

12-31-2007

An Information Systems Security Framework

Joseph Schuessler
University of North Texas

Recommended Citation

Schuessler, Joseph, "An Information Systems Security Framework" (2007). *AMCIS 2007 Proceedings*. Paper 304.
<http://aisel.aisnet.org/amcis2007/304>

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2007 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

AN INFORMATION SYSTEMS SECURITY FRAMEWORK

Joseph H. Schuessler
University of North Texas
schuessj@unt.edu

Abstract

Ever evolving Information Systems Security (ISS) risk requires that we as researchers constantly review our body of work to identify potential gaps. If we can successfully understand the nature of ISS incidents, we can begin to eliminate or mitigate the risks so that damage can be limited or occur in a more controlled fashion. This paper is an attempt to identify relevant research gaps as they relate to ISS by developing an ISS framework and identifying gaps within the existing literature.

Keywords: Information Systems Security, Security Frameworks, Security Taxonomies

Introduction

Information System's Security (ISS) has changed in scope and focus over the years. With mainframes, security issues were primarily limited to design errors, natural disasters, and threats from people with physical access to terminals. The introduction of Personal Computers (PCs), Networks, and Network Operating Systems (NOSs) drastically changed the potential frequency and type of security exposures. As networks became more standardized, their use began to spread, as did malicious code and hacking activities. The goal up to this point was to protect organizational data and keep outsiders out. Vendors responded to network and NOS security issues by hardening their hardware and software. However, the commercialization of the Internet brought about a complete refocus in how ISS interacted with users; The Internet created an ability to cost effectively link customers and businesses but at the same time, increased the requirements for protecting company and customer data. This set the stage for the security threats that practitioners face today. The goal of this paper is to examine different perspectives of computer security by synthesizing research done in the area of ISS, examine the relationships between key concepts in order to identify research gaps, and discuss how such research can help practitioners accomplish their goals of improving security within their organizations.

IS Security Research Streams

To identify different ISS research streams, 119 academic journal articles related to computer security were reviewed with articles beginning in 1991 and ending in early 2005. Keywords were tallied to identify the frequency of each keyword in different areas of research and then subjectively grouped to identify major constructs of interest. These constructs were then organized into a framework to identify where current research is occurring in the computer security field and what areas deserve further investigation. Figure 1 graphically shows each construct and its relationship to other constructs. Additionally, each keyword within a construct is shown along with its frequency as a keyword for each of the articles reviewed. Each construct is discussed below in the sequence presented in Figure 1, from top to bottom, left to right.

