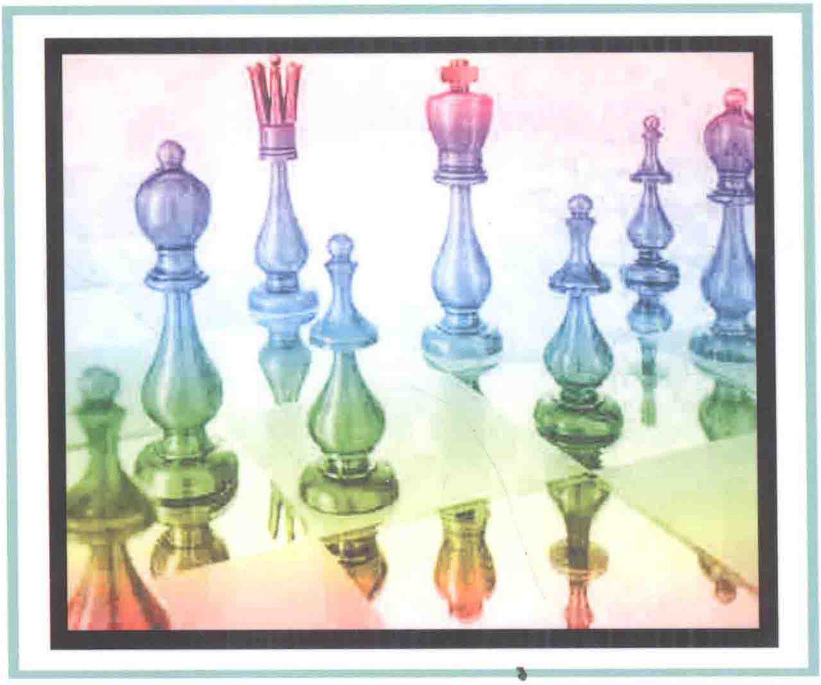
Information Security FUNDAMENTALS

Second Edition



Thomas R. Peltier

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

Information Security FUNDAMENTALS

Second Edition

Thomas R. Peltier

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

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

Printed on acid-free paper
Version Date: 20130626

International Standard Book Number-13: 978-1-4398-1062-0 (Paperback)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Library of Congress Cataloging-in-Publication Data

Peltier, Thomas R.
Information security fundamentals / Thomas R. Peltier. -- Second edition.
pages cm
Includes bibliographical references and index.
ISBN 978-1-4398-1062-0 (pbk.)
1. Computer security. 2. Data protection. I. Title.

QA76.9.A25P427 2013
005.8--dc23 2013023074

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

To the souls that left us too early: Justin Peltier, Gene Schultz,
and Brad Smith. They were always eager to try new things first—
I know they will make our next meeting a joyous occasion.

Acknowledgments

This book is the combined effort of many industry professionals. This group includes John Blackley, Maria Dailey, Pat Howard, Charles Johnson, Kimberly Logan, Kevin McLaughlin, John O'Leary, Justin Peltier, Tom Peltier, Jeff Sauntry, Quinn Shamblin, Brad Smith, and William Tompkins.

For more than a decade, SecureWorld has expanded and improved the concept of affordable regional security conferences. By ensuring knowledgeable speakers and quality educational and training programs, the security professional is able to stay current and cultivate contacts to help provide a means to get questions answered and problems solved. Mike O'Gara, Kerry Nelson, and the entire SecureWorld team are serving the industry well.

No one has all the answers to any question, so the really "smart" person cultivates good friends. Being in the information security business for nearly 40 years, I have had the great good fortune of having a number of such friends and fellow professionals. This group of longtime sources of great information includes John and Jane O'Leary, Lisa Bryson, Mike Corby, Terri Curran, Peter Stephenson, Merrill Lynch, Bob Cartwright, Pat Howard, Cheryl Jackson, Becky Herold, Ray Kaplan, Anne Terwilliger, David Lynas, John Sherwood, Herve Schmidt, Antonio and Pietro Ruvolo, Wayne Sumida, Dean Feldpausch, and William H. Murray.

