5-2012

Information Security Policy Compliance: An Ethical Perspective

Ahmad Al-Omari
Dakota State University, Ahmad.Al-Omari@dsu.edu

Omar El-Gayar
Dakota State University, omar.el-gayar@dsu.edu

Amit V. Deokar
Dakota State University, Amit.Deokar@dsu.edu

Jack Walters
Dakota State University, Jack.Walters@dus.edu

Information Security Policy Compliance: An Ethical Perspective

Ahmad AL-Omari
Dakota State University
Ahmad.Al-Omari@dsu.edu

Omar El-Gayar
Dakota State University
Omar.El-Gayar@dsu.edu

Amit Deokar
Dakota State University
Amit.Deokar@dsu.edu

Jack Walters
Dakota State University
Jack.Walters@dus.edu

ABSTRACT

Ethical issues are key factors with respect to compliance intention with information security policies (ISPs). As such, understanding employees' compliance behavior with ISPs from ethical lenses is an important first step to leverage knowledge worker assets in efforts targeted toward reducing information security risks. This study proposes an integrated model that combines the Theory of Reasoned Action (TRA) and ethics theories; deontology and teleology, to examine users' behavioral intention to comply with ISPs. This is a research in progress, and an instrument is under development to conduct a survey study to gather data from employees in the banking sector in Jordan.

Keywords: Information security policy, compliance, moral obligation, formalism, utilitarianism, ethical egoism, TRA, information security ethics, deontology, teleology.

INTRODUCTION

People are recognized to be the weakest link in information security, but also can be great assets in the effort of reducing information security threats (Bresz, 2004; Bulgurcu, Cavusoglu, & Benbasat, 2010). Studies showed that the majority of security problems are caused by employees' non-compliance behavior or violation of information security policies (ISPs) of their organizations (Myyry, Siponen, Pahnila, Vartiainen, & Vance, 2009; Trevino, 1986), which might due to the fact that ISPs fail to impact the users' on the ground, or to the ignorance of users' of ISPs existence (Mason, 1986). Protecting organization's IT assets against theft of proprietary information and from other forms of crimes and destruction begins with developing comprehensive ISPs (Whitman, Townsend, & Aalberts, 2001). Creating the best security systems, guidelines, and policies focused on the basic security goals will ensure maximum protection in return for the organization's security investment (Cohen & Cornwell, 1989; Whitman et al., 2001). These alone, however, are not enough to ensure employees' compliance (Bulgurcu et al., 2010; Herath & Rao, 2009) and will not eliminate threats if these policies are not used properly.

Research has identified the factors that motivate compliance behavior (e.g. Bulgurcu et al., 2010; Myyry et al., 2009; Siponen, Pahnila, & Mahmood, 2007) or deter abuse or misuse behaviors (e.g. D'Arcy, Hovav, & Galletta, 2009; Harrington, 1996; Siponen & Vance, 2010; Straub, 1990). Most of these studies investigate the misuse behavior from a criminological perspective or rational choice perceptions of cost and benefits of deviant behaviors. Stafford and Warr (1993) argue that punishments might have worked before, but nowadays deterrence works only if organization is serious about enforcing the policy, therefore deterrence according to Ruighaver, Maynard, and Warren (2010) should be used only on high risk behavioral patterns that can be identified without obtrusive monitoring. While literature on information security often refers to the importance of considering ethics in a holistic approach to information security (Alder, Schminke, Noel, & Kuenzi, 2008; Davison, 2000; Hartmann, 1995; Ruighaver et al., 2010), and given the fact that organizations practice deterrence rather than positive motivation to compel employees to meet ISPs requirements (Ruighaver et al., 2010), a search of the relevant literature reveals very few studies that investigate the role of ethical ideology in shaping compliance behavior or changing the misuse behavior. Ethical theories are relevant to ISPs as the decision to comply or violate ISPs can be understood as an ethical conflict, therefore ethics in information security according to Leiwo and Heikkuri (1998) can serve two purposes ; identify criteria between good and bad, and to promote good desire over the bad ones.