External Environment

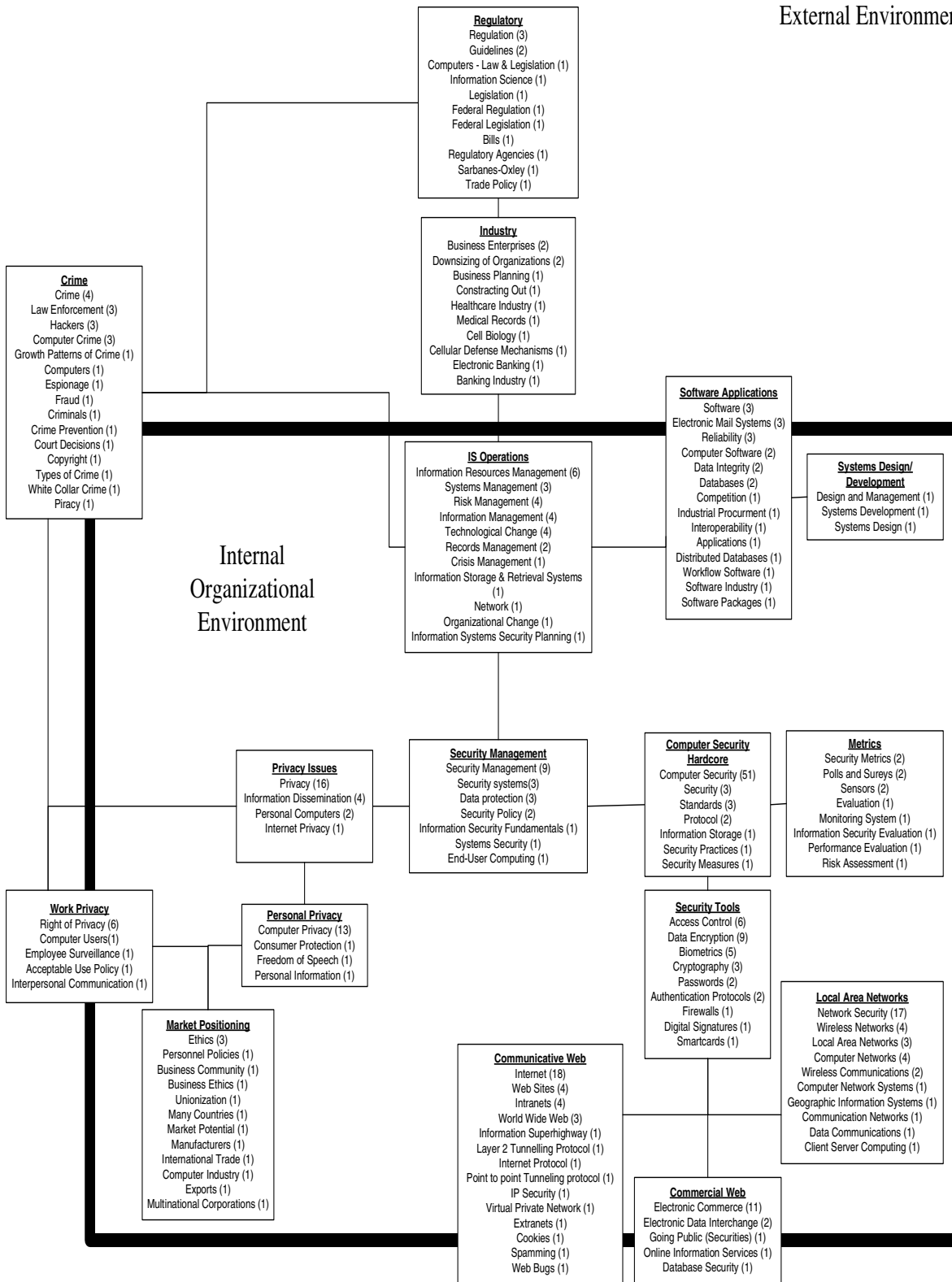


Figure 1: Computer security research framework

Regulatory

Regulatory issues are becoming increasingly important in the post 9/11 world and in the aftermath of various corporate financial scandals. New legislation has forced constraints on practitioners to implement new procedures, develop new systems, and log activities in order to comply with legal mandates. For example, the Sarbanes-Oxley Act requires that CEOs and CFOs attest to the accuracy and completeness of a company's financial records. This has placed additional pressure on IS departments to both secure and share accurate information, a seemingly paradoxical relationship. These pressures force companies to establish IT controls that dictate how data are protected, how data may be modified, and how the controls lead to compliance with Sarbanes-Oxley.

Law enforcement is also a part of the regulatory perspective. Orlikowski (1997) looked at the balance between privacy, law enforcement, and legislative bodies. This balance could serve as an opportunity for practitioners and academicians to work with privacy advocates, law enforcement officials, and those in the legislative bodies to pass and enforce regulations that reflect the concerns of all involved.

The regulatory perspective of IS security is multidimensional in that it addresses a broad range of topics yet can be very detailed oriented on a single topic. Regulations span from how security is implemented across borders (Levin 1999) to how domestic implementations affect privacy (Zorkadis 2004).

