Influence of Information Overload on IT Security Behavior: A Theoretical Framework

Full Paper

Tridib Bandyopadhyay
Kennesaw State University
tbandyop@kennesaw.edu

Humayun Zafar
Kennesaw State University
hzafar@kennesaw.edu

ABSTRACT

IT systems in organizational processes demand high level of security. The operational security of IT systems depends on end-user IT security behavior. The apparent importance of IT security requires that the end-users process and act on a multitude of IT security information and updates. Information overload (also known as infobesity, data smog etc.), in its manifest combinatorial forms of sensory, cognitive and communication overloads, impact the quality, speed and efficacy of decisions (Rogers, Puryear and Root, 2013). This research attempts to analyze similar impact of plausible IT security information overload on the IT security behavior of organizational end-users. A hierarchical model of the impact of information overload on organizational end-users' IT security behavior is proposed here. This research extends the literature of information overload in the area of information security and creates a framework for empirical validation of the theoretical underpinnings in the emerging area.

Keywords

Security, information overload, systems

INTRODUCTION

With increased use of information systems, businesses have had to deal with issues pertaining to information security, be it internal or external threats. Internal threats may come from accidental deletion or modification of data due to human errors, intentional damage by disgruntled current or former employees and employees' unauthorized access to confidential and sensitive data. Human error, although not deliberate, can still result in security breaches (Werlinger et al. 2009). Examples of human error include forgetting to change passwords, not logging off before leaving a workstation, or careless discarding of sensitive information (Warkentin and Willison 2009). This could be due to stress, lack of training or supervision, or bad system design (Lacey 2010). In this current context, we posit and argue that information overload can affect the level of performance of an organizational end user. D'Arcy et al. (2014) identified overload as one of the dark side elements of IT use, with the others being interruptions, addiction, misuse, and IT stress. Out of these, misuse was considered to be a proxy for security. The authors also specified that all or some of the dark side elements may in fact be related and synergistic, whereby providing an avenue for future research.

There is no universally agreed definition of information overload. It can mean several things, such as having more relevant information than one can assimilate or it might mean being burdened with a large supply of unsolicited information, some of which may be relevant (Butcher 1998). Regardless of the nature of the definition, as organizations face the realities of having to implement effective information security agendas, employees are saddled with numerous additional responsibilities. Some of these responsibilities include having to abide by a series of technological and policy oriented information security measures, both of which are considered essential for an effective security program (Hagen et al. 2008).

Organizational level studies that consider information overload and its impact on information security behavior on an organization's employees is currently lacking in IS research. Therefore, the purpose of this study is to investigate the impact of plausible information overload on the IT security behavior on employees.

LITERATURE REVIEW

This research considers the effect of information overload as applied to the area of organizational level end-user information security. In this section, we provide a brief review of relevant literature both for the generalized knowledge areas of information overload as well as information security.

The concept of information overload has been analyzed from several angles and multiple dimensions. The primary dimensions include a) *sensory overload*, when one or more sensory organs cannot keep up with the rate of incoming signals (Lipowski 1975), b) *cognitive overload*, where received stimuli cannot be fully or adequately analyzed by innate human abilities (Vollmann 1993), and c) *communication overload*, where the flow of communication inundates human capabilities to process them effectively (Meier 1963). More modern concepts of *knowledge overload* (Hunt and Newman 1997), and *information fatigue* (Wurman 1990) have also garnered certain support in the literature of information overload.

Information overload has also been analyzed under multiple contexts and backdrops. The main context areas are *Decision Processes*, e.g., product choice in retail marketing (Friedman 1977), *Search and Retrieval Processes*, e.g., the Internet search (Berghel 1997), and *Communication Processes*, e.g., electronic mailing (Bawden et al. 1999). In the domain of business knowledge, most always the concept of information overload has been analyzed to explain its negative impact on the performance of individuals in an organization (Schick and Gordon 1990). Our analysis of information overload in this current work also conforms to the above motivation - we intend to understand and measure the impact of information overload on the IT security behavior of the end users in a modern ICT-enabled (Information and Communication Technology enabled) organization.

In regard to organizational level information security, prior researchers have equated security as being a technical, socio-philosophical (Ratnasingham 1998), and/or a socio-organizational concern (Dhillon and Backhouse 2001). Such demarcation has possibly led to a situation where security is widely regarded as a field that lacks comprehensive research in information systems (Zafar and Clark 2009).