My working buddies also need to be acknowledged. My son Justin was the greatest asset any father and information security team could ever hope for. Over the years, we logged thousands of air miles together and touched five continents. Every day I learned something new from him. I miss him greatly each and every day.

The other working buddy is John Blackley, a strange Scotsman who makes my life more fun and interesting. I've worked with John since 1985 and have marveled at how well he takes obtuse concepts and condenses them so that even management types can understand.

Who can leave out their publisher? Certainly not me. Rich O'Hanley has taken the time to discuss security issues with numerous organizations to understand what their needs are and then presented these findings to us. A great deal of our work here is a direct result of what Rich discovered that the industry wanted. Rich is not only the world's best editor and taskmaster but also a good friend and source of knowledge. Thanks, Rich!

Introduction

The purpose of information security is to protect an organization's valuable resources, such as information, computer hardware, and software. Through the selection and application of appropriate safeguards, security helps an organization's mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets. To many, security is sometimes viewed as thwarting the business objectives of an organization by imposing poorly selected, bothersome rules and procedures on users, managers, and systems. Well-chosen security rules and procedures do not exist for their own sake—they are put in place to protect important assets and thereby support the overall business objectives.

Developing an information security program that adheres to the principle of security as a business enabler is the first step in an enterprise's effort to build an effective security program. Organizations must continually (1) explore and assess information security risks to business operations; (2) determine what policies, standards, and controls are worth implementing to reduce these risks; (3) promote awareness and understanding among the staff; and (4) assess compliance and control effectiveness. As with other types of internal controls, this is a cycle of activity, not an exercise with a defined beginning and end.

This book has been designed to give the information security professional a solid understanding of the fundamentals of security and the entire range of issues the practitioner must address. We hope that you will be able to take the key elements that comprise a successful information security program and implement the concepts into your own successful program. Each chapter has been written by a different author and will ensure that the reader gets the benefit of different ideas and approaches.

Information Security Fundamentals

Overview

The purpose of information security is to protect an organization's valuable resources, such as information, hardware, and software. Through the selection and application of appropriate safeguards, security helps an 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 will examine the elements of computer security, employee's roles and responsibilities, and common threats. We will also examine the need for management controls, policies and procedures, and risk management. Finally, we will include current examples of procedures, policies, and examples that can be used to help implement the security program at your organization.

Elements of Information Security

Information security should be based on eight major elements:

1. Information security 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 information security professional has been created to support the enterprise, not the other way around.
2. Information security is an integral element of fiduciary duty. Senior management is charged with two basic responsibilities: a *duty of loyalty*—this means that whatever decisions they make must be made in the best interest of the enterprise. They are also charged with a *duty of care*—this means that senior management is required to implement reasonable and prudent controls to protect the assets of the enterprise and make informed business decisions.

An effective information security program will assist senior management in meeting these duties.

3. Information security must be cost-effective. Implementing controls based on edicts is counter to the business climate. Before any control can be proposed, it will be necessary to confirm that a significant risk exists. Implementing a timely risk management process can complete this task. By identifying risks and then proposing appropriate controls, the mission and business objectives of the enterprise will be better met.
4. Information security responsibilities and accountabilities should be made explicit. For any program to be effective, it will be necessary to publish an information security policy statement and a group mission statement. The policy should identify the roles and responsibilities of all employees. To ensure third parties comply with our policies and procedures, the contract language indicating these requirements must be incorporated into the purchase agreements for all contract personnel and consultants.
5. System owners have information security responsibilities outside their own organization. Access to information will often extend 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 is the primary user of the information). One of the main responsibilities is to monitor usage to ensure that it complies with the level of authorization granted to the user.
6. Information security requires a comprehensive and integrated approach. To be as effective as possible, it will be necessary for information security issues to be part of the system development life cycle. During the initial or analysis phase, information security should receive as its deliverables a risk assessment, 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 an information security program to meet the specific business needs of the department.
7. Information security should be periodically reassessed. As with anything, time changes the needs and objectives. A good information security program will examine itself on a regular basis and make changes wherever and whenever necessary. This is a dynamic and changing process and therefore must be reassessed at least every 18 months.
8. Information security is constrained by the culture of the organization. The information security professional must understand that the basic information security program will be implemented throughout the enterprise. However, each business unit must be given the latitude to make modifications to meet their specific needs. If your organization is multinational, it will be necessary to make adjustments for each of the various countries. These adjustments will

