Journal of Information Privacy and Security, 10: 160–185, 2014
Published with license by Taylor & Francis
ISSN: 1553-6548 print / 2333-696X online
DOI: 10.1080/15536548.2014.974407

ARTICLES

A Model of Information Security Awareness for Assessing Information Security Risk for Emerging Technologies

Roberto J. Mejias
Colorado State University-Pueblo

Pierre A. Balthazard
St. Bonaventure University

Information systems (IS) that interconnect emerging technologies have rendered organizations increasingly vulnerable to emerging information technology (IT) attacks. Drawing on IS concepts such as systems and cybernetic theory, technological threat avoidance theory (TTAT) and general deterrence theory (GDT), this study develops an IS security (ISS) risk model that contributes to an understanding of information security awareness (ISA) and the assessment of ISS risk. Results indicate that technical knowledge, organizational impact and attacker assessment generate significant positive path coefficients with ISA. However, the constructs organizational impact and attacker assessment generated stronger path coefficients with ISA than technical knowledge. Research model results also indicate that ISA is strongly associated with ISS risk.

INTRODUCTION

The increasing use of new and emerging technologies such as mobile computing, iPads, social media, Web 2.0 networking, cloud computing, and virtual collaborative environments have enabled organizations to exchange and transfer significant amounts of data, information, and intellectual property (Kim & Yong, 2012; Mejias & Harvey, 2012). Some “ready” emerging technologies such as Dropbox, Skype, ListenLogic, FourSquare, and BYO, are quickly accessible,

Correspondence should be addressed to Roberto J. Mejias, Department of Computer Information Systems, Hasan School of Business, Colorado State University-Pueblo, 2200 Bonforte Blvd., Pueblo, CO 81001. E-mail: roberto.mejias@colostate-pueblo.edu

cost effective, and are frequently implemented often without the knowledge or participation of the organization's information technology (IT) team (Andriole, 2014). The adoption of these emerging technologies has evolved differently from traditional IT adoption, which typically incorporates processes such as requirements analysis, modeling, testing for interoperability, total cost of ownership, and return on investment analysis (Andriole, 2014). Emerging and ready technologies frequently have customer-driven requirements with uncontrolled or *ad hoc* pilot tests that have limited integration with existing technologies and architectures. The advantages of such quick emerging IT adoption are noteworthy: accelerated adoption, fail fast/fair cheap pilot tests, rapid technology-driven business process change, avoidance of large integration support costs, and improved total cost of ownership and return on investment (Andriole, 2014).

Information security, however, is rarely the primary concern of the users, developers, and designers who deploy these new technologies (Pfleeger & Caputo, 2012). As emerging technologies proliferate throughout organizations, often without the incorporation of security or compliance considerations in their architecture, organizations have become increasingly vulnerable to cyber-attacks (He, Yang, & Yang, 2013; Kumar, Park, & Subramanian, 2008; Pfleeger & Caputo, 2012). While vendors that market security hardware, software, and services have witnessed unprecedented growth, market coverage continues to remain relatively low (Dey, Lahiri, & Zhang, 2012). In light of the frequency and significant impact of cyber-attacks, the number of legislative and organizational initiatives advocating more information security awareness (ISA) has increased for organizations implementing new and emerging technologies (Bulgurcu, Cavusoglu, & Benbasat, 2010; Puhakainen & Siponen, 2010).

While ISA initiatives and IS security (ISS) risk assessments have long been recognized as fundamental to information security (Rees et al., 2011; Spears & Barki, 2010), extant IS literature has been limited in providing useful frameworks for understanding the relationship between ISA and ISS risk assessment (Bulgurcu et al., 2010; Ko & Zafar, 2009; Pfleeger & Caputo, 2012; Slusky & Pariz-Navin, 2012). Since the assessment of IS risk may be complex, an increased awareness of the consequences of cyber-attacks may prove useful in better assessing ISS risk, particularly as it relates to emerging technologies (Bulgurcu et al., 2010; Kim & Yong, 2012; Kumar et al., 2008; Zhao, Xue, & Whinston, 2013). ISS risk assessment, however, has often been undertaken as a fragmented approach by management (Bulgurcu et al., 2010; Zafar, 2011). ISS risk models are frequently poorly known, portrayed with various overlapping dimensions and developed by researchers operating under different paradigms (Bodin, Gordon, & Loeb 2008; Pfleeger & Caputo, 2012; Siponen, 2005; Spears & Barki, 2010). Additionally, these researchers frequently seem unaware of each other's research findings (Siponen, 2005). In developing a theoretical framework for ISA and ISS risk, this study therefore draws on concepts from system dynamics and cybernetic theory (Wiener, 1948), TTAT (Liang & Xue, 2009), and general deterrence theory (D'Arcy & Herath, 2011; Gibbs, 1975; Pratt et al., 2006).

This research is presented in the following manner. In the review of prior literature the authors explore how a multi-perspective approach enhances knowledge of cyber-attacks and improves the comprehension of ISA. In developing the research model, the authors identify how three relevant constructs (*technical knowledge, organizational impact* and *attacker assessment*) contribute to an understanding of IT attacks and their association with ISA and ISS risk assessment. The relationships between these constructs are discussed and translated into specific hypotheses to be tested. The authors then describe the methodology used to test the research model using confirmatory factor analysis (CFA) models and structural equation modeling techniques. Finally, the results from the testing of the research model are reported and the cyber-threat implications for researchers and practitioners developing and employing new and emerging technologies are discussed.

PRIOR RESEARCH AND THEORETICAL FRAMEWORK

Traditionally, theory building in the IS literature have been based on the use or adoption of virtuous or "good" IT. *Virtuous IT* refers to information systems designed to improve communicational, computational or decisional efficiency and performance (Liang & Xue, 2009). As seen from the volume of IS literature, numerous theories have been developed within the IS discipline or imported from other disciplines to explain why a certain technology is (or is not) adopted, given that such IT adoption is considered virtuous (Liang & Xue, 2009). Notably, a commonly held belief in the IS literature is that the acceptance or *adoption* of good IT is analogous to the *avoidance* of malicious or "bad" IT (Liang & Xue, 2009; Mejias, 2012). While acceptance and adoption theories such as innovation diffusion theory, technology acceptance theory, the theory of planned behavior, and the theory of reasoned action may be appropriate when considering the implementation of good IT, these extant theories were not intended to explain avoidance behavior relating to IT threats and emerging technologies. Subsequently, the IS literature has expended considerably less effort examining the avoidance of malicious or bad IT that cause system dysfunctions and security breaches to information systems (Liang & Xue, 2009). Drawing on concepts from systems dynamics and cybernetic theory (Weiner, 1948), technological threat avoidance theory (Liang & Xue, 2009), and general deterrence theory (D'Arcy & Herath, 2011; Gibbs, 1975; Pratt et al., 2006) may provide a more appropriate and integrated framework to understand IT attacks, ISA, and ISS risk assessment as they relate to new and emerging technologies.

Systems Dynamics and Cybernetic Theory

Systems dynamics and cybernetic theory seek to understand and model the dynamic behavior of complex systems. The primary components of system dynamics are feedback loops, flow accumulation (into reserves) and time delays (Dutta & Roy, 2008; Sveen, Rich, & Jager, 2007). Cybernetic theory (Wiener, 1948) is the interdisciplinary study of the structure of regulatory systems and is closely related to system theory and system dynamics, particularly with regard to feedback loops. The central theme of cybernetic theory is that human beings self-regulate their behavior via feedback loops to enhance or improve their current state (Carver & Scheier, 1982; Dutta & Roy, 2008; Liang & Xue, 2009). Extant IS acceptance and adoption theories such as innovation diffusion theory, technology acceptance theory, the theory of planned behavior, and the theory of reasoned action primarily advocate an approach behavior that seeks to decrease the distance between a current IT state and the desire to *adopt* a desired or virtuous IT state. In system theory and system dynamics this relationship is known as a *negative feedback loop*.

While adoption theories are valuable in advocating an approach behavior to a desired IT state, they provide an incomplete understanding of IS initiatives that seek *avoidance* from malicious IT (Liang & Xue, 2009). As such, system dynamics and cybernetic theory may be more appropriate in describing avoidance behavior as a *positive feedback loop*. A positive feedback loop seeks to *increase* the distance of a current IT state away from a bad or undesired IT state. The differences between the negative and positive feedback loops of system dynamics and cybernetic theory are analogous to the qualitative distinction between *approach* and *avoidance* theories (Carver, 2006; Liang & Xue, 2009; Mejias, 2012). Specifically, the *approach and avoidance* distinction illustrates that the adoption of good IT is not the same as the avoidance of bad or malicious IT.

While it is understandable to apply traditional IS adoption theories with regard to protecting IT, the adoption of safeguarding theories is a subgoal that should support the larger goal of avoiding cyber-attacks. Acceptance or adoption IS theories therefore, do not fully differentiate the phenomenon and efforts of threat avoidance from IT attacks (Liang & Xue, 2009; Mejias, 2012). The positive feedback loop from systems theory may provide a better theoretical basis to understanding *avoidance* behavior and a more appropriate framework relating to IT attacks (Carver, 2006; Liang & Xue, 2009). This is particularly relevant as organizations, businesses, and consumers interact with new and emerging technologies to exchange significant amounts of data, and information and intellectual property (Kim & Yong, 2012).