Past information security research has focused on insider threats (Sneha and Varshney 2009). Some researchers have also focused on security policy compliance. A compliance model for employees in an organization suggests that user compliant behavioral intention is influenced by the information security environment perceived by the users and their self-efficacy (Chan et al. 2005). User perception of the security environment is determined by an employee's observation of top management practices, direct supervisory practices, and socialization among coworkers. Another study that focused on why employees fail to implement information security threats and countermeasures even though they are aware of them (Workman et al. 2008) indicates that the extent to which people perceive the severity of a threat dictates how motivated they are to prevent it from happening.

Some researchers have equated job stress as being linked tangentially to overload. Job stress has been found to be key factor in employees violating security policies (D'Arcy et al. 2014). However, most research related to employee stress in organizations has focused primarily on job stress (Ayyagari et al. 2011; Kinman and Jones 2005; Moore 2000; O'Driscoll and Beehr 1994; Tu et al. 2005). Very few studies have covered areas that focus on the potential role of overload resulting in poor information security behavior. Lee et al. (2016) found that overload negatively impacts security behaviors of individuals in technical security-centered organizations.

Using a neutralization model to study the problem of employee information security violations, researchers found that employees rationalized their violations of security policies (Siponen and Vance 2010). Neutralization had a significant impact on an employee's intention to violate information systems security policies. However, formal and information sanctions had no significant effect. Using a mixed research design to examine user participation in IS security risk management (SRM), researchers found that user participation is an important factor for improving security control performance (Spears and Barki 2010). User participation raised organizational awareness of security risks and controls, facilitated alignment of SRM with business objectives, and improved environmental control.

Some studies have investigated employee security behaviors from an ethics perspective (Banerjee et al. 1998; Harrington 1996; Leonard and Cronan 2001). Ethics refers to informal norms and behaviors that may help deal with situations for which there are no formal rules or policies (Dhillon and Backhouse 2000). A limitation in this line of research is that there is a general difficulty in classifying behaviors as

being ethical or unethical. It is not always straightforward. According to prior studies (Calluzzo and Cante 2004), some undesirable behaviors related to use of organizational IT property were viewed as being neither ethical nor unethical. An example of such behaviors is downloading files at the workplace or at an educational institution from the Internet for personal use.

Straub and Nance (1990) addressed governance by looking at ways in which managers uncover security incidents and discipline the culprits of computer abuse. They created a normative model that formulated an approach to security administration and its evolutionary nature. They concluded that computer abuse is initially uncovered in one of three ways: internal controls, purposeful detective activity, or by accident. Regardless, the advent of an occurrence of computer abuse may necessitate a change in the way an organization views its security policies, hence highlighting the need for an evolving approach to security.

Greenway and Chan (2005) linked the existence of a firm's security policies with information privacy. They called for increased theoretically-grounded research using Institutional Approach and the Resource-Based View of the firm. Keeping with the privacy theme, Myyry et al. (2009) stated that privacy concerns lead employees to not adhere to security policies. Using the theory of Cognitive Moral Development (Kohlberg 1969) and a theory of motivational types of values (Schwartz and Zanna 1992), Myyry et al. concluded that moral reasoning, in part due to privacy concerns, was positively related to both hypothetical and actual compliance to security policies.

Ma and Pearson (2005) stressed the importance of standardized security models and their relation to increasing the level of information security in an organization. They empirically verified the international security management standard ISO 17799. One of the purposes of their study was to assist practitioners in recognizing the importance of academics and the theoretical models they create and verify.

As presented in this section, focusing on compliance with security policies, regulations, and standards is important. However, there is also a need to model the very structure of activities of individuals that either facilitates or hinders compliance. That is something that has seldom appeared in literature (Dhillon et al. 2016). In line with such observations, we propose a model of user behavior in IT security that focuses on overload issues emanating from information security compliance needs of modern complex IT systems.

RESEARCH MODEL AND HYPOTHESES

This study includes development of a model that incorporates factors based on prior research that impact IT security behavior of employees. Figure 1 presents the salient features of the proposed model.

Complexity in IT Systems

Cost effective value propositions have ensured penetration of IT systems in every level of business and decision processes; be it strategic, functional or transactional (Venkatraman 1994). Over time, information systems (henceforth IT systems) have evolved from being synonymous with data processing to complex work systems that are of strategic and tactical importance to a firm. Beginning with simple IT systems that automated stand-alone functions like the point of sale (PoS) or payroll systems, modern IT systems now synchronize business processes across multiple departments and/or organizations. As IT systems are called upon to accomplish involved tasks spanning multiple functionalities, these systems have grown in size and complexity as well. Once implemented in its entirety, current IT systems like ERP now synchronize and manage every transaction process in an organization (Shaul and Tauber 2013). Since IT systems facilitate every decision and productive process in an organization, their availability and proper functionality have also become critical to organizational survival and success. As a result, IT security management has also transformed into an expansive organizational paradigm.

