while the misperception of social norms as one type of informal control mechanisms are likely to contribute to the diffusion of this mission behaviors among employees. Especially, under the context of Chinese collectivism culture, people tend to comply with "authorities" or engage in behaviors consistent with the majority in order to cite to the benefits of them. Thus, some behaviors are prohibited by ISPs may be stealthily begin to circulate in organization. If things go on like this, this ill-formed beliefs may become a default norm. Thereby, the gap between this perceptive norm and organization recommended norm may lead to more employees involve in misperceptions to take up omission behaviors. More interested, we suspect this misperception may lead to the failure of punishment. Because of the misperception, people may deem their behaviors in line with most people must be approved by organization. Of course, the premise of this conjecture is employees intentional to avoid or ignore policies or the lack of effective SETA programs to help employees to regulate employees' behaviors. Furthermore, further empirical research is necessary to validate the conceptual model and propositions. Besides, a useful method or mechanism will be designed based on social norm approach in order to intervene the security omission behavior.

References

Al-Omari, A., El-Gayar, O., and Deokar, A. (2012). Security Policy Compliance: User Acceptance Perspective, System Science (HICSS), The 45th Hawaii International Conference, 3317-3326.

Berkowitz, A. D. (2003). Applications of Social Norms Theory to Other Health and Social Justice Issues, The Social Norms Approach to Preventing School and College Age Substance Abuse: A Handbook

For Educators, Counselors, and Clinicians, 259-279.
Berkowitz, A. D. (2004). The Social Norms Approach: Theory, Research and Annotated Bibliography, Higher Education Center for Alcohol and Other Drug Abuse and Violence Prevention. US Department of Education.
Berkowitz, A. D. (2010). Fostering Healthy Norms to Prevent Violence and Abuse: The Social Norms Approach, The Prevention of Sexual Violence: A Practitioner's Sourcebook, 147-171.
Bobek, D. D., Hageman, A. M., and Kelliher, C. F. (2013). Analyzing the Role of Social Norms in Tax Compliance Behavior, Journal of Business Ethics, 115(3), 451-468.
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.
Cox, J. (2012). Information Systems User Security: A Structured Model of the Knowing–doing Gap, Computers in Human Behavior, 28(5), 1849-1858.
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.
Das, T. K., and Teng, B.-S. (1998). Between Trust and Control: Developing Confidence in Partner Cooperation in Alliances, Academy of Management Review, 23(3), 491-512.
Dugo, T. M. (2007). The Insider Threat to Organizational Information Security: A Structural Model and Empirical Test, Auburn University
Furnell, S., and Rajendran, A. (2012). Understanding the Influences on Information Security Behaviour, Computer Fraud & Security (3), 12-15.
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.
Halbesleben, J. R., Wheeler, A. R., and Buckley, M. R.(2005). Everybody Else Is Doing It, So Why Can't We? Pluralistic Ignorance and Business Ethics Education, Journal of Business Ethics, 56(4), 385-398.
Halbesleben, J. R., Wheeler, A. R., and Buckley, M. R. (2007). Understanding Pluralistic Ignorance in Organizations: Application and Theory, Journal of Managerial Psychology, 22(1), 65-83.
Herath, T., and Rao, H. R. (2009). Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and perceived Effectiveness, Decision Support Systems, 47(2), 154-165.
Hu, Q., Dinev, T., Hart, P., and Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture, Decision Sciences, 43 (4), 615-660.
Hu, Q., Xu, Z., Dinev, T., and Ling, H. (2011). Does Deterrence Work in Reducing Information Security Policy Abuse By Employees?, Communications of the ACM, 54 (6), 54-60.
Jaeger, A. M., and Baliga, B. R. (1985). Control Systems and Strategic Adaptation: Lessons From the Japanese Experience, Strategic Management Journal, 6 (2),115-134.
Kankanhalli, A., Teo, H.-H., Tan, B. C., and Wei, K.-K. (2003). An Integrative Study of Information Systems Security Effectiveness, International Journal of Information Management, 23(2), 139-154.
Kim, J., Lee, Z., and Yoon, S. N. (2005). Pluralistic Ignorance in the Personal Use of the Internet and System Monitoring, Annual meeting of American Information System (AMCIS).
Kirsch, L. S. (1997). Portfolios of Control Modes and IS Project Management, Information Systems

Research, 8(3), 215-239.
Lee, S. M., Yoon, S. N., and Kim, J. (2008). The Role Of Pluralstic Ignorance In Internet Abuse, Journal of Computer Information Systems, 48 (3), 38-43.
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(2), 177-187.
Li, H., Zhang, J., and Sarathy, R. (2010). Understanding Compliance With Internet Use Policy From the Perspective of Rational Choice theory, Decision Support Systems, 48 (4), 635-645.
Liang, H., Xue, Y., and Wu, L.(2013). Ensuring Employees' IT Compliance: Carrot or Stick?, Information Systems Research, 24 (2), 279-294.
Liao, Q., Luo, X., Gurung, A., and Li, L. (2009). Workplace Management and Employee Misuse: Does Punishment Matter?, Journal of Computer Information Systems, 50 (2), 49-59.
Narayanaswamy, R., and Henry, R. M. (2005) Effects of Culture on Control Mechanisms in Offshore Outsourced IT Projects, Proceedings of the ACM SIGMIS CPR conference on Computer personnel research, 139-145.
Nieminen, A., and Lehtonen, M. (2008). Organisational Control in Programme Teams: An Empirical Study in Change Programme Context, International Journal of Project Management, 26(1), 63-72.
Pahnila, S., Siponen, M., and Mahmood, A. (2007). Employees' Behavior Towards IS Security Policy Compliance, System Sciences, The 40th Annual Hawaii International Conference.
Park, S., Ruighaver, A. B., Maynard, S. B., and Ahmad, A. (2011 Springer). Towards Understanding Deterrence: Information Security Managers' Perspective, Proceedings of the International Conference on IT Convergence and Security , 21-37.
Perkins, H. (2002). Social Norms and The Prevention of Alcohol Misuse in Collegiate Contexts, Journal of Studies on Alcohol and Drugs,(14), 164-172.
Puhakainen, P., and Siponen, M. (2010). Improving Employees' Compliance through Information Systems Security Training: An Action Research Study, MIS Quarterly, 34 (4), 757-778.
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.
Straub Jr, D. W., and Nance, W. D. (1990). Discovering and Disciplining Computer Abuse in Organizations: A Field Study, MIS Quarterly, 14 (1), 45-60.
Tittle, C. R. 1980. Sanctions and Social Deviance: The Question of Deterrence, Praeger New York.
Venkatesh, V., and Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies, Management Science ,46 (2), 186-204.
Warkentin, M., and Willison, R. (2009). Behavioral and Policy Issues in Information Systems Security: The Insider Threat, European Journal of Information Systems, 18 (2), 101-105.
Whitman, M. E. (2003). Enemy At the Gate: Threats To Information Security, Communications of the ACM, 46 (8), 91-95.
Workman, M., Bommer, W. H., and Straub, D. (2008). Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test, Computers in Human Behavior, 24 (6), 2799-2816.
Zhang, J., Reithel, B. J., and Li, H. (2009). Impact of Perceived Technical Protection on Security Behaviors, Information Management & Computer Security, 17 (4), 330-340.