Technology Threat Avoidance Theory (TTAT)

TTAT seeks to explain IT threat avoidance behavior by referencing systems dynamics, cybernetic theory, and multiple disciplines across a broad range of IT attacks and user populations (Liang & Xue, 2009). TTAT provides a relevant framework to explain the avoidance of malicious IT phenomena that cannot be properly explained by IS adoption or approach theories (Liang & Xue, 2009). TTAT posits that, once users perceive the emergence of an IT threat, they then employ a positive feedback loop and become motivated to distance themselves away from the threat by adopting safeguarding measures or employing coping behavior (Liang & Xue, 2009). When coping behaviors are employed, a positive feedback loop is initiated for two cognitive processes: *threat appraisal* (primary) and *coping appraisal* (secondary) (Liang & Xue, 2009). After an appraisal deems a threat to be imminent, then two coping behavior processes (*avoidance mitigation, avoidance behavior*) are activated to address the forthcoming threat. These coping behavior processes are used within the TTAT positive feedback loop to increase the distance from the current (i.e., safe) IT state and away from the undesired and malicious IT state (Liang & Xue, 2009). TTAT posits that as IT users become more cognizant of the negative consequences of malicious IT attacks they consider appropriate safeguards for a better assessment of related ISS risk (Liang & Xue, 2009). By extending prior research regarding the importance of ISS breaches, TTAT offers a useful and relevant framework for understanding the threat avoidance behavior underlying ISA (Liang & Xue, 2009).

General Deterrence Theory (GDT)

GDT is a *classic* deterrence theory that focuses on formal or legal sanctions to prevent offenders from behaving in a particular manner (Gibbs, 1975). GDT proposes that the greater the perceived certainty, severity, and swiftness of sanctions and penalties imposed on an individual in response to an illegal or illicit act, the more individuals are deterred from committing that act (D'Arcy & Herath, 2011; Gibbs, 1975). *Contemporary* deterrence theory is based on the "rational choice" view of human behavior; that individuals weigh the perceived risks and of both formal and informal sanctions in deciding whether or not to engage in an unauthorized or illicit activity (D'Arcy & Herath, 2011; Pratt et al., 2006).

GDT is one of the most widely applied theories related to behavioral IS studies and provides a prominent theoretical perspective in understanding cyber threats (Chen, Ramamurthy, & Wen, 2012; D'Arcy & Herath, 2011). Research has used deterrence theory as a foundation to predict user behavior in the workplace that is either supportive or non-compliant, particularly with regard to ISS (D'Arcy & Herath, 2011; Shepherd, Mejias, & Klein, 2014). Despite the solid foundation of GDT in criminology and empirical support predicting illicit behavior within organization settings (Pratt et al., 2006), deterrence theory may not fully explain human behavior with respect to IT threats (D'Arcy & Herath, 2011).

Traditionally, research relating to cyber-attacks and information security has been primarily considered a technical issue originating from the fields of computer engineering and computer science. These disciplines provided useful technical descriptions of how cyber-attacks are designed and executed with recommended IT safeguards for avoiding or mitigating their effects. Researchers however, advocate that understanding the complex and adverse effects of IT attacks requires the amalgamation of additional disciplines (Kumar et al., 2008; Liang & Xue, 2009; Pfleeger & Caputo, 2012). Using system dynamics and cybernetic theory, TTAT, and general deterrence theory as a theoretical foundation, the components of the research model for ISA and the assessment of ISS risk for emerging technologies are now examined.

RESEARCH MODEL AND HYPOTHESES

In developing the ISA-ISS Risk Assessment model, important distinctions must be made between *cyber-threats, cyber-exploits* and *cyber-attacks. Cyber-threats* can be defined as any potential action that may compromise the confidentiality, integrity, and availability of an information system (Whitman & Mattord, 2012) or violate information security policy (ISP; Bulgurcu et al., 2010; Zhao et al., 2013). Cyber-threats include, but are not limited to viruses, network worms, Trojan horses, denial of service (DoS) attacks, SQL injection, botnets, DNS attacks, virus hoaxes, steganography, cross-site scripting, and SCADA attacks (Ciampa, 2012; Goulder, 2011; Whitman & Mattord, 2012;).

Cyber-exploits refer to specific techniques or methods that attackers employ to breach a particular IS vulnerability or weakness (Denning & Denning, 2010; Simpson, Backman, & Corely, 2010). Examples of exploits are reconnaissance, footprinting, scanning, sniffing, spoofing, phishing, social engineering, wardriving, and hacking /cracking to name just a few.

The term *cyber-attacks* describes the materialization of a cyber-threat via the deliberate exploitation of a particular ISS weakness or vulnerability (Ciampa, 2012). Cyber-attacks have evolved from minimal threats associated with isolated intrusions to potential terrorist CBRN (chemical, biological, radiological, or nuclear) attacks on critical infrastructures.

Information Security Awareness (ISA)

The term *information security awareness* refers to a state of knowledge by which users or systems perceive the potentially negative impacts of cyber-attacks on their organization (Kruger &

Kearney, 2006; Liang & Xue, 2009; Pfleeger & Caputo, 2012) and are cognizant of their organization's information security policies (Bulgurcu et al., 2010; Mejias & Harvey, 2012). ISA has also been defined as the degree to which organizational members understand the importance of ISS, perceive options for appropriate levels of secure behavior and exercise options regarding their responsibility in maintaining the security of their IS resources (Hong & Thong, 2013). Bulgurcu et al. (2010) distinguishes between general information *security* awareness (ISA) and information security *policy* awareness (ISP). *General ISA* is defined as an employee's overall knowledge and understanding of the potential issues and ramifications of information security. Organization seek to create more ISA by encouraging security-positive behavior via SETA training, safeguarding information resources, and maintaining adherence to ISS policies (Bulgurcu et al., 2010; Kruger & Kearney, 2006).

Motivating employee awareness of the impact of cyber-attacks via mandatory ISA programs has been shown to increase awareness of security risks and related security precautions (Chen et al., 2012; Meso, Yi, & Shuting, 2013; Pfleeger & Caputo, 2012; Slusky & Parviz-Navin, 2012). Integral to ISA programs is the advocacy of threat avoidance behavior to safeguard IS resources against IT attacks (Bulgurcu et al., 2010; Liang & Xue, 2009). Knowledge of IT attacks is an important component of ISA (Bulgurcu et al., 2010) and an important factor in persuading employees to adapt appropriate threat avoidance behavior (Kim & Yong, 2012; Liang & Xue, 2009). Liang and Xue (2009) advocate that IT users must first develop an awareness of the nature of IT threats and the risks associated with a successful cyber-attack. TTAT then posits that when users perceive an imminent IT threat, they will incorporate avoidance behavior to reduce the occurrence or impact of an attack. It becomes critical therefore, that organizations educate and train users in adopting safe computing practices so that routine transactions and "safe-computing" behavior is undertaken almost subconsciously (Meso et al., 2013; Shepherd et al., 2014).

Research indicates, however, that information security is often regarded as secondary to user primary tasks (e.g., accessing information and processing and analyzing data). ISS policies and procedures are often relegated to the "back burner" when organizations face pressing issues such as production deadlines, process efficiencies, supply chain shortages, and the outsourcing of operations. When information security policies interfere with user convenience, users often ignore or even subvert secure practices as users and organizations are typically only rewarded for completing their primary tasks and not for completing them securely (Pfleeger & Caputo, 2012). Additionally, most organizations are unaware of even the most rudimentary procedures for educating their employees in securing information resources (Ko & Zafar, 2009; Pfleeger & Caputo, 2012). When perusing new sites, employees or consumers tend to infer or assume that privacy and safeguard features already exist. However, such inferences are not always correct (Kim & Yong, 2012). In this light, it is understandable that ISA programs frequently receive less priority and are allocated less development funds than other organizational functions and initiatives (Khansa & Liginlal, 2009; Spears & Barki, 2010).

A Multi-Disciplined Approach to ISA

Since ISA is a dynamic process, it is made even more difficult because ISS risk continuously changes (Kruger & Kearney, 2006; Zafar, 2011). Understanding the association between IT attacks, ISA and ISS risk assessment, suggests a multi-perspective or integrative approach for analysis (Dutta & Roy, 2008; Kumar et al., 2008; Liang & Xue, 2009). Lee and Lee (2002) and Lee, Lee, and Yoo (2003) developed holistic research models using attacker deterrence behavior and social criminology to explain the influence of ISA programs with regard to ISS vulnerabilities and risk. Jenkins, Durcikova, Ross, and Nunamaker (2010) proposed three controls (i.e., technical, educational, managerial) in a multi-perspective approach to appraise IT attacks. Dutta and Roy (2008) advocate a multi-perspective approach to ISS that combines technical, organizational and behavioral components. Siponen (2000) recommends two categories for improving ISA: frameworks categories (e.g., engineering disciplines) and content categories (e.g., interdisciplinary or non-engineering). The NIST (2006) recommends three criteria for assessing IT threats with regard to ISA: management security, operational security, and technical security (Stonebumer, Goguen, & Feringa, 2002). Bulgurcu et al. (2010) state that organizations enhance the success of their ISA programs when both technical and socio-organizational factors are considered. With the emergence of new and more pervasive IT, ISA programs encourage users to maintain security-positive behavior that supports their information security mission and regulatory compliance (Kim & Young, 2012; Kruger & Kearney, 2006).

This article posits that the analysis of IT threats from multiple perspectives provides a useful framework to explain the complexity of how organizations assess IT attacks, how threat avoidance behavior is incorporated into ISA programs and how ISA is associated with the assessment of ISS risk. Based on this literature, three perspectives (*technical knowledge, organizational impact*, and *attacker assessment*) are discussed and how they contribute to the understanding of IT attacks and the threat avoidance behavior inherent in ISA programs. (Figure 1). The association between ISA and the assessment of ISS risk is then explored.

