Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2000 Proceedings

Americas Conference on Information Systems (AMCIS)

2000

Security Knowledge Management Systems: A Solid Shield Against Computer Abuse

Younghwa Lee
University of Colorado at Boulder, yhlee@unlserve.unl.edu

Sid Davis
University of Nebraska - Lincoln, sdavi1@unlnotes.unl.edu

Zoonky Lee
University of Nebraska at Lincoln, zlee@unlnotes.unl.edu

Security Knowledge Management Systems:
A Solid Shield Against Computer Abuse

Younghwa Lee, College of Business and Administration, University of Colorado at Boulder, yhlee@unlserve.unl.edu,
Sid Davis, College of Information, Science, and Technology, University of Nebraska at Omaha, sdavi1@unlnotes.unl.edu,
Zoonky Lee, Department of Management, University of Nebraska-Lincoln, zlee@unlnotes.unl.edu

Abstract

Even though organizations have developed and implemented a number of security countermeasures, computer abuse continues to be a problem, and information systems in organizations today remain in jeopardy. Researchers recommend security awareness programs as a means to increase security interest and knowledge, but this has not provided satisfactory results.

In this paper, we introduce the concept of *security knowledge management systems* (SKMS). These systems overcome time and place limitations, consider different levels of security knowledge among users, promote voluntary participation, and provide a positive framework for learning security knowledge. SKMS gives users a way to overcome the limitations of traditional awareness programs through the ability to acquire the most current, diversified security knowledge, to search the knowledge more quickly and accurately, to store it more securely, to share it conveniently, and to maintain it cost effectively. As a result, SKMS allows users to acquire better security knowledge, while giving organizations a cost-effective way of reducing computer abuse.

Background

Despite the fact that organizations have developed and implemented a number of security countermeasures, computer abuse has continued to be a problem (Meyer, 1995; Straub and Welke, 1998; Timothy and John, 1999). Moreover, the frequency of computer abuse and its amount of loss are expected to grow as computer abuse occurs at the hands of highly sophisticated and educated criminals armed with the latest information technology (Baskerville, 1993; Straub and Nance, 1990). Computer abuse can be defined as "any intentional act associated in any way with computers where a victim suffered, or could have suffered, a loss, and a perpetrator made, or could have made again"(Parker, 1981:333). It includes all crimes against hardware, programs, data, and computer services (Kling, 1980; Hoffer and Straub, 1989; Lee, et al., 1986; Straub, 1990). There are many cases that reveal how critically organizations are victimized by computer abuse (ABA, 1984; Straub, 1986; Hoffer and Straub, 1989; BloomBecker, 1989; Goodhue and Straub, 1991; Harrington, 1995; Strain, 1991; Weiss, 1991; Meyer, 1995; Fink, 1995; Mulhall, 1997; Stephen, 1998; CSI, 1999; Ernst & Young, 2000). For example, Mulhall (1997) states that 41% of computer systems in the U.S. were subjected to various computer abuses in 1996. The Computer Security Institute (1999) reports that 51% of organizations responded on a survey experienced financial loss by computer abuse that approximate $124 million in 1999, and the figure is expected to rise continuously. Amid this growing problem, previous studies have investigated the issue of why computer abuse has not been reduced despite companies' increasing investment in computer security, have attempted to find ways to reduce computer abuse.

They usually agree on the three main causes: inappropriate enforcement and operation of a security policy, ill-suited security standards in system development/purchasing and operations, and a relatively low level of interest and awareness of organizational members in computer abuse. As a solution to these problems, the studies have recommended that organizations implement security awareness programs (Crockett, 1998; Fites and Kartz, 1993; Smith, 1993; Stephen, 1998; Ulsch, 2000; Wood, 1994; Zajac, 1988). For example, Ulsch (2000) recommends security awareness programs as the most effective tool to overcome the lack of concern about computer security within top management. Smith (1993) emphasized the importance of a security awareness program, mentioning that "raising awareness and educating a wide audience in the basics of computer security will achieve, pound for pound, a far more profound and longer lasting improvement in computer security than any purely technical solution could ever hope to achieve"(p. 237).

