IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP4993

IS Security Management Framework: A Comprehensive Life Cycle Perspective

Merrill Warkentin
Mississippi State University, Department of Management & Information Systems, College of Business and Industry, P.O. Box 9581, MS State, MS 39762-9581, mwarkentin@acm.org

Mark B. Schmidt
Department of Management & Information Systems, College of Business and Industry, P.O. Box 9581, MS State, MS 39762-9581, mbs87@msstate.edu

Allen C. Johnston
Department of Management & Information Systems, College of Business and Industry, P.O. Box 9581, MS State, MS 39762-9581, acj4@msstate.edu

Matthew Boren
Department of Management & Information Systems, College of Business and Industry, P.O. Box 9581, MS State, MS 39762-9581, BorenMB@aol.com

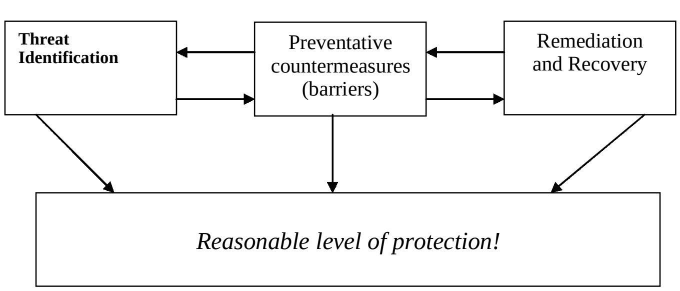
ABSTRACT

Managers of all enterprises are facing new challenges as their organizations increasingly rely on information technology (IT) for achieving goals and as their IT infrastructure is exposed to new risks. Hackers, viruses, and other threats have become more sophisticated, and newer threats have been introduced. All organizations must react to actual exposure, but should also proactively act to prevent and detect the threats. A comprehensive list of IS security threats is presented. Further, lists of the methods of detection, prevention, and remediation are presented, along with an initial taxonomy of such methods. Finally, a research agenda to explore this important domain in greater detail is presented, along with an initial set of research hypotheses.This research is supported by the Mississippi State University Center for Computer Security Research, and is funded by the National Security Agency, MDA904-02-1-0209.

INTRODUCTION

This project is premised on a model of information system security management that is comprised of three primary elements. Figure 1 depicts these components. First, the IS manager, CIO, or Chief Security Officer (CSO) must identify the threats to the security of his or her system and its resources. Some threats may pose greater risk due to a higher probability of their occurrence, greater exposure due to increased vulnerability, and/or the higher cost associated with remediation should such threats transpire. Secondly, the manager must act to prevent and deter such threats from actually penetrating his or her system boundaries and causing damage or incurring cost. In order to determine which methods of threat prevention to follow, the manager must engage in a formal risk assessment, including cost-benefit analysis of various threats and the methods to avoid or prevent them. Finally, the manager must establish and implement procedures for remediation and recovery if and when the threats occur and penetrate the organization's protective barriers. As with the earlier decisions, the methods of remediation carry various cost burdens and must be selected based on overall value proposition and ROI.

Figure 1: IS Security Management Framework



The paradigm of IT security is indeed changing. The convenience and mobility of IT can create real problems in the area of security (Yourdon, 2002). In the early days of computers, it was relatively easy to secure access to the climate controlled rooms which housed computers, but with today's miniaturized technology, criminals could very easily walk out of the building with a laptop or USB drive containing confidential company data (Yourdon, 2002). While exact figures are extremely difficult to obtain, due to a consistent lack of many organizations' willingness to disclose breaches (Hoffer and Straub, 1989; Computer Security Institute, 2003), industry estimates are that security breaches occur in 90% of organizations each year and cost $17 billion (Austin and Darby, 2003). There is a need for additional studies in the area of risk in computer security (Straub and Welke, 1998). To this end, the focus of this research is to expose decision makers to the perceived threats in today's high tech environment.

People inside an organization perpetrate most security breaches either by careless or vindictive actions (Austin and Darby, 2003). Straub and Welke (1998), propose that general deterrence theory and the model of managerial decision making form solid theoretical underpinnings for developing an effective security plan. General deterrence theory dictates that people will not participate in criminal activities if the disincentives and sanctions are strong enough (Straub and Welke, 1998). The model of managerial decision-making gives direction in developing an effective plan to address current issues.