Technical Knowledge

The largest volume of research relating to IT attacks appears to originate from the fields of computer engineering and computer science. These disciplines provide the requisite technical knowledge that is fundamental to understanding how IT system attacks are designed and executed

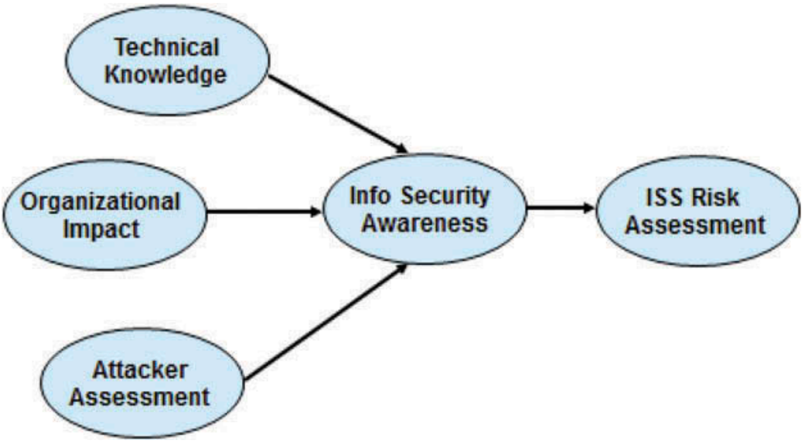

FIGURE 1 Proposed ISA and ISS Risk Assessment model.

and the IT controls that are recommended to avoid or mitigate system vulnerabilities. *System attacks* and *system vulnerabilities* are the two most prominent components that enhance *technical knowledge* of cyber-attacks (Ciampa, 2012; Goulder, 2011; Whitman & Mattord, 2012).

System Attacks

System attacks refer to the materialization of discreet or multiple cyber-threats on information systems, computer networks, and organizational information resources. System attacks may be undertaken by groups, entities, processes, or individuals that seek to alter or destroy IT assets in order to inflict damage and malfunction (Ciampa, 2012; Goulder, 2011; Whitman & Mattord, 2012). If successful, cyber-attacks may destroy or limit the functionality and availability of IS resources which may disrupt or destroy the critical operations of an organization. Cyber-attackers are continuously developing new skills and sophisticated exploits that are changing the "threatscape" with regard to emerging technologies and new user applications (McGavran, 2009; Schuessler, 2013). Knowledge of the operational underpinnings of cyber-attacks contributes to a technical understanding of IT system attacks (Ciampa, 2012; Goulder, 2011).

System Vulnerabilities

The term s*ystem vulnerabilities* refers to any weaknesses in the operating system, application software, network, or general ISS architecture that can be exploited to compromise a system's security and increase the probability of a cyber-attack. When system vulnerabilities are successfully exploited, cyber-threats materialize as cyber-attacks. System vulnerabilities include weak passwords, weak encryption, poor perimeter and network security, programming defects, hacker "backdoors" and lack of ISA training to name a few (Goulder, 2011; Whitman & Mattord, 2012). Two major types of vulnerabilities are *hard* (i.e., weakness in released software that are resolved with patches) and *soft* vulnerabilities (i.e., configuration errors in systems, networks) (Goulder, 2011). The existence of IS vulnerabilities continues to be one of the most important determinants of malicious IT attacks against compromised IS networks (Ciampa, 2012).

While IS vulnerabilities have existed before the advent of the Internet, the current proliferation of new technologies and user applications are increasingly being exploited within the current cyber-landscape (Hong & Thong, 2013; McGavran, 2009). Knowledge of the sources of system and network weaknesses contributes to better, technical understanding of cyber-attacks. Drawing from the fields of computer science and the feedback loop components of cybernetic theory (Carver & Scheier, 1982) this study posits that knowledge of system attacks and system vulnerabilities enhances a technical understanding of cyber-attacks and contributes to increased ISA of IT attacks (Mejias, 2012; Pfleeger & Caputo, 2012). Therefore, the following hypothesis is proposed:

$H_{1.0}$: Technical knowledge of IT attacks is positively associated with ISA.

Subsequently, the following hypotheses are proposed:

$H_{1.1}$: Knowledge of *system attacks* is positively associated with technical knowledge of IT attacks.
$H_{1.2}$: Knowledge of *system vulnerabilities* is positively associated with technical knowledge of IT attacks.

Organizational Impact

Traditionally in the United States, and increasingly in other countries, the business sector has financed the IS infrastructures that support organizational telecommunication and IS resources (Khansa & Liginlal, 2009; Shackelford, 2010). Approximately 80% to 90% of critical infrastructure and telecommunication networks are owned and maintained by the private business sector (U.S. Dept. of Homeland Security, 2013). As organizations are both supported and empowered by technology, the consequences of a successful IT attack on civil, governmental, private IS networks, and newer consumer-based technologies are profound (McGavran, 2009; Pfleeger & Caputo, 2012). Interestingly, the *type* of cyber-attack employed is less important than the impact of such an attack as the intended goal is the disruption of services and processes and the potential generation of financial and personal losses for an organization (Denning & Denning, 2010; Khansa & Liginlal, 2009). Evaluating which IT assets are critical to supporting key operations and assessing the impact of a cyber-attack on the financial profitability of organizations enhances the knowledge of the organizational impact of cyber-attacks.

Critical IT Asset Evaluation

Critical IT asset evaluation is a key consideration to understanding the trade-off between the probability of a cyber-attack and the relative costs of safeguarding a particular IT asset (Bodin et al., 2008; Herath & Herath, 2014; Kumar et al., 2008). As IS architectures become more "open" and new technologies become more pervasive, it becomes impossible to protect all IT assets from all potential IT threats. The partitioning of IT assets into different risk categories assists management to understand their relative criticality to organizational operations (Mejias & Harvey, 2012; Whitman & Mattord, 2012). The analysis of existing IS safeguards and their ability to mitigate IT attacks also assists management to identify potential threat vulnerabilities (Gordon, Loeb, & Lucyshyn, 2012; Spears & Barki, 2010). While most organizations lack the resources to safeguard against a wide range of IT attacks, the identification and categorization of critical IT assets allows the appropriate level of protection to be allocated to safeguard those IT assets generating the greatest impact on organizational processes.

Organizational Profitability

Cyber-attacks generate economic implications for existing and emerging technologies regardless of the nature or severity of the attack (Kumar et al., 2008; Pfleeger & Caputo, 2012). Cyber-attacks are recognized not only for their technical impact, but their economic impact as well (Herath & Herath, 2014). Revenue, profitability and financial performance have been shown to be adversely affected by IT attacks (Cavusoglu, 2010; Geng & Lee, 2013; Khansa & Liginlal, 2009; Mukhopadhyay et al., 2013; Zafar, 2011). The intimidating range of cyber-attacks and hacker exploits now facing most organizations has the potential to disrupt commercial web sites, decrease organizational and individual productivity, reduce customer trust, restrict data access, and negatively affect revenues and profitability of existing and emerging technologies (Khansa & Liginlal, 2009; Whitman & Mattord, 2012). ISA initiatives that support threat avoidance behavior have been shown to positively affect profitability, productivity, and competitive advantage

(Khansa & Liginlal, 2009; Moore et al., 2011; Spears & Barki, 2010;). A reduction in the severity of successful cyber-attacks implies fewer monetary damages for attack targets, reduced negative publicity, and a favorable impact on organizational revenues (Cavusoglu, 2010; Khansa & Liginlal, 2009; Ko, Osei-Bryson, & Dorantes, 2009). Based on these considerations this study posits that the identification of critical IT assets and knowledge of the effect of cyber-attacks on organizational profitability enhances the assessment of the organizational impact of cyber-attacks and contributes to the increased ISA of IT attacks. Therefore, the following hypothesis is proposed:

$H_{2.0}$: Assessing the organizational impact of IT attacks is positively associated with ISA.

Subsequently, the following hypotheses are proposed:

$H_{2.1}$: *Critical IT asset evaluation* is positively associated with the organizational impact of IT attacks.

$H_{2.2}$: Knowledge of o*rganizational profitability* is positively associated with the organizational impact of IT attacks.

Attacker Assessment

When IT attacks occur on existing or emerging technologies, analysis is often focused on the *technical* vulnerabilities of the targeted IT asset and less on the vulnerabilities relating to people, processes, and organizations (Pfleeger & Caputo, 2012; Spears & Barki, 2010). *Non-technical* factors underlying cyber-attacks have been increasingly considered to better understand the behavioral motivation and particular attack exploits employed by cyber-attackers (McGavran, 2009; Pfleeger & Caputo, 2012). IT countermeasures and safeguards may be more effective in deterring a particular cyber-attack when the behavioral motivation behind a particular attack is considered. As various cyber-exploits will target vulnerable IT assets and resources, organizations and individuals would be expected to employ threat avoidance behavior as described by TTAT in assessing attacker motivation, deterrence factors, and attacker profiles.

Attacker Motivation

Attacker motivation is an ideology that compels attackers to target particular IT assets and system vulnerabilities for purposes of status, ego, rebellion, blackmail, exploitation, and revenge or to facilitate economic, political, or social harm and disruption (Radcliff, 2004; Sawik, 2013; Stonebumer et al., 2002). The theory of planned behavior suggests that individual behavior can be predicted from attitudes and subjective norms. Together with perceived behavior controls they may explain a particular and demonstrated action (Bulgurcu et al., 2010). Understanding the behavioral motivations behind a particular IT attack provides useful knowledge for organizations to better assess cyber-attackers and deter related threat exploits. An understanding of the motivation and capabilities underlying cyber-attacks assists organizations to reinforce threat avoid behavior, improve ISA (Bulgurcu et al., 2010; Radcliff, 2004), and improve the assessment of cyber-attack risk (Hong & Thong, 2013; Stonebumer et al., 2002).