A great number of previous studies concerning ISPs have used Theory of Reasoned Action (TRA) (Anderson & Agarwal, 2010; Greene & D'Arcy, 2010; Pahnila, Siponen, & Mahmood, 2007; Siponen et al., 2007; Siponen, Pahnila, & Mahmood, 2010) or Theory of Planned Behavior (TBP) (Bulgurcu et al., 2010; Zhang, Reithel, & Li, 2009) as a base theory to explain the behavioral intention to comply with ISPs. Studies that incorporated the role of ethics in ISPs have regarded

noncompliance (misuse) as an unethical behavior (Harrington, 1996; Myyry et al., 2009) but none employ the ethical decision-making model based on ethics theories as in digital piracy studies where ethical factors were incorporated in models based on behavioral theories such as the TRA and TPB (Yoon, 2011). As the field of ISPs lack studies that investigate the role of ethical ideology *per se* that explain the compliance behavior, this study is an attempt to integrate a model that combines behavior theory and ethics theory. Drawing on the TRA (Ajzen & Fishbein, 1970), we propose a model that explains users' intentions to comply with ISPs (Figure 1). In this model, we postulate that employees' intention to comply with the requirements of organization's ISPs is determined by attitude toward compliance and subjective norms. Deontological and teleological ethics are hypothesized to impact attitude and subjective norms toward compliance with ISPs.

The study will try to answer the following questions:

1. What is the role of employee's deontological ethical ideology in shaping his/her behavior toward compliance with ISPs?
2. What is the role of employee's teleological ethical ideology in shaping his/her behavior toward compliance with ISPs?
3. What is the role of social pressure on employee's compliance intention with ISPs?

The next section presents a brief review of the relevant literature and highlights this study's contributions. The third section presents the research model. The fourth section describes the research methodology, survey instrument, sample, and data collection method.

LITERATURE REVIEW

Computer and information technology ethics have been a subject of investigation by researchers (e.g.Cronan & Douglas, 2006; Floridi, 1999; Harrington, 1996; Leonard, Cronan, & Kreie, 2004). Most of information systems studies that investigated the effects of ethical issues and codes had been conducted in the software piracy environment (Chan & Lai, 2011; Moores & Chang, 2006; Wagner & Sanders, 2001). Yoon (2011) integrated the theory of deontology and theory of teleology into the theory of planned behavior. Higgins and Makin (2004) tested the correlation of low self-control with software piracy. Wagner and Sanders (2001) investigated the relationship between religion and a theoretical ethical decision making process in an ethical or unethical situations. Chan and Lai (2011) examines the impact of ethical ideology on Chinese computer users' software piracy attitude and behavior. Moores and Chang (2006) proposed a model of ethical decision making that is an adaptation of the four-component model of morality. Aleassa, Pearson, and McClurg (2011) investigated the moderating effect of ethical ideology, religiosity, public self-consciousness, and low self-control on attitudes toward software piracy.

In the security field Myyry et al. (2009) argued that theories of moral reasoning are related to information security policies (ISPs) as the intention or decision to violate an ISP can be interpreted in terms of moral conflict. They found that preconventional moral reasoning is positively related to both hypothetical and actual compliance. Harrington (1996) assessed whether general and IS-specific codes of ethics affect computer abuse judgments and employees intentions to abuse information systems. North, Perryman, Burns, and North (2010) compared the levels of information security and ethics awareness of students in diverse university environments and found that technology universities' students were more aware of information systems security and ethics than those attended a liberal arts university. Munro and Cohen (2004) examined the effect of code communication on ethical behavior through its effects on code awareness and understanding. Different studies proposed frameworks for teaching information security ethics (e.g. Cohen & Cornwell, 1989; Dark et al., 2006).

