Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2009 Proceedings

Americas Conference on Information Systems (AMCIS)

2009

Developing an Information Systems Security Success Model for eGovernment Context

Kimberley Dunkerley
Nova Southeastern University, kd177@nova.edu

Gurvirender Tejay
Nova Southeastern University, tejay@nova.edu

Developing an Information Systems Security Success Model for E-Government Context

Kimberley Dunkerley
Nova Southeastern University
kd177@nova.edu

Gurvirender Tejay
Nova Southeastern University
tejay@nova.edu

ABSTRACT

Information security has received a great deal of attention from a number of researchers (Dhillon and Backhouse, 2001). However, there has been little research aimed at understanding the dimensions—within the organizational context—of information security success. The current study considers a large body of information security literature and organizes the research based on their findings. This taxonomy is used to develop a model for information security success. The utility of the proposed model within e-Government is considered. Finally the implications for research and industry are discussed.

Keywords

Information systems security success, E-government, security benefits

INTRODUCTION

As information systems have become increasingly integrated into the functioning of organizations of every type, the need to protect the information produced by those organizations and stored within their information systems has expanded. Response to this need has been the development of a myriad of information security programs. However, as organizations strive for "successful" information security and as threats to that security become increasingly sophisticated and invasive, no clear understanding of information security success and its underlying constructs has emerged. In fact, the current research is based on the assumption that measurement of the success of an information security program may be impossible without a clear understanding and operationalization of those constructs.

As the value of information systems and significance of the information they protect rise, so too does the importance of their protection. Unfortunately, many firms have found the real value of effective security only after experiencing the negative repercussions associated with a security breach (Cavusoglu et al., 2004). However, even as organizations have begun to recognize the importance of security, assessing its real value has proved to be challenging. To identify key to IS success and their effectiveness within an organization will ultimately allow organizations to better utilize their resources (Zviran and Haga, 1999). In fact, successful information security involves a "well-informed sense of assurance that information risks and controls are in balance" (Anderson, 2003, p. 310). In spite of the wealth of research, information security and success have been treated generally as separate entities. In fact, limited research has been aimed at developing and understanding the core dimensions of information security success. The argument of the current study is that, without understanding the true meaning of information security success within an organizational context, attempting to measure it is, in effect, aiming at a goal that is moving, or perhaps nonexistent – certainly poorly understood.

This research is designed to provide a starting point for developing a better understanding of the elements that comprise information security success within an organization. To that end, we will review literature present within the information security field and identify the dimensions constituting information security success, operationalize those dimensions, and create a model for ensuring IS success that can be tested empirically. Finally, we will evaluate information systems security success model in the context of e-Government and discuss appropriate implications.

REVIEW OF INFORMATION SECURITY LITERATURE

The review of information security literature was conducted as outlined by Webster & Watson (2002). We examined selected papers (no time period constraint) from information systems field using keywords capturing the definition of IS security. We also examined reference list of the reviewed articles to expand our list of articles and journals.

Data integrity has its roots grounded in the classic CIA (Confidentiality, Integrity, and Availability) triad of information protection. In the past most secure system development activities and organizational security policies have been exclusively based on these core principles (Dhillon and Torkzadeh, 2006). The increasing importance of protecting information has resulted in a large amount of research primarily focused on the technical aspects (i.e., encryption, data and software controls, and hardware controls) of protecting information in a computer-based system (e.g., Anderson, 1972; Sandhu et al., 1996; Schneier, 1996). In reaction, researchers, such as Anderson (2001) and Dhillon and Torkzadeh (2006), have become critical of a possible "over-reliance" on CIA issues at the cost of a more robust, organizationally-focused mindset. In fact, Anderson argues that information insecurity is as much due to "perverse incentives" as it is to weaknesses in the technical infrastructure.

Information systems assurance has evolved in a manner similar to general information systems development methods (Baskerville, 1993), with a reliance on checklists and other "one-size-fits-all" measures aimed at finding the specific minimum control set that will best protect information systems in general. In addition, most research has heavily focused on keeping intruders out via use of intrusion detection and other technically-focused methodologies (Denning, 1987; Daniels and Spafford, 1999; Vigna and Kemmerer, 1999; Axelsson, 2000; Frincke, 2000). However, there is evidence that to best ensure the security of information systems within an organization, the need for a secure information system must be balanced with its functionality within the organizational environment (Baskerville, 1993). Therefore, weaving security into the information system while providing flexibility for organizational growth can be a challenge, particularly in emergent organizations. In these situations, generic checklists are often found to be inadequate (Baskerville and Siponen, 2002). These various factors have led researchers to become increasingly interested in reaching beyond the "one-size-fits-all" mindset (D'Arcy and Hovav, 2007).