Deterrence Factors

Deterrence factors refer to the various actions, countermeasures, or IT controls developed to prevent intrusions or mitigate the impact of a successful cyber-attack (Ciampa, 2012; Sawik, 2013). Deterrence factors frequently refer to *technical* countermeasures such as anti-virus software, encryption, strong passwords, biometric scans, secure sites, firewalls, intrusion protection systems, redundancy, and honeypots to name a few (Sawik, 2013; Schuessler, 2013; Whitman & Mattord, 2012). *Non-technical* measures such as ISP, information assurance (IA), IT controls, SETA training, and disaster recovery planning are also considered effective deterrence strategies (Chen et al., 2012; Ciampa, 2012; Geng & Lee, 2013; He, Yang, & Yang, 2013; Meso et al., 2013; Yuan, et al., 2010; Zhao et al., 2013). Non-technical deterrence penalties such as lawsuits, prosecution, incarceration, and fines have also been employed to dissuade hackers from attacking vulnerable IT targets (Geng & Lee 2013; Png, Wang, & Wang, 2008).

New generation cyber-attacks target IT assets and system vulnerabilities with the least technical deterrence and with the least probability of detection (Goulder, 2011; Rees et al., 2011; Whitman & Mattord, 2012). Various studies demonstrate that deterrence measures reduce cyber-attacks and IT security incidents (Png & Wang, 2009; Png et al., 2008) and prove useful in understanding the motivations underlying malicious IT attacks (Bulgurcu et al., 2010). From an attacker's viewpoint, the exploitation of a system vulnerability discovered in a new or emerging technology should generate a greater likelihood of success with less effort and a reduced risk of deterrence (Denning & Denning, 2010; Png & Wang, 2009; Rees et al., 2011). GDT posits that deviant behavior (e.g., cyber-attacks) can be deterred if potential offenders fear detection and punishment (D'Arcy & Herath, 2011). Organizations that employ ISA, SETA and computer monitoring programs all serve as deterrents to reduce computer misuse (Rees et al., 2011; Shepherd, et al., 2014). Since laws or regulations may not adequately prevent cyber-attacks, the concept of deterrence as a threat avoidance behavior to reducing IT attacks has gained increasing prominence (Bulgurcu et al., 2010; Chen et al., 2012; Shepherd et al., 2014).

Attacker Profiles

Attacker profiles refer to a particular set of attributes, methods, techniques, and patterns of attacks employed by cyber-attackers when targeting a particular IT asset or vulnerability (Goulder, 2011; Simpson et al., 2010; Williams et al., 2006). Attackers seek the weakest security so that their patterns of intrusion are "target of opportunity" attacks (Radcliff, 2004). Additionally, attackers seek the least intrusive intervention for accessing IT assets with the least probability of detection (Denning & Denning, 2010; Radcliff, 2004). Williams et al. 2006, developed attacker profiles to detect cyber-attacks via pattern classifications of known and authentic attack models. Chirita, Wolfgang, and Zamfir (2005) propose metrics for analyzing rating patterns of cyber-attackers so that their potential for attack behavior could be profiled and deterred. The closer an attacker imitates a known attack model or profile, the closer the chance of detection (Rees et al., 2011). Since human behavior is complex, understanding patterns of potential cyber-attackers particularly with regard to new and emerging technologies is useful in developing behavioral profiles for understanding cyber-attacks (Radcliff, 2004; Rees et al., 2011). Knowledge of attacker behavior also assists organizations in developing threat avoidance strategies to determine which IS resources would most likely be targeted (Simpson et al., 2010). Drawing from general deterrence theory this study posits that knowledge of attacker motivation, deterrence factors, and attacker profiles enhance attacker assessment of IT attacks and contributes to increased ISA of IT attacks. Therefore, the following hypothesis is proposed:

$H_{3.0}$: *Attacker assessment* of IT attacks is positively associated with ISA.

Subsequently, the following hypotheses are proposed:

$H_{3.1}$: Knowledge of *attacker motivation* is positively associated with attacker assessment of IT attacks.
$H_{3.2}$: Knowledge of *deterrence factors* is positively associated with attacker assessment of IT attacks.
$H_{3.3}$: Knowledge of *attacker profiles* is positively associated with attacker assessment of IT attacks.

Information System Security (ISS) Risk Assessment

Assessing cyber-risk from the impact of a successful cyber-attack is fundamentally different from risk assessments relating to accidents or other phenomena that display inherently random failures (Guikema & Aven, 2010; Mukhopadhyay et al., 2013; Zafar, 2011). The ISS assessment risk process entails the ongoing identification of security threat vectors and vulnerabilities from new and emerging technologies with calculations for costs from a range of ISS countermeasures (Gordon et al., 2012; Khansa & Liginlal, 2009; Mukhopadhyay et al., 2013; Rees et al., 2011; Schuessler, 2013; Zhao et al., 2013).

Information security risk is often expressed as a combination of likelihood and impact (Pfleeger & Caputo, 2012). ISS risk assessments identify which IT assets support the most critical operations of an organization, the probability of damage to those IT assets, possible perpetrators of the malicious IT, estimates of recovery costs, related costs of network downtime, network unavailability, and related avoidance or mitigation to deter such cyber-attacks (Chen et al., 2011; Guikema & Aven, 2010; Png & Wang, 2009; Whitman & Mattord, 2012). A risk assessment of potential cyber-attacks is critical in identifying appropriate IS policy countermeasures, risk mitigation strategies and arriving at cost-effective defensive measures for minimizing risk and costs to the organization (Guikema & Aven, 2010; Mejias & Harvey, 2012; Puhakainen & Siponen, 2010; Zafar, 2011; Zhao et al., 2013). Only recently has the IS literature addressed the concept of ISS risk as related to ISA (Chen, Kataria, & Krishman, 2011; Jenkins et al., 2010; Pfleeger & Caputo, 2012; Spears & Barki, 2010).

As ISA is an ongoing process, motivating appropriate threat avoidance behavior toward new and emerging IT threats improves the assessment of ISS risk (Jenkins et al., 2010; Kruger & Kearney, 2006; Puhakainen & Siponen, 2010; Spears & Barki, 2010). The most general versions of ISS Risk Assessment models are based on decision science models which considers risk as a probability distribution of positive and negative outcomes (Bodin et al., 2008; Herath & Herath, 2014). Guikema and Aven (2010) analyzed ISS risk models that used game theory, probabilistic risk analysis and models that ignored individual attack probabilities and proposed an integrative ISS risk assessment. Chen et al. (2011) developed models to assess the failure risk of network availability due to software vulnerabilities by demonstrating the value of using diverse computer

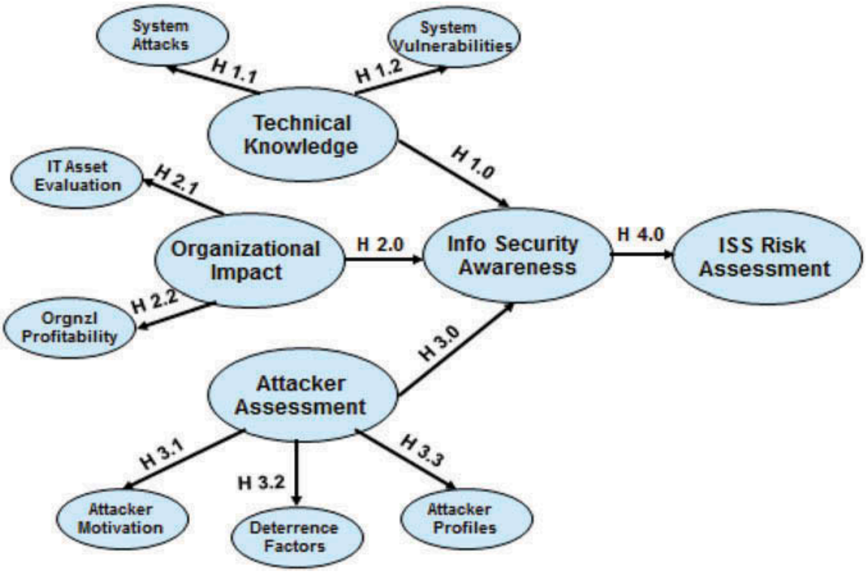

FIGURE 2 ISA-ISS risk assessment model with hypotheses.

configurations. Despite a realization of the importance of effective ISS since the 1990s, a scarcity continues in the leading IS journals of empirical studies relating to ISA and its association with the assessment of ISS risk (Bulgurcu et al., 2010; Guikema & Aven, 2010; Jenkins et al., 2010; Ko & Zafar, 2009). TTAT theory posits that as users become more aware of IT threats via ISA, they develop a better appraisal of ISS risk. Subsequently, they engage in threat avoidance behavior and coping behavior to distance themselves from a particular malicious or undesirable IT state (Liang & Xue, 2009; Mukhopadhyay et al., 2013). Therefore, it would be reasonable to assume that an increased awareness of IT attacks via the threat avoidance component in ISA programs would compel organizations and individuals to utilize appropriate risk assessment strategies to avoid cyber-attacks and safeguard their IS assets. Therefore the following hypothesis is proposed:

$H_{4.0}$: *Information security awareness* of IT attacks is positively associated with the *assessment of ISS risk*.

Based on the previous discussion, Figure 1 is expanded to include the seven aforementioned first order constructs grouped into their respective second order constructs of *technical knowledge, organizational impact*, and *attacker assessment* (Figure 2). The association between these constructs using CFA and structural equation modeling is now explored for hypotheses testing.

METHODOLOGY

Instrument and Participants

A pilot questionnaire instrument based on the current ISS literature was initially distributed to 98 undergraduate business students from a large Midwest university for the purposes of instrument refinement, data analysis, and exploratory factor analysis. A final expanded and refined 116-item questionnaire instrument was ultimately developed and distributed to 445 ISS practitioners from industry, academia and governmental agencies within the West and Midwest United States. These respondents worked within the functional areas of technology, ISS, and/or IS technical support. Response to the paper-based questionnaire was voluntary with 245 of the 445 paper surveys (55.1%) returned (questionnaire available on request). The initial pilot study sample of 98 student respondents was excluded from the final data set of 245.

