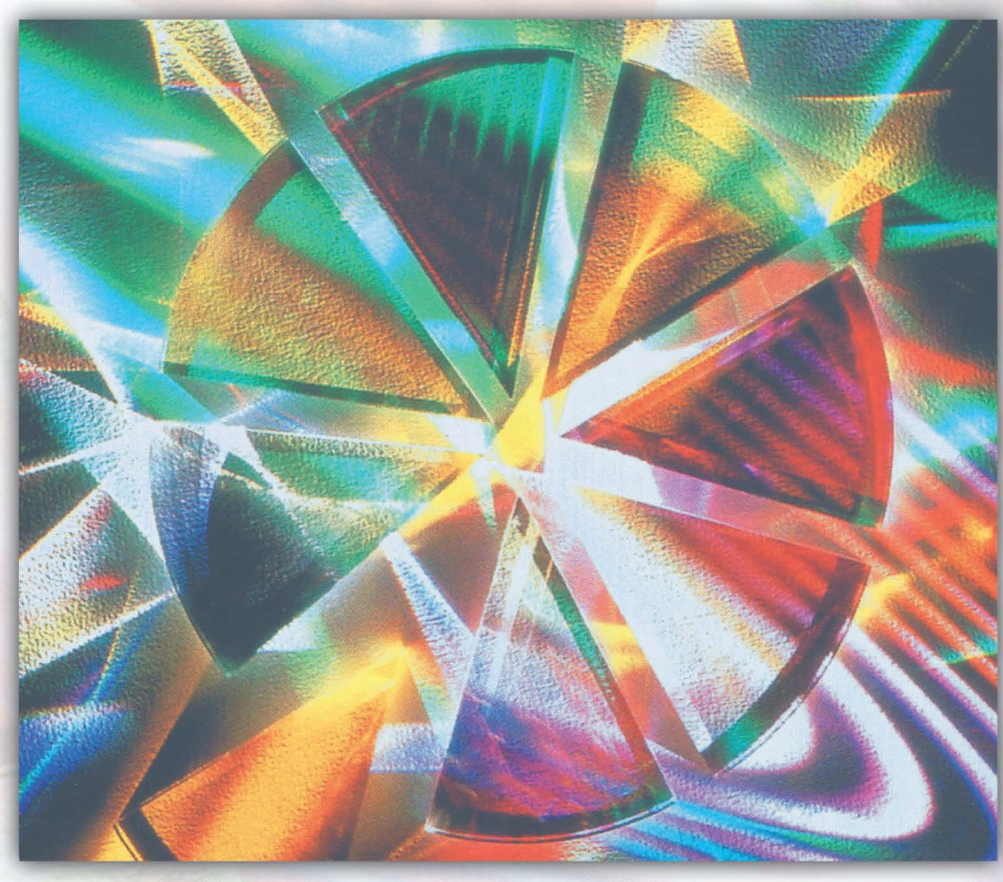
AUERBACH

Information Security Policies, Procedures, and Standards

Guidelines for Effective Information Security Management



THOMAS R. PELTIER

Information Security Policies, Procedures, and Standards

Guidelines for Effective Information Security Management

OTHER AUERBACH PUBLICATIONS

ABCs of IP Addressing
Gilbert Held
ISBN: 0-8493-1144-6

Application Servers for E-Business
Lisa M. Lindgren
ISBN: 0-8493-0827-5

Architectures for E-Business Systems
Sanjiv Purba, Editor
ISBN: 0-8493-1161-6

A Technical Guide to IPSec Virtual Private Networks
James S. Tiller
ISBN: 0-8493-0876-3

Building an Information Security Awareness Program
Mark B. Desman
ISBN: 0-8493-0116-5

Computer Telephony Integration
William Yarberry, Jr.
ISBN: 0-8493-9995-5

Cyber Crime Investigator's Field Guide
Bruce Middleton
ISBN: 0-8493-1192-6

Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes
Albert J. Marcella and Robert S. Greenfield, Editors
ISBN: 0-8493-0955-7

Information Security Architecture
Jan Killmeyer Tudor
ISBN: 0-8493-9988-2

Information Security Management Handbook, 4th Edition, Volume 1
Harold F. Tipton and Micki Krause, Editors
ISBN: 0-8493-9829-0