Although previous studies have suggested practical ways to conduct security awareness programs, such as training courses accompanied by publications, posters, newsletters, bulletins, trinkets with a security message, and security regulation statements (Fites and Kartz, 1993; Meyer, 1995; Smith, 1993; Wood, 1991; Zajac, 1988), these approaches have some limitations in providing users with useful and timely security awareness and knowledge. First, such programs focus only on managers, excluding operational-level employees who also account for a large portion of computer abuse (e.g, Hoffer, 1989; Rose and

Tom, 1989; Wood, 1991). Second, these programs have been, at best, sporadic efforts, not leading to regular, routine security related activities in organizations. As a result, the useful, just-in-time security knowledge has not been made available to organizational members. Third, such programs do not consider different levels of employee security knowledge, limiting the effectiveness of education. Finally, the compulsory nature of traditional security awareness programs has made participatory security knowledge sharing difficult (Rose and Tom, 1989; Straub and Welke, 1998; Parker, 1998).

The main purpose of this paper is to introduce a conceptual model of a new type of system called *security knowledge management systems* (SKMS), aimed at addressing the problems mentioned above. An SKMS is a type of hybrid system that combines the concept of an escalation path of *human security experts* with that of *knowledge management systems*. Both concepts have proven their value in real world settings by their ability to promote greater user satisfaction, increased interest, and efficient knowledge management (El Sawy and Bowles, 1997; Buckman, 1998). By introducing these benefits, SKMS can support organizational members through more efficient acquisition, searching, and sharing of security information.

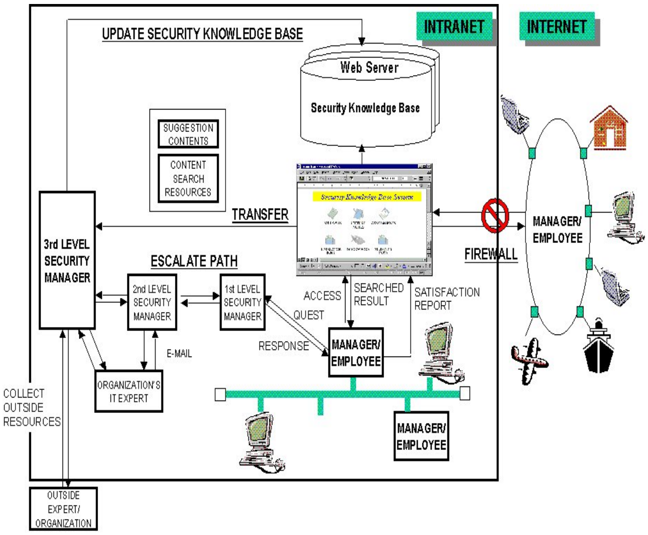
Research Model

The SKMS model, shown in Figure 1, consists of four main system modules: *knowledge acquisition*, *knowledge search*, *knowledge storage* and *knowledge sharing*. We divide the system into four modules, according to the general classification of knowledge management systems (e.g., Choo, 1998; Nonaka and Tachuchi, 1995). An organization can operate SKMS under its normal network environment, including its intranet, or using the Internet. SKMS is supported by several information technologies, such as a web-based graphical user interface (GUI) and a trusted security knowledge base (web server), as shown in Figure 1. As mentioned above, it is also characterized by a leveled escalation path of security managers. This concept is adopted from consumer support systems (e.g., help desk) that are widely used in the service industry (e.g., El Sawy and Bowles, 1997). An important aspect of SKMS involves its ability to motivate organizational members to learn more about security and to apply effective security principles. We discuss the vital issue of motivation in a subsequent section of the paper. In this section, we first discuss each of the SKMS modules in the following sections. Secondly, we discuss the issue of implementing SKMS in the organization by integrating it with traditional security awareness programs.

