5-2008

Knowledge for Managing Information System Security: Review and Future Research Directions

Huijin Guo
McMaster University, guoh4@mcmaster.ca

56F. Knowledge for Managing Information System Security: Review and Future Research Directions

Huijin Guo
McMaster University
guoh4@mcmaster.ca

Abstract
Information systems (IS) security is traditionally seen as technically-oriented. Technologies alone, however, cannot secure an organization's information systems at an optimal level. As such, scholars have called for more research on non-technical factors that play an important role in IS security, including human, managerial, and organizational issues. This paper aims to review and synthesize those studies that have been done on non-technical issues by applying knowledge management concepts as a tool and lens. It also identifies some issues that require further research.

Keywords
Information systems security, knowledge management

1 Introduction
Managing information system security is a big challenge for organizations because they rely increasingly on information technologies to carry out their business activities. If not properly managed, systems could be broken and the confidentiality, integrity, and availability of information could be compromised. Such security breaches can be costly for organizations. For example, the network of the TJX Companies, Inc. (TJX) was compromised in 2005 and 2006 and the security breach was estimated to cost the company more than 25 million US dollars (TJX, 2007a, 2007b).

Given the magnitude and the financial impact of security breaches on businesses, it is important that we can learn from those incidents happened and understand what the causes are in order to prevent such breaches in the future. There is little theoretical guide, however, for such endeavor. The majority of the information systems (IS) security literature is based on expert's opinion, anecdotal evidence, or experience (Kotulic & Clark, 2004). One of the possible reasons is that security is often regarded as technology-oriented. Prior research has emphasized mostly on technical issues as advanced encryption algorithms, authentication technologies, anti-virus, firewalls, and so forth. Technical solutions alone, however, do not guarantee security. Many systems have not been designed to be secure (ISO/IEC, 2005). In order to improve IS security, scholars have called for more research efforts on organizational problems, management issues and human behavior issues (Dhillon & Backhouse, 2000; Dutta & McCrohan, 2002; Hitchings, 1995).

This paper aims to review these non-technical security issues from a knowledge management perspective. This is because IS security management is a knowledge-intensive activity that

depends heavily on IS professionals' expertise and skills (Belsis et al, 2005). Furthermore, an organization's IS security is also dependent on IS users' awareness of security issues, particularly how their IS behaviors affect the security of the overall information systems. The paper applies knowledge management concepts, specifically knowledge management ontology as a tool and lens to review research in information systems security. By exploring relevant knowledge and knowledge activities in IS security, this paper closes with a discussion of some issues that require further study.

2 Knowledge Management Ontology

Ontology is a simplified and explicit specification of a phenomenon (Gruber, 1995). In the knowledge management (KM) context, a general-purpose ontology is proposed by Holsapple and Joshi (2003; 2004) as a foundation for KM research, study, and practice. In their KM ontology, knowledge management is "an entity's systematic and deliberate efforts to expand, cultivate, and apply available knowledge". An entity's knowledge management work can be seen as composed of "episodes". KM episode is defined as the entity's execution of some configuration of knowledge manipulation activities (KMA). Such activities are carried by some processors, who operating on available knowledge resources, with the intent to satisfy a knowledge need or opportunity. The activities are governed by various types of influences, which are those factors that determine how the entity manipulates knowledge. KMAs also result in learning and/or projections of knowledge. Projection refers to the emission of resources such as knowledge and products into the external environment.

In this KM ontology, two concepts are of particular interest here. The first one is learning, which is defined as 1) a process where knowledge resources are modified; and 2) an outcome of a knowledge management episode that involves the change in the state of the entity's knowledge. Learning can be functional or dysfunctional. The former indicates a positive change while the latter involves negative change in the state of the entity's knowledge. Learning also occurs whenever knowledge processors detect and correct errors (Argyris, 1995).

The learning process can be better explained with a theory-in-use model (Argyris et al, 1985). The model depicts the relationship among three concepts: governing variables, action strategies, and consequences. According to this model, people's action strategies are decided by governing variables, which are the values that people seek to satisfy; action strategies have intended consequences, which people expect to satisfy the global variables. Consequences give feedback to action strategies and governing variables. There are two forms of learning when the consequences are unintended: single-loop learning and double-loop learning. In the former situation, people try to change their actions while in the latter situation it is the governing variables that are to be changed.