Mukherjee (2008) states that for a strategic plan to be successful it has to extend beyond consideration of the technical aspects detailed therein. Therefore, it is not a surprise that researchers have mentioned the importance of understanding the socio-organizational aspects of information security (Dhillon and Backhouse 2001), the purpose of which is to integrate technical and managerial factors in order to analyze and evaluate information security levels at a firm. Technical factors can vary from data encryption to intrusion detection systems, whereas managerial level aspects mostly relate to policy management (Dhillon 2007). Tsoumas and Gritzalis (2006) support this notion by presenting a framework that

separates security requirements into technical controls and policy level statements. In this study, we also consider the dual nature of information systems security complexity: technical and managerial level.

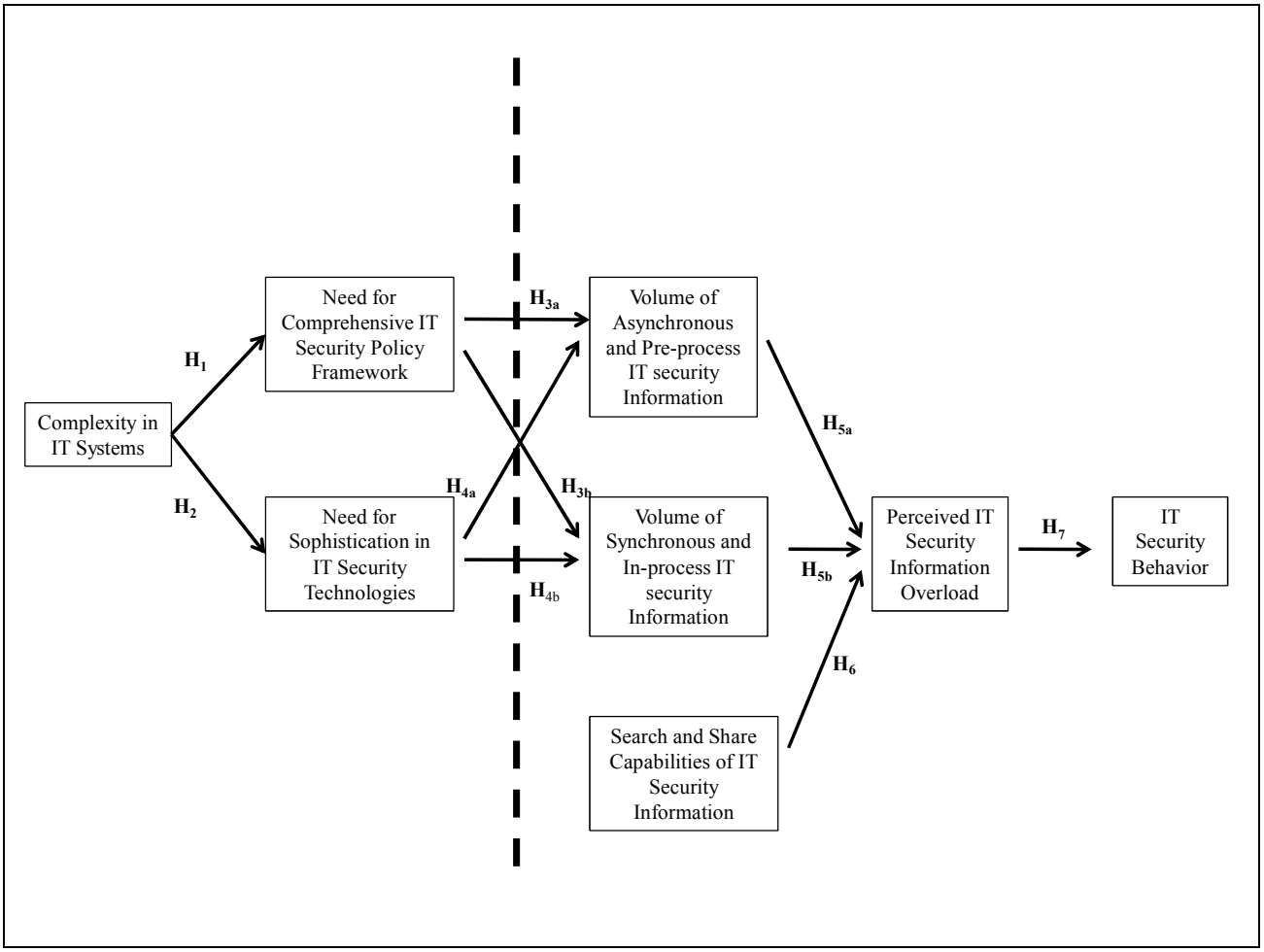

Figure 1: Research Model

Hypotheses Development

Fundamentally, traditional IS security has a "behavioral root" (Workman and Gathegi 2007), and is a subject of psychological and sociological actions of people (Parker 1981). Most prior research in organizational IS security has dealt with success and failure of security policies. General deterrence theory (GDT) has been used to investigate the effect of organizational deterrent measures on computer abuses by employees. For example, the Security Impact Model (Straub 1990) suggests that deterrent measures can reduce computer abuse by potential offenders if the risk of punishment is high (deterrent certainty) and penalties for violations are severe (deterrent severity).

Findings about the effectiveness of deterrence measures have been mixed. In one study (Kankanhalli et al. 2003), deterrent and preventive methods were found to positively impact information security effectiveness. On the other hand, severity of the deterrence method did not have a significant impact. In a different study, Lee et al. (2004) found that physical security systems (e.g. secured computer rooms) influenced a user's intention to install access control and intrusion detection software. Two other factors:

security policy and awareness did not have a significant impact, which is opposite to what was expected according to GDT.

Prior studies have also focused on employee compliance to security policies. In one such study, an Information Security Policy Compliance Model (Pahnila et al. 2007) suggests that a user's intention to comply with security policies is influenced by user attitude toward complying. Pahnila et al. [22] also state that attitude and intention are influenced by a mixture of negative and positive reinforcements. Examples of negative reinforcements include sanctions, threat appraisal, coping appraisal, and normative beliefs; whereas information quality of policies, facilitation conditions, and habits are examples of positive reinforcements. This model was tested via a survey of employees at a Finnish company. Results showed that sanctions did not have a significant impact on user intention to comply with information security policies. This result was contrary to the prediction of GDT.

Organizations employing IT systems that couple business processes across multiple firms (e.g., supply chain management systems) face higher order complexity requiring further sophistication in IT security policy framework. Specialized IT security policies are mandated to manage the varying risk profiles, organizational capabilities and structures of the partnering firms in the areas of trusted communication including data sanitation, bona fide use of extranet and VPN services, to name a few (Panko 2010).