Information Security Management Handbook, 4th Edition, Volume 2
Harold F. Tipton and Micki Krause, Editors
ISBN: 0-8493-0800-3

Information Security Management Handbook, 4th Edition, Volume 3
Harold F. Tipton and Micki Krause, Editors
ISBN: 0-8493-1127-6

Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management
Thomas Peltier
ISBN: 0-8493-1137-3

Information Security Risk Analysis
Thomas Peltier
ISBN: 0-8493-0880-1

Information Technology Control and Audit
Frederick Gallegos, Sandra Allen-Senft, and Daniel P. Manson
ISBN: 0-8493-9994-7

New Directions in Internet Management
Sanjiv Purba, Editor
ISBN: 0-8493-1160-8

New Directions in Project Management
Paul C. Tinnirello, Editor
ISBN: 0-8493-1190-X

A Practical Guide to Security Engineering and Information Assurance
Debra Herrmann
ISBN: 0-8493-1163-2

The Privacy Papers: Managing Technology and Consumers, Employee, and Legislative Action
Rebecca Herold
ISBN: 0-8493-1248-5

Secure Internet Practices: Best Practices for Securing Systems in the Internet and e-Business Age
Patrick McBride, Joday Patilla, Craig Robinson, Peter Thermos, and Edward P. Moser
ISBN: 0-8493-1239-6

Securing and Controlling Cisco Routers
Peter T. Davis
ISBN: 0-8493-1290-6

Securing E-Business Applications and Communications
Jonathan S. Held and John R. Bowers
ISBN: 0-8493-0963-8

Securing Windows NT/2000: From Policies to Firewalls
Michael A. Simonyi
ISBN: 0-8493-1261-2

TCP/IP Professional Reference Guide
Gilbert Held
ISBN: 0-8493-0824-0

AUERBACH PUBLICATIONS

www.auerbach-publications.com
To Order Call: 1-800-272-7737 • Fax: 1-800-374-3401
E-mail: orders@crcpress.com

Information Security Policies, Procedures, and Standards

Guidelines for Effective Information Security Management

THOMAS R. PELTIER

AUERBACH PUBLICATIONS

A CRC Press Company

Boca Raton London New York Washington, D.C.

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Version Date: 20131029

International Standard Book Number-13: 978-0-8493-9032-6 (eBook - PDF)

Dedication

To Lisa, my editor and life compass

Contents

Acknowledgments

It seems that I have spent the greatest part of my working life writing policies and procedures. As the result of an ongoing audit at the company where I was working, I was asked to step in and develop a set of information security policies and procedures. Because I had taken courses in writing fiction and poetry and had a poem published in the school literary journal, I felt I was highly qualified for this task. Little did I know. After a couple of attempts, I took everything I had learned about image development, character development, complex sentences and threw it all away. I had to go back to the basics and I had a lot of questions. These questions were answered by a tremendous group of professionals who have become my friends.

First in my list of acknowledgments is my mentor and friend, John O'Leary, the Director of the Computer Security Institute–Education Resource Center. No matter what the subject, John seems to have some experience in all areas of information security, and he is always ready to lend an opinion and direction. It was his encouragement to "try it; if they don't stone you, then you're onto something." John's approach is always a bit more formal than mine, but he encouraged me to find the path of least resistance. John and his wonderful wife Jane have always been available to bounce ideas off of or just to listen and offer advice.

Lisa Bryson is my friend, fellow information security professional, editor, and now my wife. We have known each other for almost 15 years and have had many a lively discussion on how security should be implemented. She always reminds me that not many people can see the smile on your face through your writings. Say what you mean, and do not be a wise guy. I hate it when she is always right.

Next on my list is Pat Howard. I must have been a very good person in a previous life to be afforded the opportunity to meet and work with Pat. He is able to take some of my ramblings, my very bad drawings on flipcharts, and turn them into finished products. He keeps me on track and provides insight on the new standards and other requirements.

John Blackley and Terri Curran are two dear friends who have allowed me to review and research their materials, and they did the same for me. Before we

were consultants, we worked at organizations that required policies, procedures, and standards, but did not want anything to impede the business process. John, Terri, and I spent many hours discussing how to get management to understand just how bright we were and that our documents were going to save our companies in spite of themselves.