A number of researchers, such as Anderson (2001) and Gordon and Loeb (2002, 2006), are studying the organizational value of information systems and how their protection supports and furthers the business as a whole. Developing an information security budget is itself a balancing act—maximizing value by investing the optimal amount in protecting assets is an important consideration (Gordon and Loeb, 2002). Although balancing risk and reward is an integral part of maximizing value, firms should not necessarily focus their investments on information sets with the highest vulnerability. Rather, a firm may be better off concentrating its efforts on information sets with midrange vulnerabilities (Gordon and Loeb, 2002).

A further factor to be considered is the exposure of information assets to other organizations; Tanaka et al. (2005) found that the level of information security investment within an organization is directly linked to their shared assets and the corresponding vulnerability level. In addition, Arora et al. (2006) argue that the disclosure of vulnerabilities and the nature and timing of that disclosure affects the risk of organizational exploitation. These findings are important, not only to the department managing the information system, but to the functioning of the organization as a whole.

Campbell et al. (2003) found a highly significant negative market reaction to information security breaches involving unauthorized access to confidential data. In fact, certain market segments like Internet-specific firms and software vendors are subjected to even greater risk of losses due to a security breaches (Hovav and D'Arcy, 2003; Telang and Wattal, 2007). Understanding the risk to the organization and attempting to manage it at an acceptable level creates value, thereby facilitating the business. However, when attempting to understand how an information security program creates value to the organization, one cannot focus solely on economic aspects – socio-organizational considerations, such as effects on organizational culture, also offer value to the organization (Backhouse et al., 2006; Dhillon and Torkzadeh, 2006; Dinev et al., 2008; Drevin et al., 2007).

Since the effectiveness of controls that are put into place to protect information assets are constrained by behaviors of human agents who access, use, administer, and maintain them (Vroom and von Solms, 2004; Stanton et al., 2005), it is clear that understanding information security success must consider the intervening power of users and their behavior. A growing body of research has focused on the user and their interaction with information security. One line of research deals with counterproductive computer usage and malicious extreme, insider threats (Dhillon, 2001; Siponen, 2001; Trompeters and Eloff, 2001; Schultz, 2002; Stanton et al., 2005).

A second subset of user behavioral research focuses on the awareness of users towards the systems—both the information system and its protective technologies—with which they interact, Dinev and Hu (2007) have found that awareness of technology is central to the formation of user attitudes surrounding and behavior toward usage of protective technologies. For instance, awareness towards the negative consequences of spyware has been found to motivate users to develop positive attitudes towards protective technologies and their intention to use them (Dinev et al., 2008). Furthermore, research suggests that intention is affected by a number of external moderators, including codes of ethics (Harrington, 1996) and cultural factors (Dinev et al, 2008). These three findings suggests that user intention—ranging from the malicious to the beneficial—

might allow them to either subvert controls protecting the information system or expand their knowledge of protective measures (Stanton et al., 2005).

Based on the extant literature, it can be logically concluded that understanding the underlying dimensions composing information security success is important. The model predicting success with information systems security in organizations is provided in the next section.

DEVELOPING AN IS SECURITY SUCCESS MODEL

This research study builds upon the body of work by Shannon and Weaver (1949), Mason (1978), and DeLone and McLean (1992, 2003), to develop a model that would predict success with information security in an organization. DeLone and McLean (1992) extended the studies by Shannon and Weaver (1949), and Mason (1978) to develop a model that would predict IS success. Shannon and Weaver (1949) identified three constructs involved in effective communications. First, the *technical* level of communications involves the accuracy and efficiency of the communication system that produces information. Second, the *semantic* level relates to the success of the information in conveying the intended meaning from sender to receiver. Finally, the *effectiveness* level is the result the information actually has on the user's behavior. Mason (1978) adapted the work by Shannon and Weaver in order to relate it specifically to information systems. For DeLone and McLean (1992), the interrelated dimensions of IS success were obtained by analyzing three levels of information presented by Shannon and Weaver, and Mason's influence level, to yield six dimensions of information systems that would yield success.

Based on extant security literature, it is clear that there are several dimensions that interact to form the information security experience within an organization. Table 1 presents the analysis of security dimensions in terms of the three levels of communication as advocated by Shanon and Weaver (1949).