Global organizations may also face hurdles related to compliance with various country specific regulations. For example, a company may need to consider both U.S. and European regulations. This is considered as one of the critical requirements for an organization, since it can consist of a patchwork of disparate and over-lapping state and federal regulations, along with privacy rules laid out by individual corporate partners. Within the European Union, a company may have to deal with the data protection directive, which unlike U.S. regulations such as HIPPA or Sarbanes-Oxley acts, provides few specifics as to how these privacy requirements should be met. While creating an IT security policy program, management therefore focuses on the need to establish a consistent set of requirements common to various U.S. and EU jurisdictions, while keeping in mind its own standards for protecting any applicable customer and supplier data. Therefore, we posit:

H1: Complex IT systems will result in a greater need for comprehensive IT security policy frameworks.

As systems become more complex so do the technical requirements for enhancing security. No company is immune to threats such as cyber-theft, and cyber-espionage by hackers, malware, and malicious insiders. This aspect of IT security research encompasses strategies such as role based access control, encryption standards, and physical security (Dhillon 2007). Role based access controls provide access privileges to employees based on their position in an organization. Encryption standards pertain to the type of encryption that may be used. Full disk encryption can be reached through technologies such as the Trusted Platform Module (TPM) technology. TPM technology makes it almost impossible to recover data from an encrypted drive if it is not attached to the computer in which it was originally installed.

With IT systems becoming more complex and involved in their implementation and use, the supporting information and network assets have also gained further prominence requiring organizations to implement sophisticated IT security measures to protect them from unauthorized and unintended uses. One notable augmentation in direction is the paradigm of 'IT security in layers'. In this, organizations secure their network perimeter with preventive technologies (e.g., firewall) and additionally engage detection technologies (e.g. IDS) to monitor suspicious network traffic inside its network perimeter. The need to implement and manage multiple IT security technologies and optimally synchronize the layered regimes of defense further upends the sophistication of these IT security technologies.

Even in an age where most attacks occur via the Internet, physical security is still an important part of a security framework. Organizations may implement this feature across various layers (Panko 2010). For example, visitors entering a company's premises may not be allowed to go through without an escort or connect to a network without being identified and security vetted. They may be physically searched by a guard if an organization desires. Also, all lobbies, corridors, and common areas may have closed circuit television monitoring. Therefore, we posit:

H2: Complex IT systems will result in a greater need for sophisticated IT security technologies.