Knowledge Acquisition Module

Security knowledge is generated from three sources: organizational members (i.e., users, IT experts, and security managers), outside sources (e.g., security consulting co., secure system vendors, or research organizations), and content-based search engines. One of the main differences between SKMS and conventional security awareness programs is that by using SKMS organizational members can play more active roles in generating security knowledge.

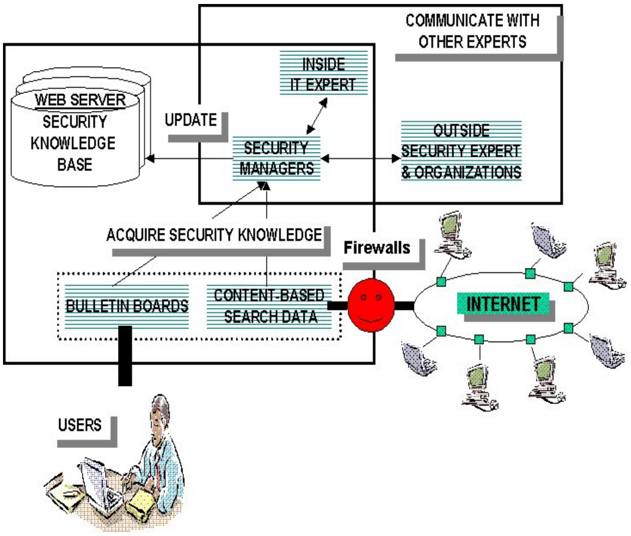
Figure 1. The Framework of SKMS



While not all knowledge is generated by users, the concept of user participation in security knowledge creation is important since many researchers report that the IT department does not often have enough information about computer abuse in the real operational world (e.g., Wood, 1991; Parker, 1998). Since users are the people who experience the risk of day-to-day computer abuse, they often know how to apply appropriate countermeasures. Organizational IT experts can also generate security knowledge. There are numerous IT experts within the organization who have special knowledge for solving specific security problems. To draw out employees' and IT experts' tacit knowledge, SKMS requires them to develop their own homepages. These homepages should contain information about their own expert knowledge along with references to experts whom they know. This concept is currently being utilized in BP AMOCO (Newing, 2000). Additionally, security managers play a key role in creating security knowledge. They develop this knowledge through their own expert knowledge, from outside security experts (e.g., security counselor, security product vendors, and specialized security organizations such as CERT), and from a variety of documents from security journals and hacker's Internet sites.

Security knowledge can also be acquired using bulletin board systems (BBS) from the SKMS homepage, as well as content-based search engines and collaborative filtering methods. Users can suggest security solutions using the BBS, while a content-based search engine automatically collects multimedia files related to computer security. A search engine can help in gathering Internet-based security information that includes audio, video, and text (Chang et al., 1999). Using an intelligent filtering algorithm, users can gather only the information they want. Collaborative filtering methods can reduce the burden on security managers for reading unnecessary information gathered by content-based search engines (Avery and Zeckhauser, 1997). Security managers update the security knowledge base after collecting all of the information and then verifying its appropriateness through communication with other security experts. Figure 2 shows the SKMS knowledge acquisition mechanism.