Measurement of Variables, Data Analysis, and Construct Validity

The seven first order constructs for each of the second order constructs (i.e., *technical knowledge, organizational impact, attacker assessment*) and the two endogenous constructs (*IS awareness, ISS risk assessment)* were measured and analyzed using 54 of the 116 survey items from the survey questionnaire. The remaining 62 survey items are beyond the scope of the current study and will be reported in subsequent research. All survey items used 7-point Likert scales. The data was examined for normality along skewness (< 2.00) and kurtosis (< 5.00) guidelines (Ghiselli, Campbell, & Zedeck, 1981) and no violations from normality were noted. The validity of the scales and related constructs was assessed for convergent validity, internal consistency, and discriminant validity.

Convergent validity was assessed via CFA to determine if all indicator survey items loaded on and measured a single underlying construct. Survey items that generated poor factor loadings on their respective constructs or cross-loaded on other constructs were eliminated from the model. As indicated in Table 1, all indicator items clustered appropriately on their respective first order constructs and above the 0.50 threshold level indicating practical significance and evidence of convergent validity (Fornell & Larcker, 1981; Hair et al., 1995). The average variance explained (AVE) for each construct in the models for this study (Table 1) was well above .50 also indicating convergent validity (Fornell & Larcker, 1981). Internal consistency was assessed by computing composite reliability (CR) for each second order construct. Composite reliability considers the possibility that indicator or manifest variables generate different factor loadings and error variances. In contrast, traditional coefficient alpha reliability scales (e.g., Cronbach's alpha) consider such error variances to be equal (Hair et al., 1995). Composite reliability scores for all constructs (Table 1) were above the recommended value of .70 indicating a good to very good degree of inter-item reliability or internal consistency (Fornell & Larcker, 1981; Nunnally & Bernstein, 1994).

With regard to discriminant validity, Table 1 indicates that factor loadings were distinctly different from each other. In Table 2, *diagonal* values represent the square root of the AVEs for a particular construct while the *off-diagonal* values represent the correlations between constructs. As Table 2 indicates, all square roots (i.e., diagonal values) of the AVE between a particular construct were all greater than the correlations *(off-diagonal values)* shared by them and the other constructs (Fornell & Larcker, 1981). This indicated that the particular items within each construct shared more common variance than any variance shared with other constructs thereby, inferring discriminant validity (Anderson, 1987). Additionally, the correlations (i.e., off-diagonal values) between pairs of different constructs (e.g., system attacks vs. system vulnerabilities) were below the .85 threshold and significantly different from unity (1.0) indicating discriminant validity (Anderson, 1987; Fornell & Larcker, 1981). These validity checks confirm that our

TABLE 1
Factor Loadings, Average Variance Explained (AVE), Composite Reliability (CR)

	Technical knowledge					*Organizational impact*			
	1	*2*	*AVE*	*CR*		*1*	*2*	*AVE*	*CR*
SA11	0.116	**0.859**			**CAE22**	0.158	**0.843**		
SA12	0.388	**0.769**			**CAE24**	0.407	**0.701**		
SA14	0.411	**0.696**	**.606**	**.82**	**CAE25**	0.072	**0.807**	**.618**	**.83**
SV15	**0.844**	0.343			**OP33**	**0.899**	0.222		
SV16	**0.810**	0.247			**OP34**	**0.866**	0.130		
SV17	**0.854**	0.354			**OP35**	**0.810**	0.187	**.738**	**.89**
SV19	**0.831**	0.186	**.697**	**.90**					

	Attacker assessment				
	1	*2*	*3*	*AVE*	*CR*
AM38	**0.819**	0.081	−0.013		
AM40	**0.822**	−0.004	0.313		
AM42	**0.855**	0.094	0.187	**.692**	**.87**
DF45	0.074	**0.934**	0.132		
DF46	0.064	**0.938**	0.102	**.876**	**.93**
AP51	0.131	0.090	**0.902**		
AP52	0.204	0.162	**0.885**	**.815**	**.89**

	Information security awareness ISS risk assessment			
	1	*2*	*AVE*	*CR*
ISA2	**0.934**	−0.001		
ISA3	**0.933**	−0.038		
ISA4	**0.655**	0.267	**.724**	**.89**
ISRA28	0.006	**0.833**		
ISRA29	0.082	**0.814**		
ISRA48	0.121	**0.823**	**.678**	**.86**

SA, system attacks; SV, system vulnerabilities; CAE, critical IT asset evaluation; OP, organizational profitability; AM, attacker motivation, DF, deterrence factors; AP, attacker profiles; ISA, information security awareness; ISRA, information systems security risk assessment; AVE, average variance explained; CR, composite reliability. Rotation method: varimax with Kaiser normalization.

scales exhibited good psychometric properties (Nunnally & Bernstein, 1994) and that structural equation modeling was appropriate and justifiable for testing the research model depicted in Figure 2.

RESULTS

Confirmatory Factor Analysis (CFA) Models

CFA models were initially developed and tested for each of the three, second order constructs. The seven first order constructs (e.g., s*ystem attacks, IT asset evaluation, attacker motivation,*

TABLE 2
Discriminant Validity: Square Root of AVE of Construct Correlations for Second-Order Constructs

Technical knowledge	*System attacks*	*System vulnerabilities*	
System attacks	**.78**		
System vulnerabilities	.647	**.84**	
Organizational impact	*Critical IT evaluation*	*Organizational profitability*	
Critical information technology (IT) asset evaluation	**.79**		
Organizational profitability	.429	**.86**	
Attacker assessment	*Attacker motivation*	*Deterrence factors*	*Attacker profiles*
Attacker motivation	**.83**		
Deterrence factors	.172	**.94**	
Attacker profiles	.327	.195	**.90**

etc.) were modeled together to confirm that they loaded appropriately on their respective second order constructs. This approach provided evidence of measurement efficacy and reduced the likelihood of confounds in structural equation modeling due to measurement error (Anderson, 1987). First and second order CFA models were assessed for feasibility of parameter estimates, appropriateness of standard errors and statistical significance of estimates to assure that they exhibited the correct sign and size and were consistent with the underlying theory.

First-and second-order CFA models revealed no excessively large or small standard errors (which would indicate a poor model fit). Standardized residual co-variances for all CFA models were within the ± 2.58 threshold (Byrne, 2009). In assessing the CFA models, the Chi-square statistic (χ^2), p values, and the following fit indices were reported: relative fit index (RFI), incremental fit index (IFI), Tucker-Lewis index (TLI) comparative fit index (CFI) and the root mean square error of approximation (RMSEA). RMSEA for all CFA models was below the recommended 0.10 threshold limit (Browne & Cudeck, 1993). As presented in Table 3, the and p-values for the second order CFA models (Figure 3) were recorded at the desired $p < .10$ level. CFA models with these significance levels are not rejected since the statistic has traditionally been shown to be sensitive to sample size (Arbuckle & Wothke, 1999; Sharma, 1996) often yielding significant results for larger sample sizes and insignificant results for smaller sample sizes (Gulliksen & Tukey, 1958).

Given the sensitivity of the statistic to sample size, researchers have subsequently used other fit indices (Sharma, 1996). For example, in empirical analyses it is common practice to evaluate models using a to degrees of freedom (*df*) ratio (χ^2/df) rather than using an insignificant value (Bentler & Bonnet, 1980). All CFA models in our study generated χ^2/df ratios that were below the upper threshold of 3.00 (Browne & Cudeck, 1993). As illustrated in Figure 3, individual second order CFA models indicated good to excellent fit with most indices approaching or exceeding the 0.90 benchmark (Hair et al., 1995). All standardized regression coefficients for second order constructs were significant at the .05 level or better. The RMSEA indices for all CFA models were below the recommended 0.10 threshold (Browne & Cudeck, 1993). Standardized residual

TABLE 3
Fit Statistics: Second-Order CFA Models and Final ISA-ISS Risk Assessment Model

Fit statistic	*Technical knowledge*	*Organization impact*	*Attacker assessment*	*ISS-ISS Risk Assessment model*
χ^2	39.70	20.40	44.90	200.80
p value	.01	.01	.001	.01
$\chi^2/\ df$	2.83	2.50	2.93	1.99
RFI	.925	.913	.891	.861
IFI	.976	.980	.960	.908
TLI	.950	.946	.925	.871
CFI	.975	.979	.960	.905
RMSEA	.086	.079	.090	.063

RFI, relative fit index; IFI, incremental fit index; TLI, Tucker-Lewis index; CFI, comparative fit index; RMSEA, root mean square error of approximation.