Who can leave out his publisher? Certainly not me; Rich O'Hanley has taken the time to discuss policies and procedures with numerous organizations to understand what their needs are and then presented these findings to me. A great deal of my work here is a direct result of what Rich discovered the industry wanted.

Others who have helped me along the way include:

- Justin Peltier, my son, fellow information security professional, and best friend
- William H. Murray, the first person I heard speak on the security needs of organizations, and who has inspired me ever since
- Hal Tipton, the steady voice of reason in this crazy profession
- Charles Cressen Wood, fellow writer
- Harry DeMaio, whose book (*Information Security and Other Unnatural Acts*) gave great insight into just how difficult our task is
- Mike Corby, my friend and now boss. (I have known Mike for over 25 years, and he has always given the best and most honest advice. If you would like the prototype for the honest man, you could stop the search when you meet Mike Corby.)
- Rich O'Hanley, not only the world's best editor and task master, but a good friend and source of knowledge. How he keeps his sanity while working with writers is totally beyond me. Thanks Rich!

Introduction

The purpose of an information security program is to protect the valuable information resources of an enterprise. Through the selection and application of appropriate policies, standards, and procedures, an overall security program helps the enterprise meet its business objective or mission charter. Because security is sometimes viewed as thwarting business objectives, it is necessary to ensure that effective, well-written policies, standards, and procedures are implemented.

When writing information security polices, standards, and procedures, it is necessary to make certain that proper grammar and punctuation are used. Part of an effective book on writing should discuss these topics. The importance of an effective topic sentence to the overall success of a policy statement must be addressed.

Since I came into the information security profession in 1977, we have discussed the need for standardization of the practice. We saw the beginnings of this process when the National Institute of Standards and Technology (NIST) began publishing such documents as *An Introduction to Computer Security: The NIST Handbook* (NIST Special Publication 800-12).

Now the International Organization of Standardization (ISO) has published the recently adopted *Information Technology— Code of Practice for Information Security Management* (ISO 17799) and its parent British Standards (BS 7799). These documents and others, such as *Banking and Related Financial Services — Information Security Guidelines* (ISO/TR 13569), the Health Insurance Portability and Accountability Act (HIPAA), Privacy of Consumer Financial Information (Graham-Leach-Bliley Act), and the Generally Accepted Information Systems Security Practices (GASSP), have stepped into the void and provided all security professionals with a map of where to take the information security program.

Although the title of this book is *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management,* security is not the end product of these documents. Good security must be measured in how well the assets of the enterprise are protected while the mission and business objectives are met. This book will teach the reader how

to develop policies, procedures, and standards that can be used in all aspects of enterprise activities.

Chapter 1

Overview: Information Protection Fundamentals

The purpose of information protection is to protect the valuable resources of an organization, such as information, hardware, and software. Through the selection and application of appropriate safeguards, security helps the organization to meet its business objectives or mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets. We examine the elements of computer security, employee roles and responsibilities, and common threats. We also examine the need for management controls, polices and procedures, and risk analysis. Finally, we present a comprehensive list of tasks, responsibilities, and objectives that make up a typical information protection program.

1.1 Elements of Information Protection

Information protection should be based on eight major elements:

1. Information protection should support the business objectives or mission of the enterprise. This idea cannot be stressed enough. All too often, information security personnel lose track of their goals and responsibilities. The position of ISSO (Information Systems Security Officer) has been created to support the enterprise, not the other way around.
2. Information protection is an integral element of due care. Senior management is charged with two basic responsibilities: a *duty of loyalty*, which means that whatever decisions it makes must be made in the best interest of the enterprise, and a *duty of care*, which means that senior management is required to protect the assets of the

enterprise and make informed business decisions. An effective information protection program will assist senior management in performing these duties.