Figure 2. Knowledge Acquisition Module

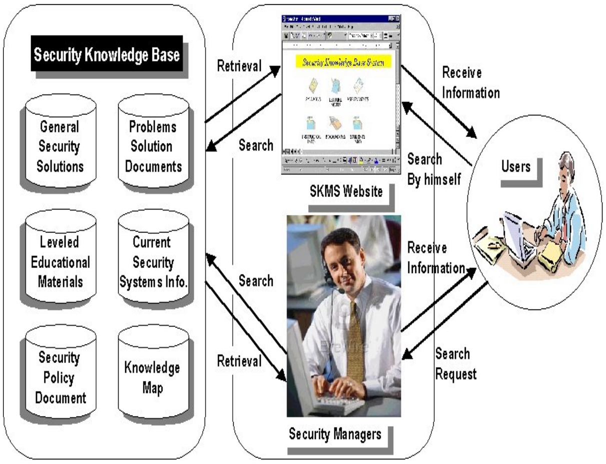


Knowledge Search Module

The second module in SKMS is the *knowledge search module*. Organizational members can search security knowledge using two search methods: a human security expert-based search and a knowledge search engine. The expert-based search method has its origins in help desk systems that utilize "escalating paths" of helpers (see Fig. 1). In such systems, helpers are usually divided into two or three levels, according to their work and scope of responsibility (i.e., the higher the level, the greater the responsibility and security knowledge). This approach has proven to have many benefits to users, such as qualified service, quick response, and increased satisfaction. It also gives each security expert the chance to concentrate on his/her own sub-domain of expertise and to increase specific knowledge on the problems that are frequently requested.

As mentioned above, users can also access a security knowledge base using context-based search engines. Users' access to certain documents can be logged, and based on the statistics, the security department can find the most frequently occurring problems in the organization. User feedback on the materials accessed from the knowledge base can also be an important resource to further refine its contents and the searching mechanism. The Knowledge search module is shown in Figure 3.

Figure 3. Knowledge Search and Storage Modules



Knowledge Storage Module

We store security knowledge on the web server in the form of documents that include multimedia data such as text, video, and voice. We refer to this web server as the "security knowledge base". In the security knowledge base, 6 kinds of security knowledge are stored (as shown in Figure 3). They are: security problem-solution documents, leveled security educational materials, general security solutions, knowledge map, organizational security policy, and the information about current security systems.

The organizational security policy document includes the organizational security policy, procedures, and records of previous punishment. We include this document in the knowledge base for two reasons. One is to give the user information related to the organization's security policy. The other is to show potential computer abusers that the organization is serious about monitoring and controlling computer abuse. The information about security systems within the organization includes a document describing the system's security functions, operating techniques, audit records, and know-how accumulated over time. Problem solution documents suggest the appropriate solutions to computer security matters. General security solutions include security tools such as vaccine programs, recent security accident reports, and the newest security newsletters.

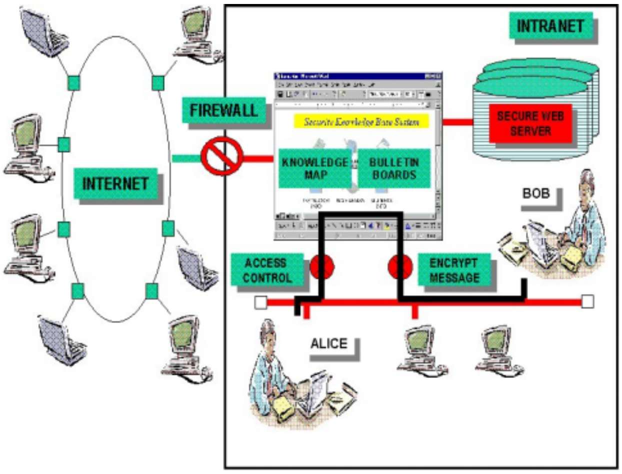
Security education materials contain the leveled security knowledge. We develop these materials based on well-known security documents published by professional security organizations (e.g., NIST, RSA, SRI International, ISO, BSI) and by well-known experts (e.g. Pfleeger, 1995, Wood, 1994). We classify these materials in three ways. One is by the level of expertise, the second is by the contents covered in each area, and the third is by user type (i.e., manager versus non-managerial employee. For example, we divide the contents of the materials into 10 sub-topics*: Risk Management*, *Physical Security*, *Cryptography*, *Application Security*, *Operating System Security*, *Database Security*, *Network Security*, *Administrative Security*, *Policy and Ethics on Security*, *and Business Continuity Planning*.