Industry

While some commonality exists in the security concerns across industries such as those imposed by Sarbanes-Oxley, other security threats are unique to individual industries. For example, while public companies across all industries must accurately and completely disclose their financial records, the healthcare industry must selectively allow access to patient's medical records depending on the needs of a particular user in order to provide medical services to patients while protecting the patient's privacy (Fiesta 1996). Violations of one's privacy regarding medical afflictions can be embarrassing leading to potential lawsuits. The banking industry is faced with a more tangible and direct threat when it comes to protecting the privacy of customers. "Cyber-criminals" (Patterson 2003) seek to obtain account information with which to extract funds from a bank's customers. Both are examples of privacy violations but the consequences can be substantially different.

Crime

When a security incident occurs, a corresponding remedy is often contingent upon being able to quantify damages and prove culpability. Perhaps no other electronic crime personifies the difficulties with this more than the piracy of copyrighted material (Delaney et al. 2003). Peer-to-peer networks have made it incredibly difficult to determine who is responsible. Additionally, establishing a monetary value for damages gives an appearance of arbitrariness regardless of the figure determined. Part of the issue in peer-to-peer networks is the anonymity involved in the sharing process. Armstrong et al. (2003) found that anonymity fuels the commission of computer related crime. Even if the identity of a perpetrator is determined, it must still be proven that a crime was committed. Computer forensics attempts to address this issue by using techniques acceptable in a court of law which consists of investigating storage devices and data processing equipment for illegal, unauthorized, or unusual activities.

Research in this area focuses on not only being able to quickly identify deviant behavior but also on how and why such behavior may occur in the first place. Because research in this area horizontally spans across several disciplines including psychology, IS, and criminology, as well as vertically spans from theoretical foundations to operational aspects, an opportunity exists for practitioners and academia alike to develop tools and techniques to address these issues.

IS Operations

IS Operations focuses on the daily management of IS including areas such as records management, risk management, and organizational change. An organization must manage its documents in such a way so that they are preserved and secured yet are still accessible to those who need them (Hart et al. 2003). An organization must also manage risk. For example, when retiring old computers, companies must destroy sensitive information on those computers or risk potential legal actions, depending on the nature of the data (Lundsford 2004). Research in this area has both a broad,

strategic focus, as well as a narrow focus reflective of the role that IS operations plays within an organization. IS Operations provides infrastructure for the entire organization. They must also cater to the unique demands of different functional areas of an organization such as manufacturing, accounting, marketing, and so on. Accordingly, research in the area of IS operations must help practitioners to develop methods and practices for efficiently providing organizational infrastructure while at the same time being able to provide customized services for different functional areas.

Software Applications

The software applications construct refers to security issues surrounding acquisition and/or development of software. Software can be developed in-house, outsourced, or purchased from a vendor, which is why the construct spans the internal organizational and external environments. In addition, some applications can operate on a variety of devices, which might be used inside organizational walls or used externally. Both impact security and usability in their own unique ways. For example, the use of handheld and wireless devices creates a software interoperability issue with respect to existing systems but additionally, there are inherent security concerns because of the portability of such devices and the ease with which they can be lost or stolen (Pietro et al. 2003). Another way in which software applications can impact security is how a particular application is designed to interoperate with the Internet. This conundrum provides academia an opportunity to develop solutions for practitioners to better manage patches, upgrades, and new rollouts.

Systems Design/Development

Systems Design/Management looks at the security issues involved in developing systems. This includes decisions such as whether to centralize systems or decentralize them, which computing platforms to use, and deciding on the infrastructure with which to facilitate communications. For example, in designing Wired Equivalent Protocol (WEP), the rush to market caused the designers to by-pass common security practices that ultimately led to a less than ideal solution for wireless network encryption (Cam-Winget 2003). An approach to avoid this type of problem is to develop and use a framework such as that proposed by El-Geyer and Fritz (2004). Their proposed framework provides a method with which to make decisions about tradeoffs in security when designing a system. The area of incorporating security in the initial phases of systems development lacks significant research. Greater emphasis on security at design time could decrease the band-aid effect of applying security measures after systems have already been implemented which sometimes offer less than ideal solutions such as the proposed WEP replacement for existing hardware (Cam-Winget 2003).