3. Information protection must be cost-effective. Implementing controls based on edicts is counter to the business climate. Before any control can be proposed, it is necessary to confirm that a significant risk exists. Implementing a timely risk analysis process can accomplish this. By identifying risks and then proposing appropriate controls, the mission and business objectives of the enterprise will be better met.
4. Information protection responsibilities and accountabilities should be made explicit. For any program to be effective, it is necessary to publish an information protection policy statement and an information protection group mission statement. The policy should identify the roles and responsibilities of all employees. To be completely effective, the language of the policy must be incorporated into the purchase agreements for all contract personnel and consultants.
5. System owners have information protection responsibilities outside their own organization. Access to information often extends beyond the business unit or even the enterprise. It is the responsibility of the information owner (normally the senior-level manager in the business that created the information or the primary user of the information). A main responsibility is to monitor usage to ensure that it complies with the level of authorization granted to the user.

   If a system has external users, its owners have a responsibility to share appropriate knowledge about the existence and general extent of control measures so that other users can be confident that the system is adequately secure. As the user base expands to include suppliers, vendors, clients, customers, shareholders, and the like, it is incumbent upon the enterprise to have clear and identifiable controls. For many organizations, the initial sign-on screen is the first indication that there are controls in place. The message screen should include three basic elements:

   a. That the system is for authorized users only
   b. That activities are monitored
   c. That by completing the sign-on process, the user agrees to the monitoring
6. Information protection requires a comprehensive and integrated approach. To be as effective as possible, it is necessary for information protection issues to be part of the system development life cycle. During the initial or analysis phase, information protection should include a risk analysis, a business impact analysis, and an information classification document. Additionally, because information is resident in all departments throughout the enterprise, each business unit should establish an individual responsible for implementing the information protection program to meet the specific business needs of the department.

7. Information protection should be periodically reassessed. As with anything, time changes the needs and objectives. A good information protection program examines itself on a regular basis and makes changes wherever and whenever necessary. This is a dynamic and changing process and therefore must be reassessed at least every 18 months.
8. Information protection is constrained by the culture of the organization. The ISSO must understand that the basic information protection program will be implemented throughout the enterprise. However, each business unit must be given the latitude to make modifications to meet its specific needs. If your organization is multinational, it is necessary to make adjustments for each of the various countries. These adjustments will have to be examined throughout the United States. What might work in Des Moines, Iowa may not fly in Berkeley, California. Provide for the ability to find and implement alternatives.

Information protection is a means to an end and not the end in itself. In business, having an effective information protection program is usually secondary to the need to make a profit. In the public sector, information protection is secondary to the services the agency provides. Security professionals must not lose sight of these tenets.

Computer systems and the information processed on them are often considered critical assets that support the mission of an organization. Protecting them can be as important as protecting other organizational resources, such as financial resources, physical assets, and employees. The cost and benefits of information protection should be carefully examined in both monetary and nonmonetary terms to ensure that the cost of controls does not exceed the expected benefits. Information protection controls should be appropriate and proportionate.

1.2 More Than Just Computer Security

Providing effective information protection requires a comprehensive approach that considers a variety of areas both within and outside the information technology area. An information protection program is more than establishing controls for the computer-held data. It should address all forms of information. In 1965, the idea of the "paperless office" was first introduced. The advent of the third-generation computers brought about this concept. However, today the bulk of all the information available to employees and others is still found in printed form. To be an effective program, information protection must move beyond the narrow scope of IT and address the issues of enterprisewide information protection. A comprehensive program must touch every stage of the information asset life cycle, from creation to eventual destruction. The fundamental element to this corporatewide program is an Information Security Policy that is part of the corporate policies and does not come from IT.

1.2.1 Employee Mind-Set toward Controls

Access to information and the environments that process it are dynamic. Technology and users, data and information in the systems, risk associated with the system, and security requirements are ever-changing. The ability of information protection to support business objectives or the mission of the enterprise may be limited by various factors, such as the current mind-set toward controls.

A highly effective method of measuring the current attitude toward information protection is to conduct a "walkabout." After hours or on a weekend, conduct a review of the workstations throughout a specific area (usually a department or a floor) and look for just five basic control activities:

1. Offices secured
2. Desk and cabinets secured
3. Workstations secured
4. Information secured
5. Diskettes secured

Conducting an initial walkabout in the typical office environment will reveal a 90 to 95 percent noncompliance rate with at least one of these basic control mechanisms. The result of this review should be used to form the basis for an initial risk analysis to determine the security requirements for the office environment. When conducting such a review, employee privacy issues must be considered.