A comprehensive IT security policy framework requires that the stakeholders of the IT systems be (i) aware of the contexts and contents of such policies, (ii) be trained to implement and translate the policies

during their productive behavior involving the IT systems and (iii) be educated to theorize, plan and implement an IT security policy doctrine that remains valid, dynamic, timely, and bears goal congruity with the mission, vision and goal of the overall organization (Whitman and Mattod 2004).

End-users of IT systems (e.g. a teller in a banking organization), whose productive functions require that they observe basic IT security behavior is the group that is focused in the IT security awareness program. This involves sharing IT security incidents that take place in and outside the organization, contextualized scenarios where such incidents could peril a business process of the organization and other symbolic and hypothesized scenarios. In order to counter general forgetfulness that erodes the efficacy of awareness initiatives over time, such sharing and broadcasting of IT security incidents are required to be periodically repeated in changed format to retain interest in the recipients. Since productive processes of most all employees these days involve IT systems, such awareness programs are typically organization wide, and are repeated in regular intervals several times during a month/year.

Employees who directly work with one or more IT systems (e.g. a network administrator) are the focus of more direct and intense training initiatives involving IT security measures. The IT security policies are implemented with the help of these employees and as such they are directly involved in maintaining the required level of IT security defense. Beyond usual IT securities specific to IT systems and their updates, salient events inside and outside an organization, (e.g. an upcoming requirement of a new regulatory compliance) require that these IT workers undergo IT security training initiatives in a regular manner such that their productive behavior remain cognizant of the impacts in the IT security aspect of the IT systems.

In order to maintain its capability to manage the organizational IT security in a relevant, efficient and timely manner, organizations charge certain employees to strategize, plan and manage the overall IT security paradigms and processes. These employees require vision to strategize and plan for organizational IT security innovations, collaborate with peers outside organizations and provide the intellectual backbone of the IT security program of an organization (Whitman and Mattord, 2004). Special educational initiatives, which may often involve outside specialists, are needed to create and maintain such higher order skills.

Beyond such asynchronous and pre-process information that remain prerequisite to adequate IT security behavior of the organizational employees, IT security policy frameworks also provision for in-process assistance to maintain organizational IT security postures and standard. For example, end-users are reminded with pop-up information to properly formulate their passwords and keys while they are at it, notifications are populated for IT workers to ensure currency of security certificates of an application etc. The specific nature of these sets of information hinges on the fact that they are synchronously pushed while the productive process is underway. From the above considerations, we posit:

H3a: Complex IT security frameworks will result in a greater need for asynchronous and pre-process IT security information.

H3b: Complex IT security frameworks will result in a greater need for synchronous and in-process IT security information.

While sophisticated IT security technologies provide better protection to the organizational IT assets, managing these technologies increase overhead in terms of additional awareness, training and education needs. For example, an organizational decision to adopt network and host based intrusion detection devices (IDS) in its network involves additional implementation of training programs for its IT employees. The same decision will also require multiple waves of awareness messages to all end-users apprising them of their expected network behavior including instructions to interpret messages of behaviors in aberration. In case the decision to implement detection technologies comes in presence of perimeter security technologies, such decision may also translate to additional educational needs for certain employees who are responsible to optimize the network assets or provide optimal IT risk management advisements for the IT systems of the organization (Holden 2003).

Since sophisticated IT security systems are sensitive in nature, their efficient use requires increased oversight and communication in order to resolve in-process decision junctures. More often than not, sophisticated IT security systems are also dynamic in nature. For example, the success of IDS depends on the network usage and congestions factors, which further requires altered coordination between the

multiple hosts and nodes of the network. On the other hand, deployed IDS may generate status messages as well as varied graphs and charts for specific employees or departments.

In essence, sophisticated IT security systems are costly in terms of their oversight and management needs which, among other things, may translate to higher information flows to the employees and departments of an organization, both in the asynchronous and synchronous mode while these systems remain deployed in operation. As a result, we envision:

H4a: Sophisticated IT security technologies will lead to higher levels of asynchronous and pre-process IT security information for organizational users.

H4b: Sophisticated IT security technologies will lead to higher levels of synchronous and in-process IT security information for organizational users.