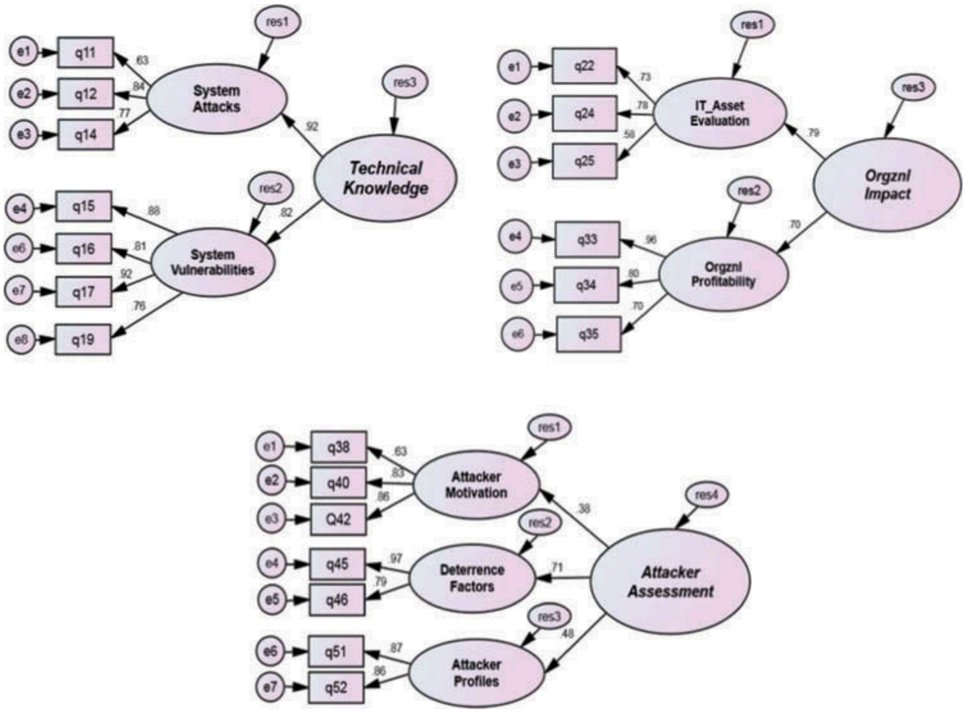

FIGURE 3 Confirmatory factor analysis models: Technical knowledge, organizational impact, and attacker assessment.

co-variances for all CFA models displayed no unusually large indicator estimates that were greater than ± 2.58 indicating that the second order CFA models for the constructs were valid to include as second order constructs in the larger, final structural model.

Final Structural Model

A preliminary ISA-ISS risk structural model initially generated poor to moderate fit statistics and negative error variances. In cases where model refinement was required, indicator or survey items were assessed and deleted one at a time and the fit of the refined model was reassessed, reflecting the process of logical model building and model purification (Anderson, 1987; Hair et al., 1995). Based on the CFA results from the first and second order models, the final structural model (Figure 4) indicated no negative error variances and no unacceptable correlations (≥ 1.00; Byrne, 2009). All indicator items generated measurement factor loadings at $p < .05$ or better. All first order constructs generated significant standardized path coefficients on their respective second order constructs at $p < .05$. The final structural model generated good to very good fit indices (Table 3) with standardized path coefficients from all three second order constructs loading onto the construct *ISA* at $p < .05$ or better. As shown in Figure 4, the path coefficient from technical knowledge to ISA ($\beta = .33$) was significant at the $p < .05$ level. The path coefficient from organizational impact to ISA ($\beta = .44$) was significant at the $p < .01$ level. The path coefficient from attacker assessment to ISA ($\beta = .43$) was significant at the $p < .05$ level. Finally, the path coefficient from ISA to ISS risk assessment was substantial ($\beta = .61$) and significant ($p < .01$).

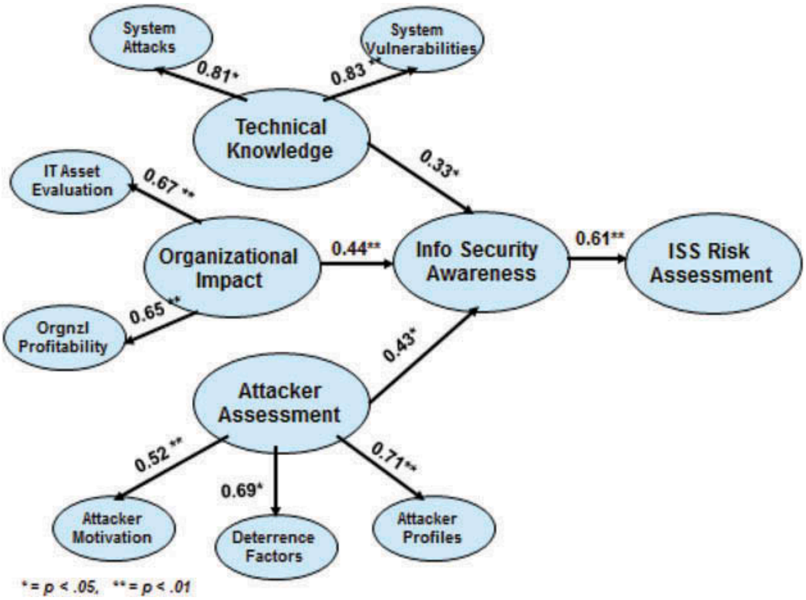

FIGURE 4 ISA-ISS Risk Assessment model with path coefficients.

DISCUSSION OF RESULTS

This study identified three constructs: *technical knowledge, organizational impact* and *attacker assessment* that provided an integrated perspective of cyber-attacks and its association with ISA and ISS security risk assessment. The validation of our CFA models and related fit statistics indicate strong support for the final ISA-ISS Risk Assessment model. As summarized in Table 4, research results support $H_{1.0}$ ($\beta = .33$, $p < .05$), which predicted that technical knowledge of IT attacks is positively associated to ISA. Hypotheses 1.1 (system attacks) and 1.2 (system vulnerabilities) were also supported as they generated positive and significant path coefficients with their second order construct, *technical knowledge*. These results support previous computer science literature that knowledge relating to the operational underpinning of system attacks and system vulnerabilities provide a technical foundation for understanding IT threats, exploits and cyber-attacks.

These results support $H_{2.0}$ ($\beta = .44$, $p < .01$), which predicted that the assessment of the organizational impact of IT attacks is positively related with ISA. Hypotheses 2.1 (IT asset evaluation), and 2.2 (organizational profitability) were also supported as they generated positive and significant path coefficients with their second order construct, *organizational impact*.

TABLE 4
Summary of Results and Testing of Hypotheses

Hi	*Hypothesis*	*Supports hypothesis?*	*β, p Levels*
$H_{1.0}$	***Technical knowledge* of information technology (IT) attacks is positively associated with information security awareness (ISA)**	Yes	$\beta = .33, p < .05$
$H_{1.1}$	Knowledge of *system attacks* is positively associated with technical knowledge of IT attacks	Yes	$\beta = .81, p < .05$
$H_{1.2}$	Knowledge of *system vulnerabilities* is positively associated with technical knowledge of IT attacks	Yes	$\beta = .83, p < .01$
$H_{2.0}$	**Assessing the *organizational impact* of IT attacks is positively associated with ISA**	Yes	$\beta = .44, p < .01$
$H_{2.1}$	*Critical IT asset evaluation* is positively associated with o*rganizational impact* of IT attacks	Yes	$\beta = .67, p < .01$
$H_{2.2}$	Knowledge of o*rganizational profitability* is positively associated with *organizational impact* of IT attacks	Yes	$\beta = .65, p < .01$
$H_{3.0}$	***Attacker assessment* of IT attacks is positively associated with ISA**	Yes	$\beta = .43, p < .01$
$H_{3.1}$	Knowledge of a*ttacker motivation* is positively associated with attacker assessment of IT attacks	Yes	$\beta = .52, p < .01$
$H_{3.2}$	Knowledge of *deterrence factors* is positively associated with attacker assessment of IT attacks	Yes	$\beta = .69, p < .05$
$H_{3.3}$	Knowledge of *attacker exploits* is positively associated with attacker assessment of IT attacks	Yes	$\beta = .71, p < .05$
$H_{4.0}$	***ISA* of IT attacks is positively associated with the *assessment of information systems security risk***	Yes	$\beta = .61, p < .01$

These results support previous IS literature that knowledge relating to the effects of cyber-attacks on critical IT assets and organizational profitability contributes to increased ISA of IT attacks.

These results also support $H_{3.0}$ ($\beta = .43$, $p < .01$) which predicted that attacker assessment of IT attacks is positively associated with ISA. $H_{3.1}$ (attacker motivation), 3.2 (deterrence factors), and 3.3 (attacker profiles) also generated positive and significant path coefficients with their second order factor, *attacker assessment*. Interestingly, the path coefficients of *organizational impact* and *attacker assessment* with ISA were stronger than the path coefficients between *technical knowledge* and ISA. The comparatively lower path coefficient of technical knowledge with ISA may be partially explained by the fact that while cyber-attacks on system vulnerabilities have traditionally been explained from a technical perspective that non-technical factors may also generate substantial threat avoidance behavior inherent to ISA (Kim & Yong, 2012; Mejias, 2012). Specifically, the high path coefficients of the first order constructs *IT asset evaluation* ($\beta = .67$, $p < .01$) and *organizational profitability* ($\beta = .65$, $p < .01$), contributed to a strong path coefficient between the *organizational impact* construct and ISA ($\beta = .44, p < .01$). Additionally, the relatively strong path coefficient of the first order constructs *attacker motivation* ($\beta = .52, p < .01$), *deterrence factors* ($\beta = .69, p < .05$), and *attacker profiles* ($\beta = .71, p < .01$), contributed to the strong path coefficients between the attacker assessment construct and ISA ($\beta = .43, p < .05$). In particular, the high path coefficients of *attacker profiles* with the attacker assessment construct suggest that knowledge regarding cyber-attacker profiles may allow organizations to more effectively assess IT safeguards to mitigate particular IT attacks which contributes to increased ISA. These research finding suggest that economic factors (i.e., organizational impact, profitability), behavioral factors (i.e., attacker assessment), and technical factors may be important contributors to ISA.

Finally, these results support $H_{4.0}$, which predicted that ISA would have a positive association with ISS risk assessment. This path coefficients was substantial ($\beta = .61$; $p < .01$) and supports prior ISS literature stating that assessing cyber-attacks from a multi-discipline perspective enhances ISA and is positively associated with ISS risk assessment (Guikema & Aven, 2010; Mejias & Harvey, 2012; Siponen, 2005; Sveen et al., 2007). The substantial association between ISA and ISS risk assessment may be partially explained by the fact that while cyber-attacks have traditionally been explained by the computer science disciplines, the inclusion of organizational and behavioral explanations generate a more integrated understanding of ISA which may assist organizations in developing risk strategies for the assessment of ISS risk (Gordon et al., 2012; Mejias & Harvey, 2012; Simpson et al., 2010).