Security Management

Effective management of security issues includes the economics of security implementations, data protection policies, and change management. While organizational changes, such as the addition of a remote site, impact an organization's general security posture, Security Management lies at a more technical level. Decisions regarding the establishment of data characteristics as well as changes to those characteristics later, such as increasing a field's size, must be weighed against their impact on all related systems. Poor implementations can lead to problems such as buffer over-run errors. The onset of end-user computing has exacerbated this issue by making it more difficult to coordinate these types of changes. Delligatta (1992) examined the need to create standards for development of end user solutions. Cavusoglu et al. (2004) identified four key economic elements that relate to the security of information systems. One key conclusion was that the expense of implementing security measures, regardless of how that expense was measured, is shrinking in relation to the costs associated with security breaches.

A major part of managing security is ensuring security managers are aware of the full range of controls available to them (Straub 1998). Managers more cognizant of system controls were able to more effectively manage system risks. Cerullo and Cerullo (2004) examined how businesses view the use of continuity plans and perceived security threats. Security management is about creating an organizational security posture that observes security practices from top to bottom of an organization. Security management has been studied more than the role of security in system design/development, but it should be noted that research in this area is also relatively limited and warrants further investigation.

Privacy Issues

Privacy issues can be divided into personal privacy and workplace privacy, each of which engender different expectations in the amount of privacy expected. Privacy issues concern the right to know what information is being kept, how it is will be used, whether or not it will be sold, how secure the information is, and whether or not incorrect information can be corrected. An early investigation of techniques to protect private information by Agranoff (1991), recommended the use of internal privacy codes by companies. Essentially encrypting sensitive customer data so that customer interests will be protected as well as protecting the company from potential lawsuits resulting from lost customer information. An alternative view of privacy concerns, put forth by the Open Information Society (OIS), advocates free access to information (Ahituv 2001). OIS supporters argue that the money and effort spent on trying to secure systems could be better spent on other money generating endeavors.

The concept of Information Organizations (IOs) (Duncan et al. 1996) has also become popular. These organizations act as third party repositories for vast amounts of personal data. Duncan (1996) advocates the development of privacy control mechanisms such as privacy mediators to “negotiate” what information is kept as well as a mechanism for correcting inaccurate information. Privacy concerns will continue to grow as technology continues to morph into new facets of everyday life.

Personal Privacy

Personal computing privacy refers to the privacy one may expect through normal use of their computer in their personal environment. The use of cookies is but one means of gathering such information (Beghel 2002). However, personal computer privacy is a two-edged sword. Going hand-in-hand with privacy are “cyberliberties” which revolve around a person’s responsibility to conduct themselves on the Internet as they would in the real world regarding legal issues (Strossen 2000). This concerns not only individuals, but organizations as well. Companies use privacy statements to develop trust with customers and in doing so, create a contract between themselves and their customers (Larson et al. 2003). While privacy issues in the workplace have similar concerns for people, they are different enough to be viewed independently.

Workplace Privacy

Workplace privacy issues differ from personal privacy in that there is a specific, identifiable organization that has direct power over the individuals being monitored. Issues such as employee surveillance have become a hot topic due to the ability to easily monitor various employee actions electronically (Boncella 2001). An approach to help stave off legal issues has been the use of Acceptable Use Policies (AUP) (Boncella 2001). Such policies allow organizations to enter into contracts with their employees by explicitly stating what company equipment may or may not be used for. Additionally, AUPs should explicitly state how conformance would be measured along with potential penalties when violations occur. Lunsford et al. (2004) discusses information management and the issue of protecting organizational data when retiring old computers. There is a responsibility when storing information, regardless of whether it is simply transactional information about customers or personal information about employees.