As IT systems are deployed and policy frameworks are implemented, business processes experience broadening of management of information that are needed or created by these systems. While deployment of IT systems is focused toward organizational value addition, such benefits may not accrue unless such overhead information is properly managed. Unfortunately, there are concerns that such information management may appear to be at variance with productive behavior of the users and enablers of the IT systems. Studies suggest (Edmunds and Morris 2000) that in presence of multiple pieces of information, human beings may be overloaded and overwhelmed, and may find it hard to pick the most relevant information and modify their productive actions accordingly. Since more sophisticated technologies and more comprehensive policy frameworks in IT security may increase such overhead information, we posit:

H5a: Multitude of asynchronous and pre-process IT security information delivered to the end-users and enablers of sophisticated IT systems will lead to perceived information overload.

H5b: Multitude of synchronous and in-process IT security information delivered to the end-users and enablers of sophisticated IT systems will lead to perceived information overload.

Over the last decade, organizations have implemented knowledge management systems. Such initiatives have not restricted themselves to productive processes only, knowledge elements have been codified in IT security area as well. For example, canned queries like FAQs in best IT security practices for IT systems and subsystems exist in most modern organizations to benefit the end-users (Lunacek, 2009). With the advent of the Web 2.0 technologies many organizations also allow organizational blogs and wikis which discuss IT security aspects of their relevant systems. Since these blogs and wikis are searchable databases and are available over the Internet, organizational end-users are trained as such and are expected to take advantage of them when needed. Specific instances resembling the predicament at hand can also be inquired with a knowledgeable coworker with the help of in-house instant messaging systems. These facilities and options tend to provide ready help for better IT security decisions by the end-users, and may alleviate, in part, the need to recollect and judge a pertinent information that is formally communicated earlier or in-process. Consequently, we posit:

H6: Search and share capabilities of IT security information will alleviate information overload of IT security.

Finally, the productive behavior of the stakeholders of IT systems, especially the end-users and the IT enablers are impacted by their overall sense of sufficiency and adequacy of information relevant to the security of the systems. Thus:

H7: Perceived overload in IT security information will affect the IT security behavior of an organizational employee.

Research Method

We plan to use a mixed methods research approach to investigate our research question. As specified earlier, the relation between information overload and security behavior has not been researched. Similarly, there is not much research in the information overload arena to begin with. Therefore, using open-ended questions through interviews and focus groups will assist us in collecting

data for constructs for which appropriate quantitative measures may not be present or possible. For the rest we plan to use surveys to collect data for analysis.

Future Work and Concluding Thoughts

IT systems have now been integrated in most business processes in an organization. This has given rise to a scenario of high dependence on IT systems across the spectrum of business organizations. IT security breaches are often one of the top 5 important concerns of CIOs' decision making (Ponemon Studies, 2015). While the benefits of IT systems are compelling, care must be exercised to keep these systems in proper functioning mode and ensure that they are not misused or abused. Algorithmic controls in the computing paradigms and risk management in the organizational use of these IT systems cannot be ensured without proper involvement of the end-users of the IT systems. Toward that end organizations institutionalize planned initiatives and interventions to have their end-users educated and trained in desirable IT security behaviors. Pervasive IT security focused situational and contextual awareness campaigns are also administered regularly to reinstate, remind and refresh the desirable IT security behaviors of the end-users. Over time, these initiatives are capable to generate stresses in terms of overloading the end-user IT security management regime. Troubling symptoms of dysfunctional end-user IT security decision making may surface in terms of casual oversight, benign mistakes and sub-optimal decisions and mistaken heuristics, to name a few. When an organization is able to appreciate the possibility of such information overload in the end-user community, fact finding missions leading to better management of IT resources and assets will result. This research is an initial attempt in this direction. In the current state, our proposed model integrates and contextualizes disparate constituents of information overload in the area of IT security. This is a nascent research in IT security information overload and to the best of our knowledge, this happens to be one of the very few attempts to model information overload as a factor in end-user IT security behavior in an organizational set up. Our future plan include further honing of the constructs of the model with the help of organizational focus groups, development of an adequate survey instrument and administer the instrument to assess the presence and impact of information overload in the organizational IT security area. We hope to bring empirical insights in the IT security information overload and its impact on decisional quality as we are able to complete this research in future.

REFERENCES

Ayyagari, R., Grover, V., and Purvis, R. 2011. "Technostress: Technological Antecedents and Implications," *MIS Quarterly* (35:4), pp. 831-858.

Banerjee, D., Cronan, T. P., and Jones, T. W. 1998. "Modeling It Ethics: A Study in Situational Ethics," *MIS Quarterly* (22:1), pp. 31-60.

Bawden, D., Holtham, C., and Courtney, N. 1999. "Perspectives on Information Overload," *ASLIB Proceedings*: MCB UP Ltd, pp. 249-255.