The quest to achieve a secure computer system is indeed a difficult one. Changes in hardware (Moore's Law) increase the likelihood of disasters. i.e. new kinds of hardware must be integrated into existing systems (Lally, 2003). Software upgrades (that are poorly tested due to pressure to get the product to market) can increase the likelihood of disaster as they are integrated into existing systems (Lally, 2003). "In spite of the seriousness of systems security risk from disasters and computer abuse, many organizations are either completely unprotected of insufficiently protected" (Straub and Welke, 1998, page 443).

Table 1

O'Brien, James. Introduction to Information Systems Essentials for the Internetworked E-Business Enterprise, 10th Edition, McGraw-Hill, 2001.	Oz, Effy. Management Information Systems, 3rd edition, Course Technology Thomson Learning, 2002.	Stair, Ralph M., Reynolds, George W. Principles of Information Systems, 5th edition, Course Technology Thomson Learning, 2001.	McKeown, Patrick, Information Technology & The Networked Economy, 2nd edition, Course Technology Thomson Learning, 2003.
• Hacking • Denial of service • Scans • Sniffer • Spoofing • Trojan horse • Back doors • Malicious applets • War dialing • Logic bombs • Buffer overflow • Password crackers • Social engineering • Dumpster diving • Cyber theft • Unauthorized use at work • Software piracy • Viruses • Privacy issues	• Risks to hardware: • Natural disasters • Blackouts and brownouts • Vandalism • Risks to applications and data: • Theft of information • Data alteration • Data destruction • Defacement • Computer viruses and logic bombs • Denial of service • Spoofing	• Computer crime: • Social engineering • Dumpster diving • Hacker • Cracker • Script bunnies • Insiders • Virus • Worms • Application virus • System virus • Logic bomb • Trojan horse • Macro virus • Password sniffer • Software piracy • Internet piracy	• Hackers • Cyberterrorists • Theft of hardware, data, or information • Credit card fraud • Virus • Worm • DOS attacks • Physical security • Data security • Internet security
Turban, Rainer, Potter, Introduction to Information Technology, 2nd edition, Wiley, 2002.	Sanderson, Ethan, Karen A. Forcht. Information Management & Computer Security. Volume 4 Number 1 1996 pp. 32-37. MCB University Press.	Kendall & Kendall, Systems Analysis and Design, 5th edition, Prentice Hall, 2002.	Bishop, Matt, Computer Security Art and Science, Addison-Wesley, 2003.
• Unintentional threats • Human errors: • Design of hardware • Design of software • Environmental hazards: • Earthquakes • Hurricanes • Sever snow • Sand • Storms • Floods • Tornadoes • Power failures • Power fluctuations • Fires • Defective air-conditioning • Explosives • Radioactive fallout • Water cooling system failures • Computer systems failures • Computer crime • Data tampering • Viruses • Denial of service	• Fraud • Disruption of services or denial of services • Unauthorized disclosure of information • Unauthorized modification of sensitive information • Illegal information brokering • Password guessing • Password file collecting • Dumpster diving • Social engineering • Virus • Internal attacks	• Physical security • Logical security • Behavioral security	• Snooping • Modification or alteration • Masquerading or spoofing • Repudiation of origin • Denial of receipt • Delay • Denial of service

Several academic studies addressing current issues facing IS professionals have identified security management as a key issue. Ball and Harris (1982) surveyed the members of the Society of Management Information Systems (SMIS) and found security to be 12th most important of 18 concerns facing society members. Dickson, Leitheiser, Nechis, and Wetherbe (1984) surveyed IS professionals and used the Delphi Technique to identify and rank the top IS issues for the 1980s. Their findings put "information security and control" 14th out of 19 identified issues. Hartog and Herbert (1986) found IS security to be increasing in importance, at least in the St. Louis area. This study found "data security" to be 6th out of 21 issues. As computers became more integrated in the workplace and as connectivity increased, the area of security became more and more important. Loch, Carr, and Warkentin (1992) conducted a study that examined the perceptions of senior MIS mangers of IS security which reported the relative importance of 12 security threats.

Table 1 presents important security issues facing IS professionals assimilated from several numerous authoritative published sources.