The second concept of interest is knowledge resource, which is defined as the knowledge that an entity can manipulate in ways to yield value. Knowledge resource is one of the four classes of organizational resources (the other three are financial, human resources, and material resources). Knowledge resource can be further analyzed in detailed components. There are two classes of knowledge resources: schematic knowledge and content knowledge. Schematic knowledge, which depends on the existence of the entity, has four components: culture, infrastructure, strategy, and purpose; content knowledge, which on the other hand exists

independently of the entity to which it belongs, has two components: artifacts and participants' knowledge. Each of the components is defined as follows:

Culture. An organization's culture refers to the basic assumptions and beliefs that are shared by its members. It includes the organization's values, principles, norms, traditions, unwritten rules, and informal procedures.

Infrastructure. An organization's infrastructure refers to the kind of knowledge that defines the organization's roles, the inter-relationships, and the regulations that govern the use of these roles and relationship. It can be viewed as the counterpart of the culture component of knowledge resource.

Purpose. An organization's purpose defines its reason for existence. It includes mission, vision, objectives, and goals. Purpose is a directional knowledge with which other schematic knowledge components are to be aligned.

Strategy. An organization's strategy defines what to do in order to accomplish its purpose. The strategy may consist of plans for using organizational resources, which includes other knowledge resource components.

Knowledge artifact. A knowledge artifact is an object that is the representation of knowledge that may be usable to knowledge processors in an organization. It is one of the knowledge contents that can exist independent of the organization that holds it. Examples of knowledge artifacts include books, reports, documents, videos, among others.

Participants' knowledge. This refers the kind of knowledge that is possessed by employees and others who participate in the organization's business activities. In addition to employees, participants also include customer, partners, suppliers, as well as computer systems.

The above ontology gives a fairly complete picture of knowledge management by identifying its major components and the interplays among these components. It provides some guidelines for using knowledge management approaches as a tool to investigate issues related to knowledge-intensive activities such as IS security management in organizations.

3 IS Security from a Knowledge Management Perspective

In IS security management, one problem needs to be addressed is how organizations manage security-related knowledge, because IS security management is a knowledge-intensive activity that depends heavily on IS professionals' expertise and skills (Belsis et al., 2005). An organization's IS security is also dependent on IS users' awareness of security issues, particularly how their IS behaviors affect the security of the overall information systems. From knowledge management ontology perspective, the following three aspects stand out in the IS security management issue: learning, knowledge resource, and knowledge manipulation activity.

3.1 Learning

Scholars in IS field have long been advocating more research efforts on organizational problems, management issues and human behavior issues (Dhillon & Backhouse, 2000; Dutta & McCrohan, 2002; Hitchings, 1995). Indeed, many security problems can be attributed to these factors. Prior research has found that human error is a significant problem for IS security (Im & Baskerville, 2005). Im and Baskerville classified three levels of human error that pose as threats to IS security: 1) skill-based errors, which attribute to mainly monitoring failures; 2) rule-based errors, which arise if good rules are misapplied or bad rules are applied; and 3) knowledge-based errors, which are caused by the fact that related knowledge is nearly always incomplete and often inaccurate. These types of errors are from a rational viewpoint, which define errors simply as deviation from expected behavior (Neumann, 1995).

Another view regards human error as complex and socially constructed behavior. According to the action theory (Argyris, 1986; Argyris et al., 1985), such errors or misunderstandings are created by individuals who unconsciously follow their theories-in-use, a form of "skilled incompetence". Argyris et al (1985) distinguish two kinds of theories of action: espoused theory is what individuals claim to follow; and theories-in-use on the other hand are those that can be inferred from their action. It is argued that security problems happen when system users' espoused theory and their theory-in-use are contradictory (Mattia & Dhillon, 2003). An organization's espoused-theories may be embedded in its goals, mission, and formal documents. Based on this argument, Mattia and Dhillon suggest that the double-loop learning proposed by Argyris et al (1985) can be used as a strategy for designing and implementing security actions that bring an organization's espoused-theory and theory-in-use into congruence.

More specifically, Mattia and Dhillon argue that operational and technical controls, which are used for routine security activities or emergency situations are types of "single-loop learning" in Argyris et al's terms. In other words, such controls focus on the "means" that reach the end result. In a double-loop learning situation, on the other hand, security practices should not only focus on the means but also pay attention to the frame or conceptualization of the problem. In other words, in double-loop security, assumptions underlying management controls should be questioned. A double-loop security design is proposed by Mattia and Dhillon to include learning that leads to new security solution, which could be either new actions or new problem-solving. The design has four basic steps: 1) discovering espoused theories and theories in use; 2) bringing the two into congruence and identifying new governing variables; 3) generating new actions; and 4) generalizing consequences into an organizational match.