Socio-Cultural Positioning

This construct is a subset of both workplace and personal privacy and views them from a social perspective with respect to ethics and cultural/political borders. Often a reflection of the society and culture of a people, the political climate of a country has implications both legally, as international borders are crossed, as well as ethically as different cultures are engaged. While the legal aspect is addressed by the Regulations construct, the impetus for such regulations are addressed by this construct. Particularly with modern technologies, often times the pace of change makes it difficult for cultural

acceptance of new technologies. Often times, countries try to address these cultural concerns by passing laws intended to provide direction for technological advances. For example many U.S. companies face export restrictions when trying to sell encryption products overseas (Levin 1999) resulting from a desire on the part of the people of the U.S. and its government to maintain a competitive business and military edge over other countries. Additionally, multinational companies face difficulties in integrating their systems because of disparate privacy law requirements in different countries or economic regions such as the European Union (Tran et al. 2002). Disparity between how Europeans and Americans view privacy has led to differences in the privacy laws between the respective economic markets. Many of these issues, while not new, have been brought into the limelight with the rapid proliferation of communication technologies and the opening of economic/political borders.

Metrics

Successful implementations of security can only be determined to be successful if they can be measured and compared to other implementations. While there have been many proposed methods for measuring security effectiveness, no single method has distinguished itself as the best method (Sharman et al. 2004). Preparing a security infrastructure must not only measure effectiveness but also system risks (Whitman 2003). Risk assessment involves evaluating the current system state, potential internal/external risks, and the potential impact on the organization should security fail. While security metrics have been researched in the past, there has been little consensus as to what constitutes good measurement of security effectiveness or risk, and as a result, the metrics construct warrants further investigation to develop appropriate and effective measurement tools and techniques.

Computer Security Hardcore

Computer Security Hardcore represents the detailed technical aspects of computer security and is practitioner oriented. It answers questions such as “what do we protect and how do we protect it?” Some of the research that has been performed in this domain includes how to operationalize the use of biometrics (Schneier 1999) and the use of Smart Cards (Shelfer et al. 2002). While each of these can be used as a tool with which to implement security, an understanding of how these types of technology work strengthens our ability to identify and appropriately apply them in practice. Other research looks at the economic issues of implementing security (Cavusoglu 2004). Cavusoglu identified the need to be able to identify the cost of security breaches, the way to manage risk, a cost effective way to configure technology, and the concept of deploying multiple technologies for greater value as ways to manage an organization’s security better. A detailed understanding of an organization’s hardware, software, policies, and procedures must be known to determine which metrics are capable of being gathered. Maier (2000) examines the use of extranets and other security measures typically used to maintain secure systems such as gateways and firewalls. Hardcore security issues are the most heavily researched area of this proposed framework.

Security Tools

As tools and techniques are used to attempt to measure the effectiveness of an IS, they are also used in implementing the information system itself. Tools such as virus scanners, firewalls, passwords are but a few of the tools in a security designer’s arsenal and each has been researched extensively. Research in this area includes an investigation of how to construct and utilize strong passwords (Wood 1996) and the impact that digital signatures have legally on Internet transactions (Pattison 1997). While this area is a glamorous segment of security research, its popularity reflects the volume of research already done in this area.

Communicative Web

Research in this area focuses on the use and risks of Internet technologies as organizational resources. This area has led to the increased importance of research in security related issues because of the interconnectedness of systems. Internet connectivity research has included comparison of competing protocol standards such as Layer 2 Tunneling Protocol, IP Sec, and Point-to-Point Tunneling Protocol and the evaluation of Virtual Private Networks (VPN) (Sirisukha et al. 2004). Along with Internet connectivity comes the use of cookies, Web Bugs (Boncella 2004), and SPAM (Bellovin 2004). The latter are issues that all Internet users face, whether casual web surfers or business users.