The security knowledge base contains critical resources that must be protected by highly trusted security measures. Since access by insiders or malicious outsiders can cause a major disaster, we consider measures to assure the integrity, confidentiality and availability of the security knowledge base. To assure the *integrity*, only the top-level security manager is allowed to modify the knowledge base. To assure the *confidentiality*, we suggest multilevel security systems that give users limited access rights. For example, when user tries to access SKMS outside the company, firewall first checks out his access right and then SKMS checks again his password and user name. Finally, to insure continuous availability, the knowledge base is implemented as a fault-tolerant system that endures in emergency situations.

Knowledge Sharing Module

SKMS performs its knowledge sharing functions under an IT organizational infrastructure such as a groupware platform or an intranet. Specially, SKMS has two sharing support modules: the BBS and the knowledge map. The BBS, managed by security personnel, includes newly updated security information, users' security suggestions, and recent punishment reports. Users can make suggestions using the BBS without fear that their comments will be accessed by anyone outside the organization. However, when a user thinks the suggestion is very critical to their organization's security, he/she can submit it directly to security managers for their feedback. The knowledge map functions like yellow pages. It maps specific problem domains to appropriate experts who have solutions. Users can then communicate with these experts using e-mail to get the necessary information. This map also increases the opportunity for users to access and share solutions among themselves, with a tutor or the designated security manager, through several communication media. Through this tutorship, users can learn about security knowledge more easily, and at the same time, security managers can learn more about the day-to-day operational situation in the organization. For sharing knowledge securely, the implementation of a trusted network is prerequisite. This includes secure network architecture for assuring continuous operation and includes user authentication, encryption, and access control systems. For example, when a user wants to access the security knowledge base from outside the organization, a firewall should screen the request to determine if that user has access privileges. Figure 4 shows the secure knowledge sharing mechanism in SKMS.

Figure 4. Secure Knowledge Sharing Module



Motivational Factor

SKMS includes motivational factors in its scope. Its importance was supported by several studies (e.g., Parker, 1998) positing that traditional awareness programs experienced the failure since they did not or less implement motivational factors for attracting organizational members. We include three main motivational factors into this model. First, SKMS includes several kinds of rewards such as incentives, bonus or fame, or fast promotion into its scope, which were not well supported by the traditional security awareness programs. As showing organizational members the highly positive correlation between the levels of interest and knowledge about a computer security and the organizational success, SKMS can motivate them. Secondly, SKMS provides them more user friendly GUI, fast and exact search engines, learning materials based on the levels of security or IT knowledge, and give diversified access channels to overcome space and time limitation. For example, it is possible to develop SKMS website as the useful and playfulness site that encompasses a lot of interesting information that is related to not only computer security, but also other issues, such as finance, sports, weather, and news site. It can induce the employee to visit SKMS website and help to mitigate the negative sight to computer security. The last is to encourage organizational members to a supportive and positive organizational culture on computer security. It can only be possible with continuous higher interest from top management.

Potential Implication

In this research, we suggest SKMS as an effective approach for promoting organizational security awareness. SKMS comprises both a security awareness program and security knowledge enhancement methods. It encompasses both managers and non-managerial employees, overcomes time and place limitations, and provides multi-level educational materials. It also gives users diversified, up-to-date security knowledge using a variety of acquisition mechanisms, and provides fast, exact search results using various search mechanisms. Additionally, it provides users with a convenient knowledge sharing method using a bulletin board system and knowledge maps, based on an attractive GUI that promotes ease-of-use.