Communication Levels	IS Security Dimensions	Supporting Literature
Technical	Information Integrity, IS Assurance, Business Enablement	Anderson (1972), Denning (1987), Sandhu et al. (1996), Daniels & Spafford (1999).
Semantic	User Intention, User Expertise	Dhillon (2001), Siponen (2001), Trompeters & Eloff (2001), Schultz (2002), Vroom & von Solms (2004), Stanton et al. (2005), Dinev et al. (2008).
Effectiveness	IS Security Benefits	Anderson (2001), Gordon and Loeb (2002), Campbell et al. (2003), Hovav and D'Arcy (2003), Tanaka et al. (2005), Arora et al. (2006).

Table 1. IS Security Dimensions for Different Communication Levels

The dimensions operating at the technical level are focused on information systems within an organization. First, information security should attempt to ensure "information integrity," which is defined as an attempt to ensure that data is precisely the same during transmission, receipt, and storage. Next, the information security controls should provide "information systems assurance," which is considered as a guarantee of integrity and availability of the information system. Finally, the information security program should ensure "business enablement" and not hinder achieving organizational objectives effectively. This dimension captures the value provided by information security controls to the business.

The semantic dimensions of security are focused on users and their interaction with the information system with specific attention to intention and knowledge. "User intention" refers to intentions of the users – ranging from beneficial to malicious – toward the information system and its protective measures, as defined by Stanton (2005). Finally, we will consider the user's knowledge, or "user expertise" that could allow them to either subvert the controls protecting the information system or raise their knowledge of protective measures (Stanton, 2005).

In the end, these variables interact with each other for a net benefit. In our case, the "security benefits" are the cumulative effect of the relationship between information systems experience (technical level) and user experience (semantic level) within their organizational context. This benefit can have a positive or a negative outcome, depending on the inputs provided. Ultimately, when considering the overall success of an information security program, controls implemented by the organization are only part of the solution. The user behavior towards an information system and its protective mechanisms presents an intervening force that will affect – for good or bad – the final net security benefits. The model predicting success with IS security in organizations is presented in figure 1.

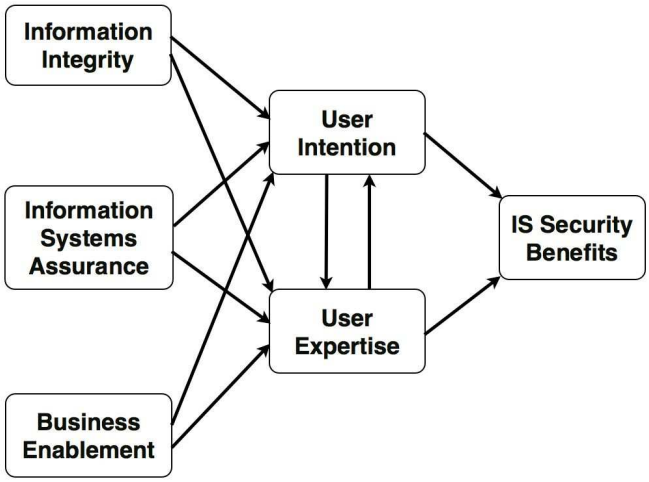

Figure 1. IS Security Success Model

CASE OF E-GOVERNMENT

As stated previously, information systems are more important than ever within organizations. In conjunction with this, the Internet is having a dramatic impact on business operations (DeLone and McLean, 2003). This impact is creating change within all organizations, but perhaps most so within the government sector. The advent of e-Government, the intersection between traditional government and the new age of delivering services to citizens via the Internet, has necessitated a shift in the paradigm of protecting our national interests while serving the citizen in a most effective manner. These national interests include everything from banking to electrical systems that power our homes and businesses.

In the past, government organizations have relied heavily on checklists and minimum-security requirements as their baseline to information systems security success (Baskerville, 1993). Furthermore, government entities are required to adhere to a variety of regulatory requirements such as the Federal Information Security Management Act (FISMA) and the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP). These constraints add a layer of complexity not present within the standard industry environment. Mandates coupled with the changes presented by advent of the Internet age shape the important, but often begrudged, role information security plays within government sector. While industry has plunged forward with sophisticated techniques such as biometric access controls and intrusion prevention devices, government organizations are often merely struggling to define roles and responsibilities. "[An] industrial age organization makes a cyber-dependent government vulnerable and inefficient" (CSIS Commission on Cybersecurity, 2009, p. 51). Understanding this effort, the proposed information security model could help government organizations focus their efforts on the dimensions of information security that are truly necessary to protect information assets.