Berghel, H. 1997. "Cyberspace 2000: Dealing with Information Overload," *Communications of the ACM* (40:2), pp. 19-24.

Butcher, H. 1998. *Meeting Managers' Information Needs*. Europa Publications.

Calluzzo, V. J., and Cante, C. J. 2004. "Ethics in Information Technology and Software Use," *Journal of Business Ethics* (51:3), pp. 301-312.

Chan, M., Woon , I., and Kankanhalli, A. 2005. "Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior," *Journal of Information Privacy and Security* (1:3), pp. 18-41.

D'Arcy, J., Herath, T., and Shoss, M. K. 2014. "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective," *Journal of Management Information Systems* (31:2), pp. 285-318.

D'Arcy, J., Gupta, A., Tarafdar, M., and Turel, O. 2014. "Reflecting on the "Dark Side" of Information Technology Use," *Communications of the Association for Information Systems* (35:1), pp. 109-118.

Dhillon, G. 2007. *Principles of Information Systems Security: Text and Cases*. Hoboken, NJ: Wiley.

Dhillon, G., and Backhouse, J. 2000. "Information System Security Management in the New Millennium," *Communications of the ACM* (43:7), pp. 125-128.

Dhillon, G., and Backhouse, J. 2001. "Current Directions in Is Security Research: Towards Socio-Organizational Perspectives," *Information Systems Journal* (11:2), pp. 127-153.

Dhillon, G., Samonas, S., and Etudo, U. 2016. "Developing a Human Activity Model for Insider Is Security Breaches Using Action Design Research," in *Ict Systems Security and Privacy Protection: 31st Ifip Tc 11 International Conference, Sec 2016, Ghent, Belgium, May 30 - June 1, 2016, Proceedings,* J.-H. Hoepman and S. Katzenbeisser (eds.). Cham: Springer International Publishing, pp. 49-61.

Edmunds, A., and Morris, A. 2000. "The Problem of Information Overload in Business Organisations: A Review of the Literature," *International journal of information management* (20:1), pp. 17-28.

Friedman, M. 1977. "Consumer Use of Informational Aids in Supermarkets," *Journal of Consumer Affairs* (11:1), pp. 78-89.

Greenaway, K. E., and Chan, Y. E. 2005. "Theoretical Explanations for Firms' Information Privacy Behaviors," *Journal of the Association for Information Systems* (6:6), pp. 171-198.

Hagen, J., Albrechtsen, E., and Hovden, J. 2008. "Implementation and Effectiveness of Organizational Information Security Measures," *Information Management & Computer Security* (16:4), pp. 377-397.

Harrington, S. 1996. "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions," *MIS Quarterly* (20:3), pp. 257-278.

Holden, G. 2003. *Guide to Firewalls and Network Security: Intrusion Detection and Vpns*. Boston, MA: Course Technology Press.

Hunt, R. E., and Newman, R. G. 1997. "Medical Knowledge Overload: A Disturbing Trend for Physicians," *Health Care Management Review* (22:1), pp. 70-75.

Kankanhalli, A., Teo, H. H., Tan, B. C. Y., and Wei, K. K. 2003. "An Integrative Study of Information Systems Security Effectiveness," *International Journal of Information Management* (23:2), pp. 139-154.

Kinman, G., and Jones, F. 2005. "Lay Representations of Workplace Stress: What Do People Really Mean When They Say They Are Stressed?," *Work & Stress* (19:2), pp. 101-120.

Kohlberg, L. 1969. "Stage and Sequence: The Cognitive-Developmental Approach to Socialization," in *Handbook of Socialization Theory and Research,* D. Goslin (ed.). Chicago: Rand McNally, pp. 347-480.

Lacey, D. 2010. "Understanding and Transforming Organizational Security Culture," *Information Management & Computer Security* (18:1), pp. 4-13.

Lee, C., Lee, C. C., and Kim, S. 2016. "Understanding Information Security Stress: Focusing on the Type of Information Security Compliance Activity," *Computers & Security* (59), pp. 60-70.

Lee, S. M., Lee , S. G., and Yoo, S. 2004. "An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories," *Information & Management* (41:6), pp. 707-718.

Leonard, L. N. K., and Cronan, T. P. 2001. "Illegal, Inappropriate, and Unethical Behavior in an Information Technology Context: A Study to Explain Influences," *Journal of the Association for Information Systems* (1:1), p. 12.

Lipowski, Z. 1975. "Sensory and Information Inputs Overload: Behavioral Effects," *Comprehensive Psychiatry* (16:3), pp. 199-221.