THREAT IDENTIFICATION

A threat "is a potential violation of security" (Bishop, 2002, page 6). It has also been described as a "set of circumstances that has the potential to cause loss or harm" (Pfleeger and Pfleeger, page 6). "Information systems are exposed to various sources of danger or loss which are termed security threats" (Warkentin and Schmidt, 2003, page 2). Threats to computer security have been taken more seriously in the wake of the 9/11 terrorist attacks. As such, there is a need for much research in the area of computer security. Indeed, in November 2002, lawmakers approved the Cyber Security Research Act, which provides $900 million to colleges and universities to create computer security centers, attract graduate students, and fund research (*Information Management Journal*, 2003 (b).

Threats can be classified on the basis of their origin (inside or outside the company); further, they can be classified on their source (human or nonhuman); and finally they can be classified based on intent (deliberate or unintentional) (see Loch, Carr, and Warkentin 1992). The following taxonomy was developed using Loch, Carr, and Warkentin's 1992 work as a starting point for the research described below. Additional threats were gleaned from, O'Brien, 2001; Oz; Stair and Reynolds, 2002; McKeown, 2003; Turban, Rainer, and Potter, 2002; Sanderson and Forcht, 1996; Kendall and Kendall, 2002; and Bishop, 2003. These lists were then synthesized to produce the following taxonomy of threats.

I. Internal
- a. Human
  - i. Deliberate
    1. Unauthorized access by employees
    2. Employees intentionally entering improper data
    3. Intentional destruction of data by employees
    4. Theft of hardware, software, data, or information
  - ii. Unintentional
    1. Data entry error by employees
    2. Accidental destruction of data by employees
    3. Improper media handling
- b. Nonhuman
  - i. Deliberate
  - ii. Unintentional
    1. Weak / ineffective controls
    2. Inadequate control over media
    3. Poor control of input / output

II. External
- a. Human
  - i. Deliberate
    1. Hackers / crackers
    2. Access to system by competitors
    3. Social engineering
    4. Dumpster diving
    5. Cyber terrorism
    6. Web site vandalism
    7. Theft of hardware, software, data, or information
  - ii. Unintentional

b. Nonhuman
    i. Deliberate
        1. Viruses / worms / trojan horses
        2. Denial of service attacks
    ii. Unintentional
        1. Natural disasters (fires, earthquakes, hurricanes, tornados, floods, storms, sever snow…)
        2. Blackouts / brownouts

THREAT DETECTION

One of the ultimate goals of computer security experts is to develop computer security software that is as effective and versatile as the human immune system (Roush, 2003). Presently, at least in terms of the immediate future, there is no guarantee of impenetrability (Straub and Welke, 1998) and system security varies with the level of knowledge and experience of the administrator (Vaughn, 2003). However, there is great incentive for increase security. Unfortunately, there is no single prevention mechanism that provides an acceptable level of security. There are several products, which when used in conjunction with one another, will help to provide a holistic security solution.

Policy: Effect policies and procedures are a paramount component of a holistic security plan (Vaughn, 2003). In fact, many security experts emphasize that effective security begins with a well-written policy (Straub and Welke, 1998).

Anti-Virus Programs: Increased connectivity and the ubiquitous use of networks have forever changed the old paradigm of virus proliferation. Before the Internet was commonplace, a virus was spread very slowly through floppy disks, today it takes just hours to spread across the globe via the Internet (Sequeira, 2002).

Firewalls: A firewall will filter packets of data entering the network and only allow those that meet a specified security level to pass through the network (Frolick, 2003). There are several types of firewalls including, static packet filtering, stateful packet filtering, stateful inspection, and proxy (Sequeira, 2003).

Intrusion Detection Systems: Intrusion detection systems (IDS) are designed to monitor traffic and send alerts to network administrators (Willebeek-Lemair, 2003). The two techniques used for IDS are anomaly detection and misuse detection (Biermann, Cloete, and Venter, 2001).

Intrusion Prevention Systems: Intrusion prevention systems (IPS) not only monitor traffic but also, attempt to bock malicious traffic before it can proceed in the network (Willebeek-Lemair, 2003). As such, IPSs are the only proactive component of prevention.