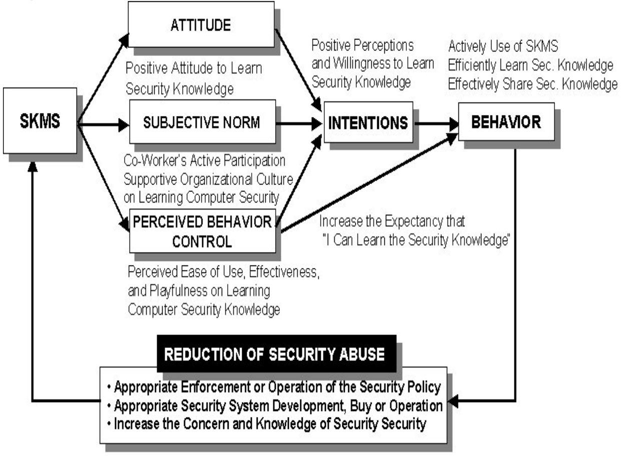
In the context of a supportive organizational culture, SKMS can help motivate users to learn security knowledge. By implementing SKMS, security managers can lessen their burden and use their slack time to focus on security enhancement in their organizations. With these features, SKMS can promote organizational members' interest in and knowledge of computer security and provide a more cost effective way to cope with computer abusers, compared to conventional security awareness programs. Table 1 shows a comparison between traditional security awareness programs and SKMS.

Table 1. Potential Comparison Between Traditional Security Awareness Programs and SKMS

SUBJECT	TRADITIONAL	SKMS
Object	Increase Awareness	Increase Awareness & Knowledge
Subject of the program	Manager	Manager &Employee
Knowledge Level	Not Consider	Consider
Time and Distance	Fixed	Flexible
User Participation	Passive	Relatively Active
Viewpoint to Security	Negative	Relatively Positive
Burden of Security Department	Heavy	Relatively light
Quality of Shared Security Knowledge	Low	High
Volumes of Knowledge	Small	Large
Timeliness	No (Slow)	Yes (Fast)
Variety of knowledge	Fixed	Variable
Knowledge Sharing	Inefficient	Efficient
Organizational Culture	Compulsive	Supportive
Security	Less Secure	More Secure

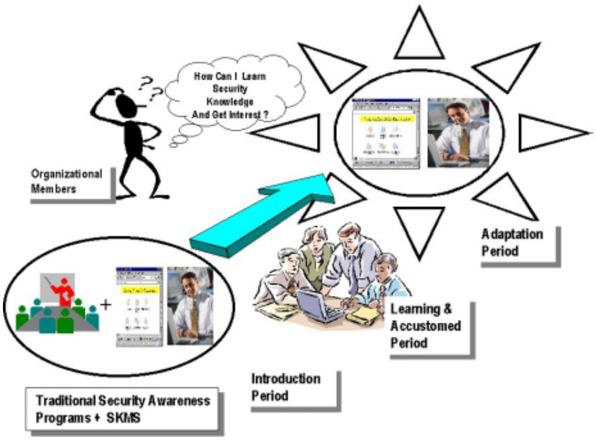
A key feature of SKMS is that it provides a number of motivational benefits to the organization, which can be explained based on the theory of planned behavior (TBP) (Ajzen, 1991). The theory suggests that the intention of behavior depends on the attitude, subjective norms, and perceived behavior control factors of the actor. Based on TBP, we can assume that if organizational members have a positive attitude, along with an environment that promotes learning and knowledge sharing, they will develop a stronger intention to access SKMS and increase their security awareness and knowledge. As is shown in Figure 5, these benefits from SKMS contribute on the reduction of computer abuse by helping organizational members enforce and operate the security policy, optimally allocating their limited budgets in developing or operating security systems, and increasing their interest in computer security.