RESEARCH MODEL

This study proposes an integrated model to understand employees' behavioral compliance intention with the ISPs that combines behavioral theory and ethics theory. The study will employ TRA and normative ethics theories; deontology and teleological to explain compliance intention (Figure 1). The TRA, developed by (Ajzen & Fishbein, 1970), has been a framework for many studies in information systems and information security field (e.g. Aleassa et al., 2011; Anderson & Agarwal, 2010; Greene & D'Arcy, 2010). TRA postulate that human behavior is determined by behavioral intentions, and behavioral intentions are a function of an individual's attitude toward the behavior and subjective norms surrounding the performance of the behavior (Ajzen, 2005). Therefore, we also posit the hypothesis related to subjective norms and attitudes toward intention to comply with the requirements of ISPS. Deontology and teleology are recognized by Kohlberg (1984) as the two major ethical principles. In this model we propose that deontology; moral obligation and formalism, will affect employees' subjective norm toward compliance with ISPs. Also, it is proposed that teleology, utilitarianism and ethical egoism will impact users' attitude toward compliance with ISP. The original TRA correlations are proposed within the context of ISPs compliance (see table 2, H1 & H2)).

Deontological theories of ethics are based on the view that certain acts are wrong in themselves, and thus are morally unacceptable, even if the consequences are pursued as morally remarkable (Walsham, 1996). Moral obligation as deontological concept refers to the feeling of guilt or the personal obligation to perform or not to perform a behavior (Cronan

& Al-Rafee, 2008). It has been investigated in IT ethics literature to predict moral intention (Cronan & Al-Rafee, 2008; Haines & Leonard, 2007). According to Ajzen (1991) moral obligation will have direct impact on intention and has been investigated in the field of psychology. Further, moral obligation as a form of normative ethical standard will help shaping employees' normative belief (see table 2, H3 & H4). Formalist ethics as deontological concept looks to a set of rules or principles for guiding behavior and actions are viewed as ethical or not to the extent that they conform to these rules (Alder et al., 2008). Thus, the acts themselves are ethical or not, regardless of their outcomes, to the extent they confirm to these rules or principles (Brady & Wheeler, 1996). Furthermore, according to Ajzen (2005), subjective norm is a function of person's normative beliefs concerning referent and his motivation to comply with that referent. Thus, we postulate that formalism as a normative ethical standard may play a role in forming personal normative beliefs as a basis (see table 2, H5 & H6).

Teleology theories involves valuing goals or ends that are "good" (Davison, 2000), they differ on the question of whose good it is that one ought to try to promote (Hunt & Vitell, 1986). Utilitarianism assumes that an individuals have moral preferences and evaluate consequences of actions as ethical or not (Alder et al., 2008) and act in the interest of others (Van Staveren, 2007). TRA according to (Fishbein & Ajzen, 1975) postulates that attitude toward the behavior is determined by a person's salient beliefs that performing the behavior will lead to certain outcomes, and his evaluations of those outcomes. As perceived consequences are factors influencing attitudes toward the behavior, Yoon (2011) argued that perceived benefits as the beliefs concerning positive consequences will have impact on attitude toward the behavior. The Technology Acceptance Model (TAM) proposed and tested the relationship between perceived benefit (usefulness) and behavioral intention (Lee, Kozar, & Larsen, 2003) (see Table 2, H6 & H7). A second teleological theory is ethical egoism, under which the consequences of an act are evaluated exclusively in terms of their damage or benefit to the individual considering the action. If an act will benefit him/her but harm others, an ethical egoist will choose to perform that act (Foxman & Kilcoyne, 1993). According to (Hunt & Vitell, 1986) teleological evaluation independently affects the intention construct as an individual may perceive a particular alternative as the most ethical alternative and, nevertheless, intend to choose another alternative because of certain preferred consequences (see Table 2, H8 & H9).