Bishop (2003) describes the goals of intrusion detection to be (1) the detection of a wide variety of intrusions from both internal and external sources; (2) the timely detection of intrusions; (3) the presence of a user-friendly format for status monitoring and alert notifications; and (4) adequate accuracy in terms of activity diagnoses. Intrusion detection is characterized by acts of vulnerability assessment and attack recognition. Intrusion detection mechanisms allow for the external and internal recognition of unusual and suspicious activity. External, or perimeter oriented, detection systems employ a variety of features to provide real-time recognition of unauthorized network traffic. Typically, these devices have the ability to recognize malicious activity patterns provided by a library of known attack patterns or statistical norms and to evoke actions based on an appropriate rule set. Additionally, these devices contain logs, notification, reconfiguration, and response capabilities based on previously established management policies. Internal detection systems are generally host-based systems that monitor system audit and activity logs within the perimeter of the network. Similar to external detection systems, these forms of discovery provide alert and logging capability; however, the nature of the analysis dictates a more narrow focus than that of perimeter oriented detection systems (Cabrera, 2002).

DETERRENCE AND PREVENTION

The next step for proactive IS security managers is to determine what countermeasures can be employed to thwart potential threats. Hoffer and Straub (1989) found that security measures deter computer crime. Examples of typical security technologies used to help deter and detect computer crime include, digital ids, intrusion detection, PCMCIA, physical security, encrypted login, firewalls, reusable passwords, anti-virus software, encrypted fields, biometrics, and access control (Computer Security Institute, 2003).

Finally, using cost benefit analysis, a particular defense strategy can be employed. It should be noted that protecting information systems is never ending cycle. Once a reasonable level of security is reached, new environmental developments are likely. As such, the three steps to a reasonable level of protection are iterative and parallel in nature.

REMEDIATION AND RECOVERY

Finally, the manager must establish and implement procedures to recovery from security disasters (large and small) and remedy the damage caused by such occurrences. As with other decisions, the selection from these alternatives will involve trade-offs between various benefits and costs incurred. Such expenses can represent substantial costs to the world economy overall. Remediation starts with disaster recovery planning, which is based on the establishment of frequent accurate backups and archives of all master and transaction databases. But other methods exist, including the establishment of hot sites and cold sites for disaster recovery and the use of SWAT teams to target the initial point of attack.

RESEARCH PLAN

The present study is designed to (1) evaluate current practices of IS managers within the IS Security domain, (2) explore relationships between such practices and various organizational factors (which types of companies are doing what?), and (3) propose a general framework for managers to follow when identifying a proactive security management course of action. The research project will follow a three-stage methodology. First, the research team will evaluate the academic, industry, and popular literature to identify four exhaustive lists: (1) security threats and vulnerabilities, (2) methods of IS threat detection, (3) methods of threat/risk prevention, and (4) methods of recovery and remediation utilized once threats have been realized. In an effort to develop a more practicable and meaningful taxonomy of IS Security Practices, this long list will be presented to an expert review panel of industry and academic leaders in the field of IS security. This panel, already partially assembled, will include recognized authors, consultants, and corporate leaders in the field. The panel will be asked to identify a reasonably sized "short list" of categories for each list.

Finally, these lists will be used as building blocks of several national surveys of CIOs, CSOs (Chief Security Officers), and others, in which the research team will ask questions related to IS security practices and perceptions of threats, costs, vulnerabilities, and so forth. In addition to private IS managers, the surveys will also be targeted at members of the US Association of State CIOs (five of which have already been contacted, and who have agreed to participate), members of the US federal government IRM managers, and others.

Using the taxonomy identified above, IS professionals will be surveyed to identify their perceptions of the level of vulnerability posed by each of the threats. Further, IS professionals will be asked their opinions regarding preparedness of their organizations as well as the level of preparedness of organizations similar to their own. Specific research hypotheses have yet to be specifically articulated, but will be based only on strong theoretical foundations. Possible hypotheses might include:

***H1**: Organizations whose managers perceive the sensitivity of their data to be relatively greater will expend greater resources in the pursuit of secure systems.*
***H2**: Military IS managers will perceive greater external threats than civilian government IS managers.*
***H3**: Large enterprises will have higher IS security budgets as a percentage of overall budget (self-reported) than small and medium sized enterprises (SMEs).*
***H4**: Organizations reporting a recent major security-related event will perceive a greater threat, and will report a more detailed and expensive security plan than other organizations.*

REFERENCES

Austin, Robert D., and Darby, Christopher A.R. "The Myth of Secure Computing," *Harvard Business Review*, Vol. 81 Issue 6, June 2003, pp. 120-126.