Figure 5. The Potential Effects of SKMS


SKMS
ATTITUDE
Positive Attitude to Learn Security Knowledge
SUBJECTIVE NORM
Co-Worker's Active Participation Supportive Organizational Culture on Learning Computer Security
PERCEIVED BEHAVIOR CONTROL
Perceived Ease of Use, Effectiveness, and Playfulness on Learning Computer Security Knowledge
Positive Perceptions and Willingness to Learn Security Knowledge
INTENTIONS
Increase the Expectancy that "I Can Learn the Security Knowledge"
Actively Use of SKMS Efficiently Learn Sec. Knowledge Effectively Share Sec. Knowledge
BEHAVIOR
REDUCTION OF SECURITY ABUSE
• Appropriate Enforcement or Operation of the Security Policy
• Appropriate Security System Development, Buy or Operation
• Increase the Concern and Knowledge of Security Security

In order for the implementation of SKMS to succeed, however, it is necessary to combine this new approach with traditional security awareness programs. The organization and organizational members need time to become familiar with the new system. To do this, an optimal strategy is to operate both traditional programs and SKMS simultaneously during the system introduction period. After having time to learn about and become accustomed into SKMS, organizational members can more easily adapt to this system. Organizations can consider integration SKMS with security outsourcing which provides more elaborated and newest security knowledge by outside security consulting company as a SKMS implementation alternative. Figure 6 shows the implementation strategy for SKMS.

Figure 6. The Implementation Strategy of SKMS


How Can I Learn Security Knowledge And Get Interest ?
Organizational Members
Adaptation Period
Learning & Accustomed Period
Introduction Period
Traditional Security Awareness Programs + SKMS

Limitation

We have suggested a conceptual model of SKMS that we believe organizations can use as an effective tool in their fight against computer abuse. However, currently, a major limitation is that the model has not yet been implemented in any organization. We are in the process of developing a prototype SKMS, which we plan to test it empirically in our future studies.

Conclusion

SKMS provides organizational members with several effective and efficient components to support acquiring, storing, searching, and sharing security knowledge. By using the system, organizational members can choose security knowledge according to their interest, level of knowledge, and work domains -- whenever, whatever, and wherever they desire. This promotes a positive attitude and greater ease in learning security knowledge. All of these benefits can help to enhance the organization's ability to fight computer abuse by enforcing and operating the appropriate security policy, incorporating security measures in the development of new systems, sharing security knowledge more efficiently, and identifying effective security solutions, and then contribute to a dramatic reduction of computer abuse.

References

ABA "Report on Computer Crime," The Task Force on Computer Crime-Section on Criminal Justice, 1984.

Ajzen, I. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50), 1991, pp. 179-211.

Avery, C. and R. Zeckhauser "Recommended Systems for Evaluating Computer Messages," *Communications of ACM* (40:3), 1997, pp. 88-89.

Baskerville, R. "Information Systems Security Design Methods: Implications for Information Systems Development," *ACM Computing Surveys* (25:4), 1993, pp. 375-414.

Bloombecker, J.J. "Short-Circuiting Computer Crime, " Datamation, Oct. 1, 1989, pp. 71-72.

Buckman, R.H. "Knowledge Sharing at Buckman Labs," *Journal of Business Strategy*, Jan/Feb, 1998, pp. 11-15.

Chang, S. F., Huang, Q., Huang, T., Puri, A., and Shahararay, B. "Multimedia Search and retrieval," A. Puri and T. Chen (eds.), in Advances in Multimedia: Systems, Standards, and Networks, 1999, NY: Marcel Dekker.

Choo, C.W. *The knowing organization: how organizations use information to construct meaning, create knowledge, and make decisions*, 1998, NY: Oxford University Press.

Crockett, J. "Employee Awareness: A Good Bet for Better Security," Consulting-Specifying Engineer, 1998, pp. 20-21.

CSI *Issues and Trends: 1999 CSI/FBI Computer Crime and Security Survey*, March 1999.

El Sawy, Omar A., and Bowles, Gene, " Redesigning the Customer Support Process for the Electronic Economy: Insights From Storage Dimensions," *MIS Quarterly* (20:4), 1997, pp. 457- 483.

Ernst & Young *Executive Guide to Internet Security*, Information Systems Assurance and Advisory Services, 2000.