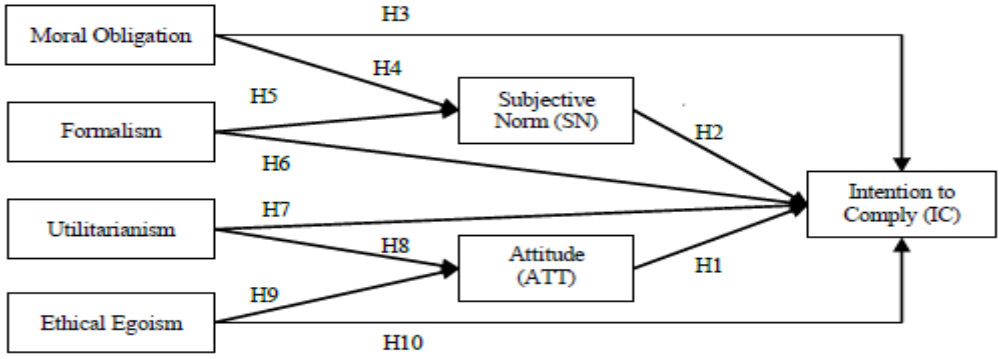

Figure 1: Research Model - Security Ethical Model

Construct	Definition	Source
Intention to Comply	An employee's intention to protect the information and technology resources of the organization from potential security breaches	(Ajzen, 1991; Bulgurcu et al., 2010)
Information security Policy (ISP)	Statement of the roles and responsibilities of employees to safeguard the information and technology resources of their organizations.	(Davis, 1989)
Deontological ethics	Universal norms that prescribe what people ought to do, how they should behave, and what is right or wrong.	(Van Staveren, 2007)
Moral obligation	The feeling of guilt or the personal obligation to perform or not to perform a behavior.	(Cronan & Al-Rafee, 2008)
Formalistic ethics	Human tendency to assess ethical situations in terms of their consistent conformity to patterns or rules or some other formal features.	(Brady & Wheeler, 1996)
Teleological ethics	Valuing goals or ends that are good.	(Davison, 2000)
Utilitarianism	Ethical framework that allows individuals to have moral preferences and to act in the interest of others, when action toward others generates a net utility gain for the individual.	(Van Staveren, 2007)
Ethical Egoism	Ethical framework in which the consequences of an act are evaluated exclusively in terms of their damage or benefit to the individual considering the action. If an act will benefit him/her but harm others, an ethical egoist still will choose to perform that act	(Foxman & Kilcoyne, 1993)

Table 1: Constructs Definitions and Sources

	Hypothesis
H1	An employee's attitude toward compliance with the organization's ISP positively affects intention to comply with the requirements of the ISP.
H2	An employee's subjective norm bout compliance with the organization's ISP positively affects intention to comply with the requirements of the ISP.
H3	An employee's moral obligation toward compliance with the organization's ISP positively affects intention to comply with the requirements of the ISP.
H4	An employee's moral obligation positively affects subjective norm toward complying with the requirements of the ISP.
H5	Formalism will positively affect subjective norm toward complying with the requirements of the ISP.
H6	Formalism will positively affects employee's intention to comply with the requirements of the ISP.
H7	Utilitarianism will positively affects employee's intention to comply with the requirements of the ISP.
H8	Utilitarianism will positively affects employee's attitude toward complying with the requirements of the ISP.
H9	Ethical egoism will negatively affect employee's attitude toward complying with the requirements of the ISP.
H10	Ethical egoism will negatively affect employee's intention to comply with the requirements of the ISP.

Table 2: Research Hypothesis

RESEARCH METHODS

We plan to conduct a survey to investigate banks employees' ethical deontological and teleological principles, attitudes, and subjective norms toward complying with the bank's ISPs to test the proposed model. A random sample of bank employees in Jordan, including those at different job levels and in different departments, will be taken. A sample of 10% of each studied bank's employees will be taken to build a sample that will have at least five times as many observations as the number of variables to be analyzed. The information will be collected directly by distributing a questionnaire to bank employees.

The survey instrument is currently being designed. To ensure that the instrument is reliable and valid, the following procedures will be followed: To ensure content validity, in addition to drawing from published literature, the questionnaire will be given to a group of experts in the field, in both the USA and Jordan, to verify that the content of the items are valid and that they measure what they are intended to measure; A pre-test will be conducted by distributing the questionnaire to a group of about 100 employees, and the results will be subjected to confirmatory factor analysis. Demographic information will be assessed in order to collect a sample that is well-matched demographically. Reliability tests will be conducted to measure the internal consistency for each construct. PLS is to be used for testing the proposed model and supporting hypotheses.