Commercial Web

The Commercial Web construct focuses on the web's ability to facilitate commercial transactions and the relationship between customers and e-tailers. E-tailers face issues trying to protect e-commerce privacy when conducting transactions with portable wireless devices (Ghosh et al. 2001). Businesses must make decisions such as sacrificing some security in order to have systems that are compatible with more potential customers or conversely, at the risk of limiting their potential customer base, implement rigorous security measures and procedures. Other issues revolve around trust between users and companies that promise, explicitly or implicitly, that the users' information will be safeguarded (Udo 2001). Trust was also addressed by Liu (2005) in which notice, access, choice, and security were identified to attempt to explain what is necessary for users to feel they can trust that they can safely conduct e-commerce transactions. While the commercial web has been the focus of a significant amount of research, the continued growth of e-commerce and our ability to deliver new services as technologies improve will continue to make research in this area of value.

Local Area Networks

Research around Local Area Network (LAN) security is extensive. As organizations have connected their systems to the Internet, research in this area has intensified and shifted to accommodate new threats. Wen (1998) examined the shift from client/server computing in traditional networks to the use of intranets/extranets. This shift has streamlined the user's perspective in that often all they see is a browser front-end, but such dependence on web technologies has shifted the threat from internal to the organization to outside the organization (Pfleeger et al. 2002). Because of the dynamic nature of network hardware and software, there will always be room for more research in this area as new technologies come online. For example, wireless networking can facilitate the easy movement of end users and reduce the load on a company's telecommunications infrastructure. However, security issues concerning wireless networking devices abound (Berghel 2004). Integrating these new technologies while maintaining the existing infrastructure demands that new techniques and tools be developed in order to make use of these new technologies while maintaining appropriate levels of security.

Gap Analysis

In developing this framework, several areas in security were identified that warrant further research: Workplace Privacy, Socio-Cultural Positioning, Security Management, Systems Design/Development, Metrics, and the Commercial Web. Research revolving around Workplace Privacy needs to address ownership of time and space. For example, should workers essentially be treated as property while in the confines of their work environment, subject to constant observation, or should there be designated times throughout a workday when employees are not monitored? The legal impact of legislation will either expand or restrict an employers' ability to conduct surveillance on their workers. The goals of future research in this area should be to establish common rules of engagement with respect to what and when employees can be monitored. This would help practitioners understand what data to capture as well as how to communicate these policies with employees.

Investigation in the area of Socio-Cultural Positioning should address how culture affects workplace privacy expectancy. Different cultures must certainly have different expectations about the degree of privacy they can expect in the workplace. This type of information would be particularly useful to global companies that operate across different political and economic borders.

Security Management research needs to develop additional theory as well as additional practitioner frameworks. Using Eisenhardt's (1991) approach to case studies future research could compare several companies that have successfully managed their security infrastructure over time. This should help researchers to develop an understanding of the elements that must be present for successful security management as well as a "cookbook" for practitioners who want to follow practices of those who have been successful.

Systems Design/Development provides an opportunity for research. While the field of systems design has developed numerous approaches for analyzing and designing systems such as the Systems Development Life Cycle (SDLC) and Rapid Application Development (RAD), security concerns have not been well integrated into these processes. This provides an opportunity for researchers to develop new development techniques that incorporate security techniques during systems design which is more appropriate for today's distributed environments.

Metrics are an area that have been investigated to some degree. However, there has been little agreement on a comprehensive approach to measure the effectiveness of information system security across industries, company size, and other characteristics. This provides an opportunity to develop instruments that can help practitioners evaluate the effectiveness of their security infrastructure and planning processes.

The final area identified that lacks comprehensive investigation is the Commercial Web. While some research has been done in this domain, the annual growth of e-commerce and its relative size compared to the rest of the economy suggests that a tremendous amount of growth remains. However, to meet this growing demand, the infrastructure used to support e-commerce will have to change. Business processes, telecommunication infrastructure such as Internet 2, and changing consumer demands provide research opportunities.