Fites, P., and M.P.J., Kratz *Information Systems Security-A Practitioner's Reference*, 1993, NY: Van Nostrend Reinhold.

Fink, D. "IS Security Issues for the 1990s-Implications for Management," *Journal of Systems Management*, March/April, 1995, pp. 47-49.

Goodhue, D.L., and D.W. Straub "Security Concerns of Systems Users: A Study of Perceptions of the Adequacy of Security Measures," *Information & Management* (20:1), 1991, pp.13-27.

Harrington, S.J. "Computer Crime & Abuse by IS Employees," *Journal of Systems Manag*ement, March/April, 1995, pp. 7-11.

Hoffer, J. A., and D. W. Straub "The 9 to 5 Underground: Are You Policing Computer Crimes?" *Sloan Management Review* (30:4), 1989, pp. 35-44.

Lee, J.A.N., G. Segal, and R. Steier "Positive Alternatives: A Report on the ACM Panel on Hacking," *Communications of the ACM* (29), 1986, pp. 297-299.

Loch, K.D., Carr H.H., and Warkentin, M.E. "Threats to Information Systems: Today is Reality, Yesterday is Understanding," *MIS Quarterly* (17:2), 1992, pp. 173-186.

Kling, R. "Computer Abuse and Computer Crime as Organizational Activities," *Computer/Law Journal* (2), 1980, pp.186-196.

Meyer, J. *From the Editor, Computer & Security* (14:1), 1995, pp. 2-3.

Mulhall, T. "Where Have All the Hackers Gone - Part 3: Motivation and Deterrence," *Computer & Security* (16:4), 1997, pp. 291-297.

Newing, R. BP AMOCO: Shared Learning from the US Army,http://www.usa.ft.com/ftsurveys/q56e6.htm(2000).

Nonaka, I. And H. Takeuchi *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation*, 1995, NY: Oxford University Press.

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

Parker, D.B. *Fighting Computer Crime-A New Framework for Protecting Information*, 1998, NY: John Wiley & Sons.

Pfleeger, C.P. *Security in Computing*, 1997, NJ: Prentice-Hall.

Rose, K., and R. Tom "Computer Security: Who's Minding The Store," *The Academy of Management Executive* (3:1), 1989, pg. 63-66.

Shimeall, T.J. and J. J. McDermott "Software Security in an Internet World: An Executive Summary," *IEEE Software*, July 1999, pp.58-62.

Smith, M. *Commonsense Computer Security*, 1993, Berkshire, England: McGraw-Hill.

Stephen, H. "Recent Security Surveys," *Computers & Security* (17:3), 1998, pp. 207-210.

Strain, I. *Top Bosses Pose the Main Security Threat*, Computer Weekly, Oct, 3., 1991, pp. 22.

Straub, D. W. and R. J. Welke "Coping With Systems Risk: Security Planning Models for Management Decision Making", *MIS Quarterly* (22:4), 1998, pp. 441-465.

Straub, D. W. and W. D. Nance "Discovering and Disciplining Computer Abuse in Organizations: A Field Study," *MIS Quarterly* (14:1), 1990, pp. 45-62.

Straub, D. W. *Deterring Computer Abuse: the Effectiveness of Deterrent Countermeasures in the Computer Security Environment*, Indiana University Graduate School of Business, 1986.

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

Ulsch, M. "Getting Executive Attention," *Security Management*, Jan. 2000, pp. 32-33.

Weiss J. "User-Friendly Security," *Security Management* (35:1), 1991, pp. 42-46.

Wood, C.C. *Effective Information Security Management*, Elsevier Advanced Technology, 1991, Oxford, UK.

Wood, C.C *Information Security Policies Made Easy, Baseline Software*, California, 1994.

Zajac, B. P., Jr. " Personnel: The Other Half of Data Security," *Computer & Security* (7:2), *1988*, pp. 131-132.