LIMITATIONS

Several limitations exist regarding the degree in which these findings may be generalized to a larger population. The first refers to the limitation of the research model, which was restricted to three perspectives (i.e., technical knowledge, organizational impact, attacker assessment) to understand IT attacks and its purported relationship to ISA. While these perspectives are referenced in much of the computer science and IS literature, additional perspectives such as governmental intervention or privacy legislation may offer additional insights into understanding IT attacks and its relationship to ISA.

The second limitation refers to the level of analysis undertaken in the current study. Specifically, the study did not differentiate between cyber-attacks posed by individual, organizations, or nation states on other individuals, organizations, or nation states. Intuitively, these factors could possibly constitute important "level of analysis" considerations. Nevertheless, while providing additional depth in knowledge, these levels of analysis would not discount our findings here.

Finally, the development of the survey items in the questionnaire and the associations between the perceptual measures in our study should be viewed with caution due to the potential for common methods variance. Since these self-reported measures originated from a same-source, same-instrument design, overlapping variances may lead to possible erroneous inferences that a substantive correlation exists between variables (MacKenzie, Podsakoff, & Podsakoff, 2011; Podsakoff & Organ, 1986). However, several remedial survey and data approaches to reduce common methods variance recommended by Lindell and Whitney (2001) and Podsakoff and Organ (1986) were incorporated in our analysis. These included *scale trimming* and *Harman's 1-factor test* confirming that one dominant factor did not account for the majority of the variance in our research results, which would suggest the likelihood of common methods variance.

IMPLICATIONS

Overall, the study found strong empirical support for the ISA-ISS Risk Assessment model with several implications for researchers and practitioners. First, understanding the complexity of the association between IT attacks, ISA and ISS risk assessment suggests an integrative or multi-perspective approach. The comparatively stronger path coefficients of the organizational impact and the attacker assessment constructs with ISA suggests that non-technical perspectives may provide useful insights and complement our understanding of IT attacks and its association with ISA.

Second, systems and cybernetic theory, the threat *avoidance* behavior components of TTAT and GDT may provide a more appropriate framework than traditional IS *adoption* theories such as innovation diffusion theory, technology acceptance theory, the theory of planned behavior, and the theory of reasoned action when analyzing IT threats and ISA initiatives. As the *adoption* of virtuous IT is not the same as the *avoidance* of malicious IT, IS adoption theories may not fully explain the phenomenon of organizations seeking threat avoidance from IT threats and cyber-attacks (Liang & Xue, 2009).

Third, organizations find it challenging to understand the nature of ISS risk and balancing multiple perceptions of ISS risk (Pfleeger & Caputo, 2012). When cyber-attacks exploit system vulnerabilities there is clear loss in the confidentiality, integrity and availability of information generating a range of implications for practitioners. The substantial association of ISA with ISS risk assessment suggests that as organizations become more cognizant of the impact of IT attacks, they may become better informed to assess the associated risks to their IS resources. Additionally, an increased awareness of the consequences of emerging cyber-attack vectors may induce organizations to invest more efficiently in their information security (Rees et al., 2011; Zhao et al., 2013).

Fourth, a multi-perspective view of IT attacks supports current legislative initiatives for increased cyber-security and ISA training (Bulgurcu et al., 2010; Kumar et al., 2008; Meso, 2013; Puhakainen & Siponen, 2010; Yuan et al., 2010). As organizations face new and emerging cyber-attacks on their operations, management may realize the value of assessing ISS risk from a technical, organizational, and behavioral perspective.

Fifth, previous studies have found that increased information security is often perceived as an inconvenience that interferes with the primary goals of a business (Kim & Yong, 2012; Pfleeger & Caputo, 2012). Convenience does not necessarily have to be sacrificed to enhance security as organizations may simply want users to internalize ISA guidelines as a prescriptive commitment to generate a greater awareness of information security. Finally, while organization may be cognizant of information security issues, they often fail to apply ISS practices correctly (Pfleeger & Caputo, 2012; Siponen, 2000). When confronted with uncertainty about the security of their interaction with a new technology, users assume that privacy and safeguard features already exist and will protect the safety of their actions (Kim & Yong, 2012; Pfleeger & Caputo, 2012). Indeed, while emerging technologies that employ TCP/IP protocols such as hypertext transfer protocol secure (HTTPS), secure sockets layer/transport layer security (SSL/TLS) and secure VPN tunneling with encryption can continue to achieve both better performance and enhanced security (Ciampa, 2012; Kim & Yong, 2012), organizations must continue to engender appropriate ISA behavior.

CONCLUSION

Drawing on concepts from systems dynamics and cybernetic theory, TTAT, and GDT, this study posits that the analysis of emerging IT threats from a multi-disciplinary perspective contributes to an understanding of ISA behavior and its association with ISS risk assessment. Contributions from different paradigms and disciplines helps researchers "make sense" of different research methods and assumptions underlying ISA and the assessment of ISS security risk as it applies to the proliferation of emerging technologies (Guikema & Aven, 2010; Siponen, 2005). In developing the ISA-ISS Risk Assessment model, the study found that the positive feedback loop or *avoidance* component from systems and cybernetic theory and the threat avoidance behavior components from TTAT and GDT provided a more appropriate framework for analyzing IT threats than traditional IS *adoption* models. Specifically, while traditional IS adoption models advocate an *approach* behavior (i.e., negative feedback loop) that decreases the distance between a current IT state and a desired IT state, *avoidance* models (i.e., positive feedback loop) seek to increase the distance of their current IT state away from a malicious IT state. This *approach* and *avoidance* distinction illustrates that the adoption of good IT is not equivalent to the avoidance of bad or malicious IT.

The results from testing the ISA-ISS Risk Assessment model found that the constructs *technical knowledge, organizational impact* and *attacker assessment* of IT attacks generated strong path coefficients with ISA. The path coefficients of the attacker assessment and organizational impact constructs with ISA were stronger than the path coefficients between the technical knowledge construct and ISA. Additionally, ISA was found to be strongly and significantly associated with ISS risk assessment. The authors believe these research findings address an important gap in current ISS research regarding the association of ISA and the assessment of ISS risk regarding new and emerging technologies. While ISA initiatives assessments have long been recognized as fundamental to information security, extant IS literature has been limited in providing useful frameworks for understanding the relationship between ISA and ISS risk assessment (Bulgurcu et al., 2010; Pfleeger & Caputo, 2012). The perilous implications are that if the impact of a changing IT threat landscape from new and emerging technologies is not well understood, an accurate assessment of ISS risk may neither be well understood. The authors encourage further research in this direction.

REFERENCES

Anderson, J. C. (1987). An approach to confirmatory measurement, structural equation modeling of organizational properties. *Management Science*, *33*, 525– 541.

Andriole, S. J. (2014). Ready technology: Fast tracking emerging business technologies. *Communications of the ACM*, *57*(2), 40–42.

Arbuckle, J. L., & Wothke, W. (1999). *Amos 4.0 user's guide*. Chicago, IL: Small Waters Corp.

Bentler, P., & Bonnett, D. (1980). Significance tests and goodness of fit in the analysis of covariance structures. *Psychological Bulletin*, *88*, 588–606.

Bodin, L., Gordon, L. A., & Loeb, M. P. (2008). Information security and risk management. *Communications of the ACM*, *51*(4), 64–68.

Browne, M., & Cudeck, R. (1993). Alternative ways of assessing model fit. In K. A. Bollen and J. S. Long (Eds.), *Testing structural equation models*. Newbury Park, CA: Sage.

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

Byrne, B. (2009). *Structural equation modeling with AMOS: Basic concepts, application, and programming* (2nd ed.). New York, NY: Routledge, Taylor and Francis Group.

Carver, C. S. (2006). Approach, avoidance, and self-regulation of affect and action. *Motivation and Emotion*, *30*, 105–110.

Carver, C. S., & Scheier, M. F. (1982). Control theory: A useful conceptual framework for personality-social, clinical, and health psychology. *Psychological Bulletin*, *92*(1), 111–135.

Cavusoglu, H. (2010). Making sound security investment decisions. *Journal of Information Privacy and Security*, *6*(1), 53–71.

Chen, P. Y., Kataria, G., & Krishman, R. (2011). Correlated failures, diversification, and information security risk management. *MIS Quarterly*, *35*, 397–422.

Chen, Y., Ramamurthy, K., & Wen, K. W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, *29*(3), 157–188.

Chirita, P. A., Wolfgang, N., & Zamfir, C. (2005). Preventing shilling attacks in online recommender systems (pp. 67–74). In *WIDM '05: Proceedings of the 7th Annual ACM International Workshop on Web Information and Data Management*. New York, NY: Web Information and Data Management (WIDM).

Ciampa, M. (2012). *Security+ guide to network security fundamentals* (4th ed.). Boston, MA: Course Technology, Cengage Learning.

D'Arcy, J., & 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.

Denning, P. J., & Denning, D. E. (2010). The profession of IT: Discussing cyberattack. *Communications of the ACM*, *53*(9), 29–31.

Dey, D., Lahiri, A., & Zhang, G. (2012). Hacker behavior, network effects, and the security software market. *Journal of Management Information Systems*, *29*(2), 77–108.

Dutta, A., & Roy, R. (2008). Dynamics of organizational information security. *System Dynamics Review*, *24*, 349–375.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural models with unobserved variables and measurement error. *Journal of Marketing Research*, *18*, 39–50.