CONCLUSIONS AND FUTURE WORK

In this article, we have proposed a new research model that can help understand the compliance behavior of employees with respect to ISPs. The research model is unique in taking a users' ethical perspective at this research issue. The conceptual research model, hypotheses and research method are presented. Future work will include instrument design, data collection, data analysis, and discussion of the findings and implications for research and practice.

REFERENCES

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, *50*(2), 179-211.

Ajzen, I. (2005). *Attitudes, personality, and behavior*: Maidenhead, Berkshire, England; New York: Open University Press.

Ajzen, I., & Fishbein, M. (1970). The prediction of behavior from attitudinal and normative variables. *Journal of experimental social psychology*, *6*(4), 466-487.

Alder, G., Schminke, M., Noel, T., & Kuenzi, M. (2008). Employee Reactions to Internet Monitoring: The Moderating Role of Ethical Orientation. *Journal of Business Ethics*, *80*(3), 481-498.

Aleassa, H., Pearson, J., & McClurg, S. (2011). Investigating Software Piracy in Jordan: An Extension of the Theory of Reasoned Action. [Article]. *Journal of Business Ethics*, *98*(4), 663-676.

Anderson, C. L., & Agarwal, R. (2010). Practicing Safe Computing Special Issue Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, *34*(3), 613-643.

Brady, F. N., & Wheeler, G. E. (1996). An empirical study of ethical predispositions. *Journal of Business Ethics*, *15*(9), 927-940.

Bresz, F. (2004). People–Often the weakest link in security, but one of the best places to start. *Journal of Health Care Compliance*, *6*(4), 57-60.

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

Chan, R. Y. K., & Lai, J. W. M. (2011). Does ethical ideology affect software piracy attitude and behaviour? An empirical investigation of computer users in China. *European Journal of Information Systems*, *20*(6), 659-673.

Cohen, E., & Cornwell, L. (1989). A question of ethics: Developing information system ethics. *Journal of Business Ethics*, *8*(6), 431-437.

Cronan, T., & Douglas, D. (2006). Toward a comprehensive ethical behavior model for information technology. *Journal of Organizational and End User Computing, 18*(1), i-xi.

Cronan, T. P., & Al-Rafee, S. (2008). Factors that influence the intention to pirate software and media. *Journal of Business Ethics, 78*(4), 527-545.

D'Arcy, J., Hovav, A., & 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.

Dark, M., Epstein, R., Morales, L., Countermine, T., Yuan, Q., Ali, M., . . . Harter, N. (2006). *A framework for information security ethics education.* Paper presented at the Proceedings of the 10th Colloquium for Information Systems Security Education, University of Maryland, University College, Adelphi, MD.

Davison, R. M. (2000). Professional ethics in information systems: A personal perspective. *Communications of the AIS, 3*(2es), 4-es.

Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*: MA: Addison-Wesley.

Floridi, L. (1999). Information ethics: On the philosophical foundation of computer ethics. *Ethics and Information Technology, 1*(1), 33-52.

Foxman, E. R., & Kilcoyne, P. (1993). Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues. *Journal of Public Policy & Marketing, 12*(1), 106-119.

Greene, G., & D'Arcy, J. (2010). *Assessing the Impact of Security Culture and the Employee-Organization Relationship in IS Security Compliance.* Paper presented at the Proceedings of the 5th Annual Symposium on Information Assurance, New York, USA.

Haines, R., & Leonard, L. N. K. (2007). Situational influences on ethical decision-making in an IT context. *Information & Management, 44*(3), 313-320.

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.

Hartmann, A. (1995). *Comprehensive information technology security: A new approach to respond ethical and social issues surrounding information security in the 21st century.* Paper presented at the Proceedings of the IFIP TC11 11th international conference of Information Security, Cape Town, South Africa.