Ma, Q., and Pearson, J. M. 2005. "Iso 17799:" Best Practices" in Information Security Management?," *Communications of the Association for Information Systems* (15:31), pp. 577-591.

Meier, R. L. 1963. "Communications Overload: Proposals from the Study of a University Library," *Administrative Science Quarterly* (7:4), pp. 521-544.

Moore, J. E. 2000. "One Road to Turnover: An Examination of Work Exhaustion in Technology Professionals," *Mis Quarterly* (24:1), pp. 141-168.

Mukherjee, I. 2008. "The Complexity Paradigm: Implications for Information Systems and Their Strategic Planning," *Journal of Computer Science* (4:5), pp. 382-392.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. 2009. "What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules&Quest; an Empirical Study," *European Journal of Information Systems* (18), pp. 126-139.

O'Driscoll, M. P., and Beehr, T. A. 1994. "Supervisor Behaviors, Role Stressors and Uncertainty as Predictors of Personal Outcomes for Subordinates," *Journal of organizational Behavior* (15:2), pp. 141-155.

Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' Behavior Towards Is Security Policy Compliance," *40th Hawaii International Conference on System Sciences*, p. 156b.

Panko, R. 2010. *Corporate Computer and Network Security*, (2 ed.). Upper Saddle River, NJ: Prentice Hall.

Parker, D. 1981. *Computer Security Management*. Reston, VA: Reston Publishing Company.

Ratnasingham, P. 1998. "Trust in Web-Based Electronic Commerce Security," *Information Management and Computer Security* (6), pp. 162-166.

Schick, A. G., and Gordon, L. A. 1990. "Information Overload: A Temporal Approach* 1," *Accounting, Organizations and Society* (15:3), pp. 199-220.

Schwartz, S. H., and Zanna, M. P. 1992. "Universals in the Content and Structure of Values: Theoretical Advances and Empirical Tests in 20 Countries," in *Advances in Experimental Social Psychology,* M.P. Zanna (ed.). San Diego, CA: Academic Press, pp. 1-65.

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

Sneha, S., and Varshney, U. 2009. "Enabling Ubiquitous Patient Monitoring: Model, Decision Protocols, Opportunities and Challenges," *Decision Support Systems* (46:3), pp. 606-619.

Spears, J. L., and Barki, H. 2010. "User Participation in Information Systems Security Risk Management," *MIS Quarterly* (34:3), pp. 503-522.

Straub , D. W. 1990. "Effective Is Security," *Information Systems Research* (1:3), pp. 255-276.

Straub, D. W., and Nance, W. D. 1990. "Discovering and Disciplining Computer Abuse in Organizations: A Field Study," *MIS Quarterly* (14:1), pp. 45-60.

Tsoumas, B., and Gritzalis, D. 2006. "Towards an Ontology-Based Security Management," *20th International Conference on Advanced Information Networking and Applications*, pp. 985-992.

Tu, Q., Wang, K., and Shu, Q. 2005. "Computer-Related Technostress in China," *Communications of the ACM* (48:4), pp. 77-81.

Venkatraman, N. 1994. "It-Enabled Business Transformation: From Automation to Business Scope Redefinition," *Sloan Management Review* (35), pp. 73-73.

Vollmann, T. E. 1993. "Cutting the Gordian Knot of Misguided Performance Measurement," *Industrial Management & Data Systems* (91:1), pp. 24-26.

Warkentin, M., and Willison, R. 2009. "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," *European Journal of Information Systems* (18:2), pp. 101-105.

Werlinger, R., Hawkey, K., and Beznosov, K. 2009. "An Integrated View of Human, Organizational, and Technological Challenges of It Security Management," *Information Management & Computer Security* (17:1), pp. 4-19.

Whitman, M. E., and Mattod, H. J. 2004. *Management of Information Security*. Boston, MA USA: Thomson.

Workman, M., Bommer , W. H., and Straub, D. W. 2008. "Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test," *Computers in Human Behavior* (24:6), pp. 2799-2816.

Workman, M., and Gathegi, J. 2007. "Punishment and Ethics Deterrents: A Study of Insider Security Contravention," *Journal of the American Society for Information Science and Technology* (58:2), pp. 212-222.

Wurman, R. S. 1990. *Information Anxiety: What to Do When Information Doesn't Tell You What You Need to Know*. New York, NY: Bantam.

Zafar, H., and Clark, J. G. 2009. "Current State of Information Security Research in Is," *Communications of the Association for Information Systems* (24:Article 34), pp. 557-596.