System security

Government organizations, arguably more than any other, value integrity of the data transacted within their information systems, particularly at the highest levels of secrecy. In fact, the government so values the secrecy of its data that United States law strictly controls the export of cryptographic products to foreign governments. "Information integrity" measures the desired characteristics of the information itself (Flowerday and von Solms, 2005). Attributes of this dimension are integrity, confidentiality, and authenticity. Integrity means "its outputs fully and fairly reflect its inputs, and its processes are complete,

timely, authorized, and accurate" (Boritz, 2004). Associated with this attribute is confidentiality, or the aversion of data disclosure to unauthorized individuals. Authenticity ensures that data, transactions, and communications are genuine for conduct of government operations.

"Information systems assurance" measures the desired security characteristics of an information system. Information integrity relies on information systems assurance as "information has its integrity only when the accuracy, completeness, timeliness, validity, and processing methods are safeguarded" (Flowerday and von Solms, 2005, pp.606). One of the critical attributes of this dimension is the availability of IS, or the assurance that it is available when needed. Another critical attribute for a government organization is the response time. It is a measure of assurance that the IS will respond in a timely and efficient manner. Finally, reliability of IS is a crucial need for government organizations. Daily missions, from delivering mail to delivering a bomb, depend on the information systems being available and dependable. In addition to military operations, IS assurance ensures better service delivery to citizens, improved services for businesses, and empowerment through information.

Enabling the operations of a government organization is very simple: without information security, the job cannot be done with confidence. In fact, Hale and Brusil (2007) argues that "enterprises that deal with the general public are missing out on business if they do not link security to business strategy …" (pp.526). CSIS (2009) describes the failure to secure cyberspace as "[diluting] our investment in innovation while subsidizing the research and development of foreign competitors" (p. 11). In current climate, mission assurance assumes importance for government sector. It is a measure of the ability to utilize IS to promote the mission of an organization. A security control should support normal functioning of operations. This emphasizes the role of usability, as an attribute balancing the security needs with the needs of user to ensure that protections do not hinder critical functions. Another attribute relevant for our context is the risk reduction or mitigation. This attribute is the ability of protective technologies to reduce or remove outstanding risks to a government entity.

User security

In the context of critical government functions, it becomes extremely vital to understand the user's intent towards IS and its protective technologies, on a spectrum from positive to negative (Stanton et al, 2005). A factor of this is the user's actions, or their actual actions towards those same entities. This is one of the dimensions of user's behavior, with the other dimension being "user expertise." The latter dimension describes user's knowledge of the organizational environment, both technical and non-technical (Stanton et al, 2005). Technical knowledge refers to the user's savvy with technical assets. On the other hand, non-technical knowledge involves user's awareness about security policy and various controls to protect information assets and organizational mission.

Security effectiveness

"Security benefits" within e-Government context remains the most important measure of success with an information security program. As argued in Wood (1991), "the benefits of information security cannot be characterized definitively with traditional cost-benefit analysis" (pp.399). Some attributes include cost savings, time-savings, regulatory compliance, and enhanced security culture. Cost savings can be measured as a reduction in extraneous budgetary spending on security concerns. Time-savings can be measured as a reduction in man-hours spent dealing with security incidents, both internal and external. Regulatory compliance is a measure of the adherence to applicable regulatory requirements. Finally, enhancing the organizational security culture can be described as the creation or promotion of a culture among users who are constantly and consistently aware of threats to the IS and their role in its protection. Government organizations will benefit from all of the above, with the added advantage of direct conservation of taxpayer money while securing critical information assets from unknown threats. CSIS (2009) recommends government to treat cybersecurity as "… a strategic issue on par with weapons of mass destruction and global jihad …" (p. 15).

Government organizations that choose to apply the proposed security model potentially stand to improve their overall security stance by creating a positive cycle. However, a possible limitation of this treatment is the need to complete supplementary, potentially unnecessary steps in order to meet regulatory requirements. In addition, the organization will require strong leadership that understands how to define information security success within that organization's context, necessitating individuals who understand both information security and needs of the organization. In contrast, a government entity that chooses to continue with the status quo could very well follow the guidance to the letter while generating excessive paperwork and neglecting more important dimensions of information security. On paper, this organization could look prepared to face cyber threats based on a checklist or minimum requirements, but without considering the government context and user behavior, could in reality be woefully ill equipped.