1.3 Roles and Responsibilities

As discussed before, senior management has the ultimate responsibility for the protection of the organization's information assets. One responsibility is the establishment of the function of Corporate Information Officer (CIO). The CIO directs the day-to-day management of information assets of the organization. The ISSO and Security Administrator should report directly to the CIO and are responsible for the day-to-day administration of the information protection program.

Supporting roles are performed by the service providers and by the Systems Operations team that designs and operates the computer systems. They are responsible for implementing technical security on the systems. The telecommunications department is responsible for providing communication services, including voice, data, video, and fax. Security mechanisms must be implemented to protect these communication services.

The information protection professional must establish strong working relationships with the audit staff. If the only time you see the audit staff is when they are in for a formal audit, then you probably do not have a good working relationship. It is vitally important that this liaison be established and that you meet to discuss common problems at least each quarter.

Other groups include the physical security staff and the contingency planning group. These groups are responsible for establishing and implementing controls and can form a peer group to review and discuss controls. The group responsible for application development methodology will assist in the implementation of information protection requirements in the application system development life cycle. The quality assurance group can assist in ensuring that information protection requirements are included in all development projects prior to movement to production.

The Procurement group can work to get the language of the information protection policies included in the purchase agreements for contract personnel. Education and Training can assist in the development and implementation of information protection awareness programs and in training supervisors on how to monitor employee activities. Human Resources will be the organization responsible for taking appropriate action on any violations of the organization information protection policy.

An example of a typical job description for an information security professional is shown in Exhibit 1.

Exhibit 1 Typical Job Description

Director, Design and Strategy

Location: Anywhere, World
Practice Area: Corporate Global Security Practice
Grade:

Purpose:

To create an information security design and strategy practice that defines the technology structure needed to address the security needs of its clients. The information security design and strategy will complement security and network services developed by the other Global Practice areas. The design and strategy practice will support the clients' information technology and architecture and integrate with each enterprise's business architecture. This security framework will provide for the secure operation of computing platforms, operating systems, and networks, both voice and data, to ensure the integrity of the clients' information assets. To work on corporate initiatives to develop and implement the highest quality security services and ensure that industry best practices are followed in their implementation.

Working Relationships:

This position reports in the Global Security Practice to the Vice President, Global Security. Internal contacts are primarily Executive Management, Practice Directors, Regional Management, as well as mentoring and collaborating with consultants. This position will directly manage two professional positions: Manager, Service Provider Security Integration; and Service Provider Security Specialist. Frequent external contacts include building relationships with clients, professional information security organizations, other information security consultants, vendors of hardware, software, and security services, and various regulatory and legal authorities.

(*continued*)

Exhibit 1 Typical Job Description (continued)

Principal Duties and Responsibilities:
The responsibilities of the Director, Design and Strategy include, but are not limited to, the following:

- Develop global information security services that will provide the security functionality required to protect clients' information assets against unauthorized disclosure, modification, and destruction. Particular focus areas include:
  - Virtual private networks
  - Data privacy
  - Virus prevention
  - Secure application architecture
  - Service provider security solutions
- Develop information security strategy services that can adapt to clients' diverse and changing technological needs.
- Work with Network and Security practice leaders and consultants, create sample architectures that communicate the security requirements that will meet the needs of all client network implementations.
- Work with practice teams to aid them from the conception phase to the deployment of the project solution. This includes quality assurance review to ensure that the details of the project are correctly implemented according to the service delivery methodology.
- Work with the clients to collect their business requirements for electronic commerce, while educating them on the threats, vulnerabilities, and available risk mitigation strategies.
- Determine where and how you should use cryptography to provide public key infrastructure and secure messaging services for clients.
- Participate in security industry standards bodies to ensure strategic information security needs will be addressed.
- Conduct security focus groups with the clients to cultivate an effective exchange of business plans, product development, and marketing direction to aid in creating new and innovative service offerings to meet client needs.
- Continually evaluate vendors' product strategies and future product statements and advise which will be most appropriate to pursue for alliances, especially in the areas of:
  - Virtual private networks
  - Data privacy
  - Virus prevention
  - Secure application architecture
  - Service provider security solutions
- Provide direction and oversight of hardware and software-based cryptography service development efforts.