3.2 Knowledge resources

Based on the KM ontology (Holsapple & Joshi, 2004), there are six categories of knowledge: culture, infrastructure, purpose, strategy, artifacts, and participants' knowledge. The first four are schematic knowledge and the last two are content knowledge.

3.2.1 Purpose and Strategy

While it is generally understood that the purpose of security is to achieve confidentiality, availability, and integrity of business information, there has not been many studies on what kind of strategy that organizations should take to accomplish this purpose, although there is no

shortage of studies to seek innovative and robust technological solutions such as encryption and access control.

One exception is the discussion by Parker (1997). In terms of the purpose of IS security, Parker argues that the need of confidentiality is decreasing, i.e. fewer kinds of information require confidentiality. On the other hand, the importance of ownership, control, integrity, and authenticity of information is increasing. As such, organizations may need to reconsider the military-origin classification of information, such as what is confidential and what is top-secret.

Parker further contends that the strategy to achieve confidentiality may also need to change. Instead of the traditional military-origin "need-to-know" principle, a new discretionary "need-to-withhold" principle should be adopted. The latter principle suggests that an organization is better off by giving everyone in the organization its information except for a small amount that must be withheld. Another strategy is to rely on the rapid obsolescence of secret information rather than trying to protect it. For example, by the time competitors obtain the trade secret information, it may have already been obsolete and useless.

3.2.2 Culture

In the KM ontology, culture refers to norms, beliefs, and basic assumptions shared by the members of an organization. In the IS security literature, the importance of organizational culture has been recognized. Information systems security is not a technical problem, but a social and organizational one that involves people because it is them that operate and use those systems (Dhillon & Backhouse, 2000). An organizational subculture and a common belief system are needed to make members of the organization committed to their activities that might have impacts on IS security (Dhillon, 1999). Such culture should also promote responsibility, integrity of people, trustworthiness, and ethicality (Dhillon & Backhouse, 2000).

Dhillon and Torkzadeh (2006) took a step further to study IS security issues in terms of the values of people from an organizational perspective. By using the value-focused thinking to identify fundamental objectives for IS security and the means to achieve them, their study suggests that organizationally grounded principles and values are necessary for maintaining security of information systems in organizations. More specifically, Dhillon and Torkzadeh identified 25 clusters of objectives held by organizational members for IS security. There are nine fundamental objectives and 16 means objectives. Examples of fundamental objectives include enhancing management development practices, maximizing integrity of business processes, and maximizing organizational integrity. Examples of mean objectives include increasing trust, providing open communication, and maximizing awareness. These objectives can be used for developing IS security measures.

Smith and Hasnas (1999) investigated the ethical issues in information systems in general. While raising an important issue of ethics in IS, their study identifies some challenges facing organizations when they deal with ethical dilemmas. One of the challenges is that applying different ethical theories on the same ethical situation may have conflicting conclusions. Thus, it is important for organizations to pay attention to this issue and have a clear communication with employees in terms of what kinds of behavior are considered ethical and acceptable related to information systems use in general and security in particular.

3.2.3 Infrastructure

In the KM ontology, infrastructure refers to an organization's roles, their relationships, and the regulations that govern them. In the context of information system security, policy, as one type of organizational regulation, is of particular interest.

Security policy refers to the set of rules, and practices that regulate how an organization manages, protects, and distributes its resources to achieve specified security objectives (Sterne, 1991). Security objectives are often reflected in the purpose and strategy as discussed previously. Recognizing the limitation of existing security policy approach, Baskerville and Siponen (2002) proposed a meta-policy as a guide to establish how policies should be created, implemented, and enforced. Some of the policy features are: 1) policy requirements, which include identification and classification of security subjects and objects, as well as the elaboration of the process by which the organization will determine who need to access what information; 2) How policies is designed, e.g. the creation of policy and sub-policies hierarchy and when the adjustment of the level of abstraction and enforcement needed; and 3) How policies are to be implemented, and if necessary how they should be tested in order to determine whether the goals of policies are met.

Siponen and Iivari, on the other hand, take a different theoretical perspective to study the design of successful IS security polices and guidelines (2006). They identify six normative theories that can offer insights on how IS policies and guidelines handle exceptional situations, where business opportunities may require temporary violations of those policies and guidelines.