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

Higgins, G. E., & Makin, D. A. (2004). Self-Control, Deviant Peers, and Software Piracy. *Psychological reports, 95*(3), 921-931.

Hunt, S. D., & Vitell, S. (1986). A General Theory of Marketing Ethics. *Journal of Macromarketing, 6*(1), 5-16.

Kohlberg, L. (1984). *The Psychology of Moral Development: The Nature and Validity of Moral Stages*. San Francisco: Harper & Row.

Lee, Y., Kozar, K. A., & Larsen, K. R. T. (2003). The technology acceptance model: Past, present, and future. *Communications of the Association for Information Systems, 12*(1), 50.

Leiwo, J., & Heikkuri, S. (1998). *An analysis of ethics as foundation of information security in distributed systems.* Paper presented at the Proceedings of the Thirty-First Hawaii International Conference on System Sciences.

Leonard, L. N. K., Cronan, T. P., & Kreie, J. (2004). What influences IT ethical behavior intentions--planned behavior, reasoned action, perceived importance, or individual characteristics? *Information & Management, 42*(1), 143-158.

Mason, R. O. (1986). Four Ethical Issues of the Information Age. *Mis Quarterly, 10*(1), 5-12.

Moores, T. T., & Chang, J. C. J. (2006). Ethical decision making in software piracy: Initial development and test of a four-component model. *Mis Quarterly, 30*(1), 167-180.

Munro, K., & Cohen, J. (2004). *Ethical Behavior and Information Systems Codes: The Effects of Code Communication, Awareness, Understanding, and Enforcement*. ICIS 2004 Proceedings. Paper 74. http://aisel.aisnet.org/icis2004/74.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules An empirical study. *European Journal of Information Systems, 18*(2), 126-139.

North, M., Perryman, D. A., Burns, S., & North, S. (2010). A comparative study of information security and ethics awareness in diverse university environments. *Journal of Computing Sciences in Colleges, 25*(5), 223-230.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). *Employees' Behavior towards IS Security Policy Compliance.* Paper presented at the 40th Annual Hawaii International Conference on System Sciences, HICSS 2007. .

Ruighaver, A. B., Maynard, S. B., & Warren, M. (2010). Ethical decision making: Improving the quality of acceptable use policies. *Computers & Security, 29*(7), 731-736.

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: an empirical study. In H. Venter, Eloff, M., Labuschagne, L., Eloff, J., von Solms, R. (Ed.), *IFIP International Federation for*

Information Processing, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments (pp. 133-144): Boston: Springer.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with Information Security Policies: An Empirical Investigation. *Computer, 43*(2), 64-71.

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

Stafford, M. C., & Warr , M. (1993). Reconceptualization of General and Specific Deterrence. *Journal of Research in Crime and Delinquency, 30*(2), 123-135.

Straub, D. (1990). Effective IS security. *Information Systems Research, 1*(3), 255-276.

Trevino, L. K. (1986). Ethical Decision Making in Organizations: A Person-Situation Interactionist Model. *The Academy of Management Review, 11*(3), 601-617.

Van Staveren, I. (2007). Beyond Utilitarianism and Deontology: Ethics in Economics. *Review of Political Economy, 19*(1), 21-35.

Wagner, S. C., & Sanders, G. L. (2001). Considerations in ethical decision-making and software piracy. *Journal of Business Ethics, 29*(1), 161-167.

Walsham, G. (1996). Ethical theory, codes of ethics and IS practice. *Information Systems Journal, 6*(1), 69-81.

Whitman, M. E., Townsend, A. M., & Aalberts, R. J. (2001). Information systems security and the need for policy. In G. Dhillon (Ed.), *Information Security Management: Global Challenges in the New Millennium*. Hershey, PA, USA: Idea Group Publishing.

Yoon, C. (2011). Theory of Planned Behavior and Ethics Theory in Digital Piracy: An Integrated Model. *Journal of Business Ethics*, 1-13.

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security, 17*(4), 330-340.