Accountability:
Maintain the quality and integrity of the services offered by the Global Security Practice. Review and report impartially on the potential viability and profitability of new security services. Assess the operational efficiency, compliance to industry standards, and effectiveness of the client network designs and strategies that are implemented through the company's professional service offerings. Exercise professional judgment in making recommendations that may impact business operations.

Exhibit 1 Typical Job Description (continued)

Knowledge and Skills:

- 10 Percent Managerial/Practice Management
  - Ability to supervise a multidisciplinary team and a small staff; must handle multiple tasks simultaneously; ability to team with other Practice Directors and Managers to develop strategic service offerings
  - Willingness to manage or to personally execute necessary tasks, as resources are required
  - Excellent oral, written, and presentation skills
- 40 Percent Technical
  - In-depth technical knowledge of information-processing platforms, operating systems, and networks in a global distributed environment
  - Ability to identify and apply security techniques to develop services to reduce clients' risk in such an environment
  - Technical experience in industrial security, computer systems architecture, design, and development, physical and data security, telecommunications networks, auditing techniques, and risk analysis principles
  - Excellent visionary skills that focus on scalability, cost-effectiveness, and implementation ease
- 20 Percent Business
  - Knowledge of business information flow in a multinational, multiplatform networked environment
  - Solid understanding of corporate dynamics and general business processes; understanding of multiple industries
  - Good planning and goal-setting skills
- 20 Percent Interpersonal
  - Must possess strong consulting and communication skills
  - Ability to work with all levels of management to resolve issues
  - Must understand and differentiate between tactical and strategic concepts
  - Must be able to weigh business needs with security requirements
  - Must be self-motivating

Attributes:

Must be mature, self-confident, and performance oriented. Will clearly demonstrate an ability to lead technological decisions. Will establish credibility with personal dedication, attention to detail, and a hands-on approach. Will have a sense of urgency in establishing security designs and strategies to address new technologies to be deployed addressing clients' business needs. Will also be capable of developing strong relationships with all levels of management. Other important characteristics will be the ability to function independently, holding to the highest levels of personal and professional integrity. Will be an excellent communicator and team player.

Specific requirements include:

- Bachelor's degree (Master's degree desirable), advanced degree preferred
- Fifteen or more years of information technology consulting or managerial experience, eight of those years spent in information security positions

(*continued*)

Exhibit 1 Typical Job Description (continued)

- CISSP certification preferred (other appropriate industry or technology certifications desirable)

Potential Career Path Opportunities:
Opportunities for progression to a VP position within the company

1.4 Common Threats

Information processing systems are vulnerable to many threats that can inflict various types of damage resulting in significant losses. This damage can range from errors harming database integrity to fires destroying entire complexes. Losses can stem from the actions of supposedly trusted employees defrauding a system, from outside hackers, or from careless data entry. Precision in estimating information protection-related losses is not possible because many losses are never discovered, and others are covered up to avoid unfavorable publicity.

The typical computer criminal is an authorized, nontechnical user of the system who has been around long enough to determine what actions would cause a "red flag" or an audit. The typical computer criminal is an employee. According to a recent survey in the "Current and Future Danger: A CSI Primer on Computer Crime & Information Warfare," more than 80 percent of the respondents identified employees as a threat or potential threat to information security. Also included in this survey were the competition, contract personnel, public interest groups, suppliers, and foreign governments.

The chief threat to information protection is still errors and omissions. This concern continues to make up 65 percent of all information protection problems. Users, data entry personnel, system operators, programmers, and the like frequently make errors that contribute directly or indirectly to this problem.

Dishonest employees make up another 13 percent of information protection problems. Fraud and theft can be committed by insiders and outsiders, but are more likely to be done by employees. In a related area, disgruntled employees make up another 10 percent of the problem. Employees are most familiar with the information assets and processing systems of the organization, including knowing what actions might cause the most damage, mischief, or sabotage.

Common examples of information protection-related employee sabotage include destroying hardware or facilities, planting malicious code (viruses, worms, Trojan horses, etc.) to destroy data or programs, entering data incorrectly, deleting data, altering data, and holding data "hostage."