Conclusions

ISS is a diverse and dynamic subject, deserving not only of research in developing new methods and techniques but also in confirmatory analyses that validate existing techniques and methods in a changing environment. Research in the area of ISS serves not only as an opportunity for academicians to further the field, but also for practitioners to better practice their profession. Research in the area of ISS is vast and has shifted over the years. However, due to this dynamic nature of new technologies, the field will continue to require an extensive amount of research in the future.

- Agranoff, Michael H. "Controlling the Threat to Personal Privacy." In *Information Systems Management*, 48: Auerbach Publications Inc., 1991.
- Ahituv, Niv. "The Open Information Society." *Association for Computing Machinery. Communications of the ACM* 44, no. 6 (2001): 48.
- Armstrong, H L, and P J Forde. "Internet Anonymity Practices in Computer Crime." *Information Management & Computer Security* 11, no. 5 (2003): 209.
- Bellovin, Steven M. "Spamming, Phishing, Authentication, and Privacy." *Association for Computing Machinery. Communications of the ACM* 47, no. 12 (2004): 144.
- Berghel, Hal. "Hijacking the Web." *Association for Computing Machinery. Communications of the ACM* 45, no. 4 (2002): 23.
- Boncella, Robert J. "Internet Privacy - at Home and at Work." *Communications of the Association for Information Systems* 7, no. 14 (2001): 1-28.
- Cam-Winget, Nancy, Russ Housley, David Wagner, and Jesse Walker. "Security Flaws in 802.11 Data Link Protocols." *Association for Computing Machinery. Communications of the ACM* 46, no. 5 (2003): 35.
- Cavusoglu, Hasan, Huseyin Cavusoglu, and Srinivasan Raghunathan. "Economics of It Security Management: Four Improvements to Current Security Practices." *Communications of the Association for Information Systems* 14 (2004): 65-75.
- Cerullo, Virginia, and Michael J. Cerullo. "Business Continuity Planning: A Comprehensive Approach." In *Information Systems Management*, 70-78: Auerbach Publications Inc., 2004.
- Delaney, Edwin M, Claire E Goldstein, Jennifer Gutterman, and Scott N Wagner. "House Considers Bill to Enhance Criminal Enforcement of Internet Copyright Piracy Measures." *Intellectual Property & Technology Law Journal* 15, no. 9 (2003): 16.
- Delligatta, Ann. "Empowering the User Community." In *Information Systems Management*, 63: Auerbach Publications Inc., 1992.
- Duncan, George T, and Sandra Kaufman. "Who Should Manage Information and Privacy Conflicts?: Institutional Design for Third-Party Mechanisms." *International Journal of Conflict Management* 7, no. 1 (1996): 21.
- Eisenhardt, Kathleen M. "Building Theories from Case Study Research." *Academy of Management Review*. 14, no. 4 (1989): 532-550.
- El-Gayer, Omar F., and Brian D. Fritz. "A Framework for Decision Support in Information Systems Security." Paper presented at the Proceedings of the Tenth Americas Conference on Information Systems, New York, New York, August 2004 2004.
- Fiesta, Janine. "Legal Issues in the Information Age--Part 1." *Nursing Management* 27, no. 8 (1996): 15.
- Ghosh, Anup K, and Tara M Swaminatha. "Software Security and Privacy Risks in Mobile E-Commerce." *Association for Computing Machinery. Communications of the ACM* 44, no. 2 (2001): 51.
- Hart, Peter E, and Ziming Liu. "Trust in the Preservation of Digital Information." *Association for Computing Machinery. Communications of the ACM* 46, no. 6 (2003): 93.
- Joshi, James B D, Walid G Aref, Arif Ghafoor, and Eugene H Spafford. "Security Models for Web-Based Applications." *Association for Computing Machinery. Communications of the ACM* 44, no. 2 (2001): 38.
- Larson, Linda Lee, Robert K Larson, and Janet Greenlee. "Privacy Protection on the Internet." *Strategic Finance* 84, no. 12 (2003): 49.
- Levin, Staci I. "Who Are We Protecting? A Critical Evaluation of United States Encryption Technology Export Controls." *Law and Policy in International Business* 30, no. 3 (1999): 529.
- Liu, Chang, Jack T Marchewka, June Lu, and Chun-Sheng Yu. "Beyond Concern - a Privacy-Trust-Behavioral Intention Model of Electronic Commerce." *Information & Management* 42, no. 2 (2005): 289-304.
- Lunsford, Dale L, Walter A Robbins, and Pascal A Bizarro. "Protecting Information Privacy When Retiring Old Computers." *The CPA Journal* 74, no. 7 (2004): 60.
- Maier, Phillip Q. "Ensuring Extranet Security and Performance." In *Information Systems Management*, 33: Auerbach Publications Inc., 2000.