Marchinkowski and Stanton (2003) analyzed extant information security policies from a number of organizations to ascertain the motivational assumption. Although motivation is just one of several factors associated with effective policy, the study found that motivation factors do not receive enough attention in the research or practitioner literatures. It also raised a question of how information security figures into employees' performance evaluations.

3.2.4 Artifacts

An artifact in the KM ontology refers to an object is or hold a representation of knowledge that may be useful for a knowledge processor in the organization. Examples of such artifact include documents and reports. In the IS security context, Belsis et al (2005) conducted a field research and identified a number of security-related knowledge artifact ("sources"). These artifacts can be classified into three levels of abstraction: strategic, tactical, and operations. Strategic-level artifacts include security policy document, which deals with the design and dissemination of security policies. At tactical level, the artifacts include risk analysis document, documented countermeasures, audit trail reports, automatic logs, and audit documentation. At the operations level, the knowledge artifacts include network alerts and logs.

Two types of artifacts widely used in information systems security are checklist and standards. Checklists are based on the assumption that solutions and procedures can be observed and turned into a list, hence "checklist", for solving security problems (Siponen, 2005). Examples

of such IS security checklists include the risk checklist proposed by Moulton & Moulton (1996) and the control checklist proposed by Wood et al (1987). IS security standards are usually the best practices for managing security in organizations. One example of such standards is ISO/IEC 27002. The standard "establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization" (ISO/IEC, 2005). It contains best practices of control objectives and controls in areas of information security management such as security policy, physical and environmental security, access control, among others.

3.2.5 Participants' knowledge

In the KM ontology, participant's knowledge refers the knowledge that is possessed by a knowledge processor who participates in the organization's business activities. Participants can be employees, customers, or suppliers, among others. In the IS security context, however, research seemed to have been focusing on employees who use the organization's information systems to carry out their routine business activities.

From a *domain* perspective, employees' knowledge can be classified as business knowledge and information technology (IT) knowledge. Information systems security knowledge can be viewed as a sub-category of IT knowledge. Understandably, as a common sense IT and IS security people have necessary IT knowledge to manage organizational information systems; and end-users (or business people) have necessary business knowledge to carry business activities and make critical decisions.

In order to achieve effective security management, however, IT people should also have necessary business knowledge. Such business knowledge is critical for IT people to understand how IT risks impact the organization's business performance and to manage security in a cost-effective manner. It will also enable IT people to have better communications with end-users and business people. Such knowledge is also defined as "business competence of IT professionals" (Bassellier & Benbasat, 2004), which is comprised of organization-specific knowledge and interpersonal and management knowledge. The former can be further broken down to more specific areas of knowledge: organizational overview, organizational unit, organizational responsibility, and IT-business integration; and the latter can be broken down to areas of knowledge networking, interpersonal communication, and leadership.

IT knowledge of end-users is equally important for effective security management. Lack of necessary IT knowledge and skills causes human errors, which are a significant issue for information systems security (Im & Baskerville, 2005). Such IT knowledge and skills are also defined as "IT competence" (Bassellier et al, 2001).

Based on its *mode*, IT competence can be classified as explicit knowledge and tacit knowledge (Nonaka, 1994; Polanyi, 1962). Explicit knowledge is often codified and can be transmitted in formal and systematic language; tacit knowledge, on the other hand, involves personal quality and is difficult to be formalized and transmitted. Based on Bassellier et al's classification, end-users' explicit IT knowledge include knowledge in areas of technology, applications, systems development, management of IT, and access to IT knowledge (e.g. knowing who to contact for more information on IT); tacit knowledge includes end-users' experience in IT projects and experience in the management of IT.

Based on its *primary type*, IT knowledge of end-users can be classified into descriptive, procedural, and reasoning knowledge (Holsapple & Whinston, 1996). Each of them describes some different aspect of a knowledge object. Descriptive knowledge is about the "state of some world", which include descriptions of past, present, future, and hypothetical situations. It is about "know what". Procedural knowledge is about the detailed procedures of doing something. It is about "know how". Reasoning knowledge, however, specifies the conclusions that can be drawn from certain pre-conditions. It is about "know why". It can be argued that this classification scheme loosely reflects the "depth" of knowledge. Descriptive knowledge is the least in-depth while reasoning knowledge is the most in-depth understanding of a subject matter. According to this classification, the explicit IT knowledge (Bassellier et al., 2001) falls into the category of descriptive knowledge, because it focuses on "the understanding of benefits of different IT, not on their specific features".