The loss of the physical facility or the supporting infrastructure (power failures, telecommunications disruptions, water outage and leaks, sewer problems, lack of transportation, fire, flood, civil unrest, strikes, etc.) can lead to serious problems and makes up eight percent of information protection-related problems.

The final area is malicious *hackers* or *crackers.* These terms refer to those who break into computers without authorization or exceed the level of authorization granted to them. Although these problems receive the largest amount of press coverage, they only account for five to eight percent of the total picture. They are real and they can cause a great deal of damage. But when attempting to allocate limited information protection resources, it may be better to concentrate efforts in other areas. To be certain, conduct a risk analysis to see what your exposure might be.

1.5 Policies and Procedures

An information protection policy is the documentation of enterprisewide decisions on handling and protecting information. In making these decisions, managers face hard choices involving resource allocation, competing objectives, and organization strategy related to protecting both technical and information resources as well as guiding employee behavior.

When creating an information protection policy, it is best to understand that information is an asset of the enterprise and is the property of the organization. As such, information reaches beyond the boundaries of IT and is present in all areas of the enterprise. To be effective, an information protection policy must be part of the organization asset management program and must be enterprisewide.

There are as many forms, styles, and kinds of policy as there are organizations, businesses, agencies, and universities. In addition to the various forms, each organization has a specific culture or mental model of what a policy is, how it is to look, and who should approve the document. The key point here is that every organization needs an information protection policy. According to the 2000 CSI report on Computer Crime, 65 percent of respondents to its survey admitted that they do not have a written policy. The beginning of an information protection program is the implementation of a policy. The program policy creates the attitude of the organization toward information and announces internally and externally that information is an asset and the property of the organization and is to be protected from unauthorized access, modification, disclosure, and destruction.

This book leads the policy writer through the key structure elements and then reviews some typical policy contents. Because policies are not enough, this book teaches the reader how to develop standards, procedures, and guidelines. In each section the reader is given advice on the structural mechanics of the various documents as well as actual examples.

1.6 Risk Management

Risk is the possibility of something adverse happening. The process of risk management is identifying those risks, assessing the likelihood of their occurrence, and then taking steps to reduce the risk to an acceptable level. All risk

analysis processes use the same methodology. Determine the asset to be reviewed. Identify the risk, issues, threats, or vulnerabilities. Assess the probability of the risk occurring and the impact to the asset or the organization should the risk be realized. Then identify controls that would bring the impact to an acceptable level.

The 2001 CRC Press book titled *Information Security Risk Analysis* discusses effective risk analysis methodologies. The book takes the reader through the theory of risk analysis:

- Identify the asset
- Identify the risks
- Prioritize the risks
- Identify controls and safeguards

The book helps the reader understand qualitative risk analysis and then gives examples of this process. To make certain that the reader receives a well-rounded exposure to risk analysis, the book presents eight different methods, ending with the Facilitated Risk Analysis Process (FRAP).

The primary function of information protection risk management is the identification of appropriate controls. In every assessment of risk, there will be many areas for which it will not be obvious what kind of controls are appropriate. The goal of controls is not to have 100 percent security. Total security would mean zero productivity. Controls must never lose sight of the business objectives or mission of the enterprise. Whenever there is a contest for supremacy, controls lose, productivity wins. This is not a contest, however. The goal of information protection is to provide a safe and secure environment for management to meet its duty of care.

When selecting controls, you will need to consider many factors, including the information protection policy of the organization, the legislation and regulations that govern your enterprise, along with safety, reliability, and quality requirements. Remember that every control will require some performance requirements. These performance requirements may be a reduction in user response time, additional requirements before applications are moved into production, or additional costs.

When considering controls, the initial implementation cost is only the tip of the cost iceberg. The long-term cost for maintenance and monitoring must be identified. Be sure to examine any and all technical requirements and cultural constraints. If your organization is multinational, control measures that work and are accepted in your home country might not be accepted in other countries.

Accept residual risk. At some point management must decide if the operation of a specific process or system is acceptable, given the risk. There can be any number of reasons that a risk must be accepted. These include but are not limited to:

- The type of risk may be different from previous risks.
- The risk may be technical and difficult for a layperson to grasp.
- The current environment may make it difficult to identify the risk.