Geng, X., & Lee, Y. J. (2013). Competing with piracy: A multichannel sequential search approach. *Journal of Management Information Systems*, *30*(2), 159–184.

Ghiselli, E. E., Campbell, J. P., & Zedeck, J. P. (1981). *Measurement theory for the behavioral sciences*. San Francisco, CA: Freeman Press.

Gibbs, J. P. (1975). *Crime, punishment, and deterrence*. New York, NY: Elsevier.

Gordon, L.A., Loeb, M. P., & Lucyshyn, W. 2012. Reducing the challenges to making cyber security investments in the private sector. In *Principal investigator's meeting TTA: Cyber economics*. College Park, MD: University of Maryland Smith School of Business.

Goulder, M. H. (2011). *Network defense: Security and vulnerability assessment*. Course Technology Series, *5*(5). Boston, MA: Cengage Learning, EC-Council Press.

Guikema, S. D., & Aven, T. (2010). Assessing risk from intelligent attacks: A perspective on approaches. *Reliability and System Safety*, *95*, 478–483.

Gulliksen, H., & Tukey, J. W. (1958). Reliability for the law of comparative judgment. *Psychometrika*, *23*(2), 95–110.

Hair, J., & Anderson, R. E., Tatham, R. L., & Black, W. C. (1995). *Multivariate data analyses*. Englewood Cliffs, NJ: Prentice Hall.

He, W., Yang, X., & Yang, L. (2013). Supporting case-based learning in information security with web-based technology. *Journal of Information Systems Education*, *24*(1), 31–40.

Herath, H. S. B., & Herath, T. C. (2014). IT security auditing: A performance evaluation decision model. *Decision Support Systems*, *57*(1), 54–63.

Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly*, *37*(1), 275–298.

Jenkins, J. L., Durcikova, A., Ross, G., & Nunamaker, J. F., Jr. (2010). Encouraging users to behave securely: Examining the influence of technical, managerial, educational controls on users' secure behavior. In *Proceedings of the 31st ICIS Conference* (pp. 3159–3168). St. Louis, MO: International Association for Computing and Information Systems.

Khansa, L., & Liginlal, D. (2009). Quantifying the benefits of investing in information security. *Communications of the ACM*, 52(11), 113–117.

Kim, B. C., & Yong, W. P. (2012). Security versus convenience? An experimental study of user misperceptions of wireless internet service quality. *Decision Support Systems*, *53*(1), 1–11.

Ko, M., Osei-Bryson, K. M., & Dorantes, C. (2009). Investigating the impact of publicly announced information security breaches on three performance indicators of the breached firms. *Information Resource Management Journal*, *22*(2), 1–21.

Ko, M., & Zafar, H. (2009). Current state of information security research in IS. *Communications of Association for Information Systems (CAIS)*, *24*(34), 557–596.

Kruger, H. A., & Kearney, W. D. 2006. A prototype for assessing information security awareness. *Computers and Security*, *25*, 289–296.

Kumar, R. L., Park, S., & Subramanian, C. (2008). Understanding the value of countermeasure portfolios in information systems security. *Journal of Management Information Systems*, *25*(2), 214–279.

Lee, J., & Lee, S. (2002). A holistic model of computer abuse within organizations. *Information Management and Computer Security*, *10*(2), 57–63.

Lee, S. M., Lee, S. G., & Yoo, S. (2003). An integrative model of computer abuse based on social control and general deterrence theories. *Information and Management 41*(6), 707–718.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, 33(1), 71–90.

Lindell, M. K., & Whitney, D. (2001). Accounting for common method variance in cross-section research designs. *Journal of Applied Psychology*, *86*(1), 114–121.

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement, and validation procedures in MIS and behavioral research: Integrating new, existing techniques. *MIS Quarterly*, *35*, 293–334.

McGavran, W. (2009). Intended consequences: Regulating cyberattacks. *Tulane Journal of Technology and Intellectual Property*, *12*, 259–275.

Mejias, R. J. (2012). An integrative model of information security awareness for assessing information systems security risk. In *Proceedings of the 45th Hawaii International Conference Systems Sciences* (pp. 3258–3267). Big Island, HI: IEEE Computer Society.

Mejias, R. J., & Harvey, M. (2012). A case for information security awareness programs to protect global information, innovation and knowledge resources. *International Journal of Transitions and Innovation Systems*, *2*, 302–324.

Meso, P., Yi, D., & Shuting, X. (2013). Applying protection motivation theory to information security training for college students. *Journal of Information Privacy and Security*, *9*(1), 47–67.

Moore, A. P., Cappelli, D. M., Caron, T. C., Shaw, E., Spooner, D. and Trzeciak, R. F. (2011). A preliminary model of insider theft of intellectual property. *Journal of Wireless Mobile Networks Ubiquitous Computing, and Dependable Applications*, *2*(1), 28–49.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. and Sadhukhan, S. K. (2013). Cyber-risk decision models: to insure IT or not? *Decision Support Systems*, *56*, 11–26.

National Institute of Standards and Technology (NIST). (2006). *NIST-100, Technology Administration, U.S. Dept. of Commerce, Information Security Handbook: A Guide for Managers*, prepared by P. Bowen, J. Hash, and M. Wilson. Washington, DC: NIST.

Nunnally, J. C., & Bernstein, J. H. (1994). *Psychometric theory* (3rd ed.). New York, NY: McGraw-Hill.

Pfleeger, S. L., & Caputo, D. D. (2012). *Leveraging behavioral science to mitigate cyber-security risk*. MITRE Technical Report 12-0499. Bedford, MA: MITRE Corporation.

Png, I. P. L., & Wang, C. Y. (2009). Information security: Facilitating user precautions vis-á-vis enforcement against attackers. *Journal of Management Information Systems*, 26(2), 97–121.

Png, I. P. L., Wang, C. Y., & Wang, Q. H. (2008). The deterrent and displacement effects of info security enforcement: International evidence. *Journal of Management Information Systems*, *25*(2), 125–144.

Podsakoff, P. M., & Organ, D. W. (1986). Self-reports in organizational research: Problems and prospects. *Journal of Management*, *12*, 531–544.

Pratt, T. C., Cullen, F. T., Blevis, K. R., Daigle, L. E., & Madensen, T. D. (2006). The empirical status of deterrence theory: A meta-analysis. In F. T. Cullen, J. P. Wright, and K. R. Blevins (Eds.), *Taking stock: The status of criminological theory* (pp. 37–76). New Brunswick, NJ: Transaction Publishers.

Puhakainen, P., & Siponen, M. (2010). Improving employee compliance through IS security training: An action research study. *MIS Quarterly*, *34*, 757–778.

Radcliff, D. (2004). What are they thinking? *Network World*, *21*(9), 40–44.

Rees, L .P., Deane, J. K., Rakes, T. R., & Baker, W. H. (2011). Decision support for cyber security risk planning. *Decision Support Systems*, *51*, 493–505.

Sawik, T. (2013). Selection of optimal countermeasure portfolio in IT security planning. *Decision Support Systems*, *55*(1), 156–164.

Schuessler, J. H. (2013). Contemporary threats and countermeasures: A security evaluation. *Journal of Information Privacy and Security*, *9*(2), 3–20.

Shackelford, S. J. (2010). Estonia years three later: A progress report on combating cyber attacks. *Journal of Internet Law*, *138*, 22–29.

Sharma, S. (1996). *Applied multivariate techniques*. New York, NY: John Wiley & Sons.

Shepherd, M. M., Mejias, R. J., & Klein, G. (2014). A longitudinal study to determine the effects of non-technical deterrence on reducing employee internet abuse frequency. In *Proceedings of the 47th Hawaii International Conference on Systems Sciences (HICSS)* (pp. 3159–3168). Waikoloa, HI: IEEE Computer Society.

Simpson, M. T., Backman, K., & Corely, J. (2010). *Hands on ethical hacking and network defense* (2nd ed.). Boston, MA: Thompson Course Tech.

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

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

Slusky, L. & Parviz-Navin, P. (2012). Student information security practices and awareness. *Journal of Information Privacy and Security*, *8*(4), 3–26.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, *34*, 503–522.

Stonebumer, G., Goguen, A., & Feringa, A. (2002). *Risk management guide for IT Systems*. Washington, DC: National Institute of Standards and Technology (NIST) U.S. Dept. of Commerce. Publication No. 800–3.

Sveen, F. O., Rich, E., & Jager, M. (2007). Overcoming organizational challenges to secure knowledge. *Information Systems Frontiers*, *9*, 481–492.

U.S. Dept. of Homeland Security. (2013). *Privacy Office, 2013 Report to Congress*. Washington, DC: U.S. Dept. of Homeland Security.

Whitman, M. E., & Mattord, H. J. (2012). *Principles of information security* (4th ed.). Boston, MA: Thompson Course Technology.

Wiener, N. (1948). *Cybernetics: Control and communication in the animal and the machine*. Cambridge, MA: MIT Press.

Williams, C.A, Mobasher, B., Burke, R., & Bhaumik, R. (2006). Detecting profile injection attacks in collaborative filtering: a classification-based approach. In *WebKDD'06: Proceedings of the 8th Knowledge Discovery on the Web International Conference on Advances in Web Mining and Web Usage Analysis* (pp. 167–186). Philadelphia, PA: Association for Computing Machinery.

Yuan, X., Jiang, K., Murthy, S., Jones, J., & Yu, H. (2010). Teaching security management with case studies experiences and evaluation. *Journal of Education Informatics and Cybernetics*, *2*(2), 25–30.

Zafar, H. (2011). Security risk management at a Fortune 500 firm: A case study. *Journal of Information Privacy and Security*, *7*(4), 23–53.

Zhao, X., Xue, L., & Whinston, A. B. (2013). Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements. *Journal of MIS*, *3*(1), 123–152.