In the IS security context, some studies focused on the end-users' awareness of security problem. Such awareness can also be classified as a descriptive knowledge in terms of general understanding of security issues but without in-depth "know-how" and "know-why". Siponen (2000; 2001) investigated IS security awareness from a human behavioral perspective and argued that more focus should be put on normative and prescriptive awareness.

3.3 Knowledge Manipulation Activity

In the KM ontology, knowledge manipulation activity refers to the acquisition, selection, generation, assimilation, and emission of knowledge, which occur in the "conduct of knowledge management" (Holsapple & Joshi, 2004).

In the IS security context, organizational security planning is one of such knowledge manipulation activities. Straub and Welke (1998) proposed a security planning model for management decision-making on security issues. The security risk planning model includes four phases: 1) recognition of security problem or need; 2) risk analysis; 3) alternatives generation; and 4) planning decision. Each phase involves some processes of knowledge resources. For example, risk analysis may involves an understanding of organizational strategy, end-users' general level of IT knowledge and skills, and the design documentation of an information system, among others. Such analysis may generate a list of risks and their priorities. Taking this knowledge of risk as an input, the next phase may generate a list of alternatives that might alleviate the risks. This kind of knowledge activities may go on until a decision is made. The output could be a documented IS security strategy, which is also a knowledge resource according to the KM ontology.

A similar approach is the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework (Alberts et al, 1999). The OCTAVE framework has three phases: 1) building enterprise-wide security requirement; 2) identifying infrastructure vulnerabilities; and 3) demining security risk management strategy. Similar to that of previous approach, each phase in this OCTAVE framework involves the knowledge manipulation activities. For example, in the first phase of assessment, several types of knowledge need to be analyzed: enterprise knowledge, operational area knowledge, and staff knowledge.

4 Discussion and Future Research

This paper reviewed research in information systems security from a knowledge management perspective. More specifically, it applied the knowledge management ontology to investigate knowledge and knowledge activities associated with IS security. It found that the current IS security research on non-technical factors has been focusing on three aspects: knowledge resources, knowledge manipulation activities, and learning.

There has not been sufficient research, however, on the other two aspects of knowledge management ontology: knowledge influence and projection. Knowledge influences include managerial, resources, and environmental factors, all of which could impact the overall security management organizations. It is not clear, however, how and to what extent these factors impact IS security. One research in this direction is the study by Knapp et al (2006). They found that top management's support is a significant predictor of security culture and policy enforcement in organizations.

Projection is the other aspect that future research could be conducted. One specific area is security knowledge sharing among organizations such as businesses, software vendors, and security solution providers. Possible research questions include how and why organizations share security knowledge such as virus information and software vulnerabilities, what benefits organizations can achieve by sharing such knowledge, and what factors encourage or discourage organizations to share their security knowledge.

The literature review also revealed two issues that worth further research. The first issue is what kind of strategy can best manage information systems security. Parker (1997) contrasted two different strategies: need-to-know approach and need-to-withhold approach. The question is, can the latter approach perform better than the former? What are the conditions, environmental or organizational, should be met in order for this to happen? The second issue is what level of business knowledge is needed for IT professionals and what level of IT knowledge is needed for business people and end-users. Although prior research suggested that both types of knowledge are important for the two groups of people, it is still unclear what level of knowledge is optimal.

References

Alberts, C. J., Behrens, S. G., Pethia, R. D., & Wilson, W. R. (1999). *Operationally Critical Threat, Asset, and Vulnerability Valuation (OCTAVE) Framework*. Pittsburgh, PA: Carnegie Mellon Software Engineering Institute.

Argyris, C. (1986). Skilled incompetence. *Harvard Business Review, 64*(5), 74-79.

Argyris, C. (1995). Action science and organizational learning. *Journal of Managerial Psychology, 10*(6), 20-26.

Argyris, C., Putnam, R., & Smith, D. M. (1985). *Action science* (1st ed.). San Francisco: Jossey-Bass.

Baskerville, R. L., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management, 15*, 337-346.

Bassellier, G., & Benbasat, I. (2004). Business Competence of Information Technology Professionals: Conceptual Development and Influence on It-Business Partnerships. *MIS Quarterly, 28*(4), 673-694.