DISCUSSING EMERGENT ISSUES

There are many challenges facing government organizations as they attempt to transform into e-Government organizations. Some of these include balancing the need to be as secure as possible with the growing requirement to provide e-enabled services to both citizens and other government and non-government organizations; introducing change into an environment that is unprepared or unwilling to change; and securing critical assets with a mandated set of tools that may be less sophisticated than the attacks occurring against the IS. While the information security success model proposed within this paper cannot eliminate these issues, it could help address these challenges by better focusing organizational efforts on the true path to information security: defining what success means to the organization, operationalizing the constructs that lead to success for that organization, and understanding the intervening power of users interacting with the information system. By doing these things, an organization can better assure the privacy and safety of the information assets that will power government transformation for years to come.

After reviewing the various approaches that information security researchers have taken, several observations have been made. First, an emphasis has been placed on many "means to the end." A good number of research studies have focused on measures to address one or more of the core dimensions, such as technical security, risk management, or security culture. While this is undoubtedly valuable research, it is a mistake to believe that securing the technical assets of an organization while neglecting other dimensions will facilitate a secure organization. Information security must be viewed as a continual, interactive process rather than a single "fix."

Another issue is with the placement of emphasis on individual dimensions and not their interactions. Again, many studies have focused on individual dimensions. However, a limited number of studies have focused on the interaction between the dimensions. This is important, as the model shows a causal process, particularly with the intervening power of the user and their behavior. More studies need to be directed at the whole life cycle of information security and how different dimensions interact and affect each other.

This information is powerful from both a research and a practitioner standpoint for a variety of reasons. First, organizations can use the findings to better focus their attention towards dimensions that actually constitute success. Better focusing the attention and assets of the organization will save time and money, thus creating additional value and further enabling the business. From a research perspective, the conceptualized model will provide ample opportunity for empirical study in a variety of organizational contexts, such as within emergent organizations. Broadly, emergent organizations (along with their noncomitant information systems) are constantly changing (Baskerville and Siponen, 2002). These types of organizational structures can benefit from a more straightforward approach to information security. Finally, this research will help bridge the gap between extensive work that has been done in both information systems success and information security disciplines.

CONCLUSION

In conclusion, significant literature has been reviewed to better understand different elements of information security success that have been proposed by researchers. From this literature, six interrelated elements have emerged as core dimensions of information security success. From these findings a parsimonious model for IS security success has been proposed. In addition, utility of the model within the context of e-Government has been discussed. The model introduced in this paper should be useful for future research efforts in several ways. The security elements of the model have never been studied as interrelated dimensions of an encompassing model. Research on these relationships would provide a better understanding of the interaction between security structure within an organization and an individual utilizing the information system and its protective technologies. In addition, applying the model within various organizational contexts would provide a better understanding of how information security varies within these contexts.

REFERENCES

1. Anderson, J. (1972). Computer security technology planning study. Deputy for Command and Management Systems, United States Air Force, Fort Washington, PA.
2. Anderson, J.M. (2003). Why we need a new definition of information security. *Computers & Security*, 22, 4, 308.
3. Anderson, R. (2001). Why Information Security is Hard – An Economic Perspective. *Proceedings of 17th Annual Computer Security Applications Conference*, Dec 10-14, New Orleans, Louisiana, 10-14.