Information protection professionals sometimes forget that the managers hired by our organizations have the responsibility to make decisions. The job of the ISSO is to help the information asset owners identify risks to the assets. Assist them in identifying possible controls and then allow them to determine their action plan. Sometimes, they will choose to accept the risk, and this is perfectly permissible.

1.7 Typical Information Protection Program

Over the years, the computer security group responsible for access control and disaster recovery planning has evolved into the enterprisewide information protection group. Included in their ever-expanding roles and responsibilities are:

- Firewall control
- Risk analysis
- Business impact analysis
- Virus control and virus response
- Computer emergency response
- Computer crime investigation
- Records management
- Encryption
- E-mail, voice-mail, Internet, video-mail policy
- Enterprisewide information protection program
- Industrial espionage controls
- Contract personnel nondisclosure agreements
- Legal issues
- Internet monitoring
- Disaster planning
- Business continuity planning
- Digital signature
- Secure single sign-on
- Information classification
- Local area networks
- Modem control
- Remote access
- Security awareness programs

In addition to these elements, the security professional now has to ensure that standards, both in the United States and worldwide, are examined and acted upon where appropriate. This book discusses these new standards in detail.

1.8 Summary

The role of the information protection professional has changed over the past 25 years and will change again and again. Implementing controls to be in

compliance with audit requirements is not the way to run such a program. There are limited resources available for controls. To be effective, information owners and users must accept the controls. To meet this end, it will be necessary for information protection professionals to establish partnerships with their constituency. Work with your owners and users to find an appropriate level of controls. Understand the needs of the business or the mission of your organization. Make certain that information protection supports those goals and objectives.

Appendix G

References

1. Bryson, Lisa. Protect your boss and your job: Due care in information security. *Computer Security Alert*. Number 146, May 1995, pp. 4 and 8.
2. d'Agenais, J. and J. Carruthers. *Creating Effective Manuals*. Cincinnati, OH: South-Western Publishing Co., 1985.
3. DeMaio, H. *Information Protection and Other Unnatural Acts*. New York: AMACOM, 1992.
4. Frank, Milo O., *How to Get Your Point Across in 30 Seconds or Less*. New York: Pocket Books, 1986.
5. Frank, Stanley D., *The Evelyn Wood Seven-Day Speed Reading and Learning Program*. New York: Barnes & Noble Books, 1990.
6. Fine, N. The economic espionage act: Turning fear into compliance. *Competitive Intelligence Review*. Volume 8, Number 3, Fall 1997.
7. Fites, P. and M. Kratz. *Information Systems Security: A Practitioner's Reference*. New York: Van Nostrand, 1993.
8. Guttman, B. and E. Roback. *An Introduction to Computer Security: The NIST Handbook*. Gaithersburg, MD: U.S. Department of Commerce, 1995.
9. Jordan, K. Ethics and compliance programs: Keeping your boss out of jail and your company off of the front pages. *Betterley's Risk Management*. April, 1998.
10. Krause, M. and H. Tipton (editors). *Handbook of Information Security Management*. New York: Auerbach, 1998.
11. Lincoln, J. A. EPA's policy on incentives for self-policing, federal sentencing guidelines and other carrots and sticks. *Forum for Best Management Practices*. 1997.
12. Navran, F. A decision maker's guide to the federal sentencing guidelines for ethics violations. *Navran Associates' Newsletter*. March 1996.
13. Palmer, I. and G. Potter. *Computer Security Risk Management*. New York: Van Nostrand Reinhold, 1989.
14. Peltier, T. *Policies and Procedures for Data Security*. San Francisco, CA: Miller Freeman, 1991.
15. Peltier, Thomas R., *Information Security Policies and Procedures: A Practitioner's Reference*. Boca Raton, FL: CRC Press, 1999.
16. Tomasko, R. *Rethinking the Corporation: The Architecture of Change*. New York: AMACOM, 1993.

17. Information-Technology — Code of Practice for Information Security Managment. ISO/IEC, 2000.
18. Banking and Related Financials Services — Information Security Guidelines. ISO, 1997.