Bassellier, G., Reich, B. H., & Benbasat, I. (2001). Information Technology Competence of Business Managers: A Definition and Research Model. *Journal of Management Information Systems, 17*(4), 159-182.

Belsis, P., Kokolakis, S., & Kiountouzis, E. (2005). Information systems security from a knowledge management perspective. *Information Management & Computer Security, 13*(3), 189-202.

Dhillon, G. (1999). Managing and controlling computer abuse. *Information Management & Computer Security, 7*(4), 171-175.

Dhillon, G., & Backhouse, J. (2000). Information systems security management in the new millennium. *Communications of the ACM, 43*(7), 125-128.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal, 16*, 293-314.

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review, 45*(1), 67-87.

Gruber, T. R. (1995). Toward principles for the design of ontologies used for knowledge sharing. *International Journal of Human and Computer Studies, 43*(5/6), 907-928.

Hitchings, J. (1995). Deficiencies of the traditional approach to information security and the requirements for a new methodology. *Computer & Security, 14*, 377-383.

Holsapple, C. W., & Joshi, K. D. (2003). A knowledge management ontology. In C. W. Holsapple (Ed.), *Handbook on Knowledge Management* (Vol. 1, pp. 89-124). Berlin: Springer-Verlag.

Holsapple, C. W., & Joshi, K. D. (2004). A formal knowledge management ontology: Conduct, activities, resources, and influences. *Journal of the American Society for Information Science and Technology, 55*(7), 593-612.

Holsapple, C. W., & Whinston, A. B. (1996). *Decision Support Systems : A Knowledge-Based Approach*. Minneapolis/St. Paul: West Pub. Co.

Im, G. P., & Baskerville, R. L. (2005). A longitudinal study of information system threat categories: The enduring problem of human error. *The DATA BASE for Advances in Information Systems, 36*(4), 68-79.

ISO/IEC. (2005). Information Technology - Security Techniques - Code of Practice for Information Security Management (ISO/IEC 27002). Geneva, Switzerland: International Organization for Standardization.

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: Management's effect on culture and policy. *Information Management & Computer Security, 14*(1), 24-36.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management, 41*(597-607).

Marcinkowski, S., & Stanton, J. M. (2003). *Motivational aspects of information security policies.* Paper presented at the IEEE International Conference on Systems, Man and Cybernetics.

Mattia, A., & Dhillon, G. (2003). Applying double loop learning to interpret implications for information systems security design, *IEEE International Conference on Systems, Man and Cybernetics* (Vol. 3, pp. 2521-2526).

Moulton, R. T., & Moulton, M. E. (1996). Electronic communication risk management: A checklist for business managers. *Computer & Security, 15*(5), 377-386.

Neumann, P. G. (1995). *Computer-Related Risks*. New York: ACM Press.

Nonaka, I. (1994). A dynamic theory of organizational knowledge creation. *Organization Science, 5*(1), 14.

Parker, D. B. (1997). The strategic values of information security in business. *Computer & Security, 16*, 572-582.

Polanyi, M. (1962). *Personal Knowledge: Towards a Post-Critical Philosophy*. New York: Harper Torchbooks.

Siponen, M. T. (2005). An analysis of the traditional IS security approaches: Implications for research and practices. *European Journal of Information Systems, 14*, 303-315.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41.

Siponen, M. T. (2001). Five Dimensions of Information Security Awareness. *ACM SIGCAS Computers and Society, 31*(2), 24-29.

Siponen, M., & Iivari, J. (2006). Six design theories for IS security policies and guidelines. *Journal of the Association of Information Systems*, 7(7), 445-472.

Smith, H. J., & Hasnas, J. (1999). Ethics and information systems: The corporate domain. *MIS Quarterly, 23*(1), 109-127.

Sterne, D. F. (1991). On the buzzword "security policy", *IEEE Symposium on Security and Privacy* (pp. 219-230).

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision-making. *MIS Quarterly, 22*(4), 441-469.

TJX. (2007a). Annual Report of 2006: The TJX Companies, Inc.

TJX. (2007b). Quaterly Report of The TJX Companies, Inc (SEC Form 10-Q, for the Quaterly Period Ended April 28, 2007).

Wood, C. C., Banks, W. W., Guarro, S. B., Garcia, A. A., Hampel, V. E., & Sartorio, H. P. (1987). *Computer Security: A Comprehensive Controls Checklist*. New York: John Wiley & Sons.