4. Arora, A., Nandkumar, A., and Telang, R. (2006). Does information security attack frequency increase with vulnerability disclosure? An empirical analysis. *Information Systems Frontiers*, 8, 5, 350.
5. Axelsson, S. (2000). The base-rate fallacy and the difficulty of intrusion detection. *ACM Transactions on Information Systems Security*, 3, 3, 186–205.
6. Backhouse, J., Hsu, C.W., and Silva, L. (2006). Circuits of power in creating de jure standards: Shaping an international information systems security standard. *MIS Quarterly*, 30, 413-438.
7. Baskerville, R. (1993). Information systems security design methods: Implications for information systems development. *ACM Computing Surveys*, 25, 4, 375-413.
8. Baskerville, R. and Siponen, S. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management,* 15, 5/6, 336-346.
9. Boritz, J.E. (2004). Managing enterprise information integrity: Security, control, and audit issues. Rolling Meadows, IL: IT Governance Institute.
10. CSIS Commission on Cybersecurity (2009). *Securing cyberspace for the 44th presidency*. Retrieved April 20, 2009 from the CSIS website: http://www.csis.org.
11. Campbell, K., Gordon, L.A., Loeb, M.P., and Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security*, 11, 3, 431-448.
12. Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, 9, 1, 69-104.
13. Daniels, T. E. and Spafford, E. H. (1999). Identification of host audit data to detect attacks on low-level IP. *Journal of Computing Security*, 7, 1, 3–35.
14. D'Arcy, J. and Hovav, A. (2007). Towards a best fit between organizational security countermeasures and information systems misuse behaviors. *Journal of Information Systems Security*, 3, 2, 3-30.
15. DeLone, W. H. and McLean, E. R. (1992). Information system success: The quest for the dependent variable. *Information Systems Research*, 3, 1, 60-95.
16. DeLone, W. H. and McLean, E. R. (2003). The DeLone and McLean model of information systems success: A ten-year update. *Journal of Management Information Systems*, 19, 4, 9-30.
17. Denning, D. (1987). An intrusion-detection model. *IEEE Transactions on Software Engineering*. 13, 2, 222–226.
18. Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers & Security*, 20, 165-172.
19. Dhillon, G. and Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal*, 11, 2, 127-153.
20. Dhillon, G. and Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, 16, 293-314.
21. Dinev, T., Goo, J., Hu, Q., and Nam, K. (2008). User behaviour towards protective information technologies: The role of national cultural differences. *Information Systems Journal*, 8, 7, 1-22.
22. Dinev, T. and Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, 8, 7, 386-408.
23. Drevin, L., Kruger, H.A., and Stegn, T. (2007). Value-focused assessment of ICT security awareness in an academic environment. *Computers & Security*, 26, 36-43.
24. Flowerday, S. and Von Solms, R. (2005). Real-time information integrity = system integrity + data integrity + continuous assurances. *Computers & Security*, 24, 8, 604-613.
25. Frincke, D. (2000). Balancing cooperation and risk in intrusion detection. *ACM Transactions on Information Systems Security*, 3, 1, 1–29.
26. Gordon, L.A. and Loeb, M.P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, 5, 4, 438-457.
27. Gordon, L.A. and Loeb, M.P. (2006). Budgeting process for information security expenditures. *Communications of the ACM*, 49, 1, 121-125.

28. Hale, J. and Brusil, P. (2007). Secur(e/ity) management: A continuing uphill climb. *Journal of Network and Systems Management*, 15, 525-533.
29. Harrington, S.J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly*, 20, 3, 257-278.
30. Hovav, A. and D'Arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review*, 6, 2, 97-121.
31. Mason, R.O. (1978). Measuring information output: A communication systems approach. *Information & Management,* 1, 5, 219–234.
32. Pendegraft, N. and Rounds, M. (2007). A simulation model of information systems security. *International Journal of Information Security and Privacy*, 1, 4, 62-69, 71-74.
33. Sandhu, R. S., Coyne, E. J., Feinstein, H. L., and Youman, C. E. (1996). Role-based access control models. *IEEE Computing*, 29, 2, 38–47.
34. Schneier, B. (1996). Applied Cryptography (2nd ed.), Wiley, New York.
35. Schultz, E.E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security*, 21, 6, 526-531.
36. Shannon, C.E. and Weaver, W. (1949). The Mathematical Theory of Communication. University of Illinois Press, Urbana, IL.
37. Siponen, M.T. (2001). On the role of human morality in information systems security. *Information Resources Management Journal*, 14, 4, 15-23.
38. Stanton, J.M., Stam, K.R., Mastrangelo, P., and Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, 24, 124-133.
39. Tanaka, H., Matsuura, K., and Sudoh, O. (2005). Vulnerability and information security investment: An empirical analysis of e-local government in Japan. *Journal of Accounting and Public Policy*, 24, 37-59.
40. Telang, R. and Wattal, S. (2007). An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Transactions on Software Engineering*, 33, 8, 544.
41. Trompeters, C.M. and Eloff J.H.P. (2001). A framework for the implementation of socio-ethical controls in information security. *Computers & Security*, 20, 384-91.
42. Vigna, G. and Kemmeerer, R. A. (1999). NetSTAT: A network-based intrusion detection system. *Journal of Computing Security*, 7, 1, 37–71.
43. Vroom, C. and Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, 23, 3, 191-198.
44. Wood, C.C. (1991). Using information security to achieve competitive advantage. *Computers & Security*, 10, 5, 399-405.
45. Webster, J. and Watson, R.T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, 26, 2, xiii-xxiii.
46. Zviran, M. and Haga, W.J. (1999). Password security: An empirical study. *Journal of Management Information Systems*, 15, 4, 161-184.