- Orlikowski, Steve. "Government Initiatives in Information Technology Security." *Information Management & Computer Security* 5, no. 3 (1997): 111.
- Patterson, Aubrey B. "Fighting Hackers, Fraud and Wrong Perceptions." *American Bankers Association. ABA Banking Journal* 95, no. 4 (2003): 14.
- Pattison, Michael. "Legal Implications of Doing Business on the Internet." *Information Management & Computer Security* 5, no. 1 (1997): 29.
- Pfleeger, C. P., and S. L. Pfleeger. *Security in Computing*. Upper Saddle River, NJ: Prentice-Hall, 2002.
- Pietro, Roberto Di, and Luigi V Mancini. "Security and Privacy Issues of Handheld and Wearable Wireless Devices." *Association for Computing Machinery. Communications of the ACM* 46, no. 9 (2003): 75.
- Schneier, Bruce. "The Uses and Abuses of Biometrics." *Association for Computing Machinery. Communications of the ACM* 42, no. 8 (1999): 136.
- Sharman, Raj, and Raghav H. Rao. "Metrics for Information Security - a Literature Review." Paper presented at the Proceedings of the Tenth Americas Conference on Information Systems, New York, New York, August 2004 2004.
- Shelfer, Katherine M, and J Drew Procaccino. "Smart Card Evolution." *Association for Computing Machinery. Communications of the ACM* 45, no. 7 (2002): 83.
- Sirisukha, Sid, and Mikhail Kotykhov. "Information Systems Security: A Model for Vpn Performance Evaluation." Paper presented at the Proceedings of the Tenth Americas Conference on Information Systems, New York, New York, August 2004 2004.
- Straub, Detmar W, and Richard J Welke. "Coping with Systems Risk: Security Planning Models for Management Decision Making." *MIS Quarterly* 22, no. 4 (1998): 441-69.
- Strossen, Nadine. "Cybercrimes V. Cyberliberties." *International Review of Law, Computers & Technology* 14, no. 1 (2000): 11.
- Tran, Elizabeth, and MaryAnne Atkinson. "Security of Personal Data across National Borders." *Information Management & Computer Security* 10, no. 5 (2002): 237.
- Udo, Godwin J. "Privacy and Security Concerns as Major Barriers for E-Commerce: A Survey Study." *Information Management & Computer Security* 9, no. 4 (2001): 165.
- Wen, H. Joseph. "From Client/Server to Intranet." *Information Management & Computer Security* 6, no. 1 (1998): 15.
- Whitman, Michael E. "Enemy at the Gate: Threats to Information Security." *Association for Computing Machinery. Communications of the ACM* 46, no. 8 (2003): 91-94.
- Wood, Charles Cresson. "Constructing Difficult-to-Guess Passwords." *Information Management & Computer Security* 4, no. 1 (1996): 43.
- Zorkadis, V, and P Donos. "On Biometrics-Based Authentication and Identification from a Privacy-Protection Perspective: Deriving Privacy-Enhancing Requirements." *Information Management & Computer Security* 12, no. 1 (2004): 125.