Ball, Leslie, and **Harris**, Richard. "SMIS Members: A Membership Analysis," ***MIS Quarterly***, Vol. 6 Issue 1, March 1982, pp. 19-38.

Biermann, E., Cloete E., and L.M. Venter. "A Comparison of Intrusion Detection Systems," *Computers & Security*, Vol. 20 Issue 8, 2001, pp. 676-683.

Bishop, M., 2002. *Computer Security: Art and Science* (1e), Addison-Wesley Pub Co.

Cabrera, J.B.D., and Mehra, R.K. "Control and Estimation Methods in Information Assurance – A Tutorial on Intrusion Detection Systems," *Proceedings of the 41st IEEE Conference on Decision and Control*, 2002, pp. 1402-1407.

Computer Security Institute. *2003 CSI/FBI Computer Crime and Security Survey*. http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf. Accessed 7-26-03.

Dickson, Gary W., Leitheiser, Robert L., Wetherbe, James C., and Nechis M. "Key Information Systems Issues for the 1980's," ***MIS Quarterly***, Vol. 8 Issue 3, September 1984, pp. 135-148.

Frolick, Mark N. "A New Webmasters's Guide to Firewalls and Security," *Information Systems Management*, Vol. 20 Issue 1, 2003, pp. 29-35.

Hoffer, Jeffrey A., and Straub, Detmar W. Jr. "The 9 to 5 Underground: Are You Policing Computer Crimes?" *Sloan Management Review*, Vol. 30 Issue 4, Summer 1989, pp. 35-44.

Information Management Journal (b). Security Efforts Still Lacking., January / February 2003, Vol. 37 Issue 1, p15.

Kendall, Kenneth E., and Kendall, Julie E. *Systems Analysis and Design, 5th edition*, Prentice Hall, 2002.

Lally, Laura. "Identifying Security Threats and Mitigating their Impact: Lessons from Y2K and 9/11," *Proceedings of the 2003 Conference of the Information Resources Management Association (IRMA)*.

Loch, Karen D., Carr, Houston H., and Warkentin, Merrill E. "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly*, Vol. 16 Issue 2, June 1992, pp. 173-186.

McKeown, Patrick. *Information Technology & The Networked Economy, 2nd edition*, Course Technology Thomson Learning, 2003.

O'Brien, James. *Introduction to Information Systems Essentials for the Internetworked E-Business Enterprise, 10th Edition*, McGraw-Hill, 2001.

Oz, Effy. *Management Information Systems, 3rd edition*, Course Technology Thomson Learning, 2002.

Pfleeger, Charles P.; and Pfleeger, Shari Lawrence. *Security in Computing, 3rd edition*, Prentice Hall, 2003.

Sanderson, Ethan, and Forcht, Karen A. *Information Management & Computer Security*, Vol. 4 Issue 1, 1996, pp. 32-37.

Sequeira, Dinesh, 2003, "Intrusion Prevention Systems – Security's Silver Bullet," http://www.sans.org/rr/paper.php?id=366 , Accessed 9-29-03.

Stair, Ralph M.; and Reynolds, George W. *Principles of Information Systems, 5th edition*, Course Technology Thomson Learning, 2001.

Straub, Detmar W., and Welke, Richard J. "Coping with Systems Risk: Security Planning Models for Management Decision Making (n1)," ***MIS Quarterly*, Vol.** 22 Issue 4, December 1998, pp. 441-469.

Straub, Jr., Detmar W., and Nance, William D. "Discovering and Disciplining Computer Abuse in Organizations: A Field Study," ***MIS Quarterly*, Vol. 14 Issue 1**, March 1990, pp. 44-59.

Vaughn, Rayford B. "Advances in the Provision of System and Software Security – Thirty Years of Progress," *Advances in Computers*, Vol. 58, 2003.

Warkentin, Merrill and Schmidt, Mark B. "Evaluating Executive Perceptions of IS Security Threats and Responses: A Post 9/11 Critique," Proceedings of the 2003 IS OneWorld International Conference. April 2003, Las Vegas, NV.

Willebeek-Lemair, Marc, 2003, "IPSs instantly grant or deny access," *Network World 20(30)*, p. 27.

Yourdon, Edward. *Byte Wars: The Impact of September 11 on Information Technology,* Upper Saddle River, NJ: Prentice Hall, 2002.