have to be examined throughout the United States too. What might work in Des Moines, Iowa, may not fly in Berkley, California. Provide for the ability to find and implement alternatives.

Information security is a means to an end and not the end in itself. In business, having an effective information security program is usually secondary to the need to make a profit. In the public sector, information security is secondary to the agency's services provided to its constancy. We, as security professionals, must not lose sight of these goals and objectives.

Information systems and the information processed on them are often considered to be 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 security should be carefully examined in both monetary and nonmonetary terms to ensure that the cost of controls does not exceed the expected benefits. Information security controls should be appropriate and proportionate.

The responsibilities and accountabilities of the information owners, providers, and users of computer services and other parties concerned with the protection of information and computer assets should be explicit. 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 we expand the user base 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:

1. The system is for authorized users only
2. Activities are monitored
3. By completing the sign-on process, the user agrees to the monitoring

More than Just Computer Security

Providing effective information security requires a comprehensive approach that considers a variety of areas both within and outside of the information technology area. An information security program is more than establishing controls for the computer-held data. In 1965, the idea of the "paperless office" was first introduced. The advent of third-generation computers brought about this concept. However, today, a vast quantity of all the information available to employees and others is still found in nonelectronic form. To be an effective program, information security must move beyond the narrow scope of IT and address the issues of enterprise-wide information security. A comprehensive program must touch every stage of the information asset life cycle from creation to eventual destruction.

Employee Mindset Toward Controls

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

A highly effective method of measuring the current attitude toward information security 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. Desks and cabinets secured
3. Workstations secured
4. Information secured
5. Electronic media secured

When conducting an initial walkabout, the typical office environment will have a 90% to 95% 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 assessment to determine the security requirements for the workstation area. When conducting such a review, employee privacy issues must be remembered.

Roles and Responsibilities

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

Supporting roles are performed by the service providers and include Systems Operations, whose personnel design and operate the computer systems. They are responsible for implementing technical security on the systems. Telecommunications is responsible for providing communication services, including voice, data, video, and wireless.

The information security professional must also 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 don't have a good working relationship. It is vitally important that this liaison is established and that you meet to discuss common problems at least each quarter.

Other support 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 security requirements in the application system development life cycle. Quality assurance can assist in ensuring that information security requirements are included in all development projects before moving on to production.

The Procurement Group can work to get the language of the information security policies included in the purchase agreements for contract personnel. Education and Training can assist in the development and conducting of information security awareness programs and for training supervisors in the responsibility to monitor employee activities. Human Resources will be the organization responsible for taking appropriate action for any violations of the organization's information security policy.

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

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 security–related losses is not possible because many losses are never discovered, whereas others are hidden 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 *Current and Future Danger: A CSI Primer on Computer Crime & Information Warfare* by Richard Power, more than 80% 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 security is still errors and omissions. This concern continues to make up 65% of all information loss problems. Users, data entry

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.

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:
  - Wireless security
  - 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 to 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

Figure I.1 Sample information security job description.

- Determine where and how cryptography should be used 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:
  - Remote access
  - Data privacy
  - Virus prevention
  - Secure application architecture
  - Service provider security solutions
- Provide direction and oversight of hardware-based 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 affect business operations.

Knowledge and Skills

- 40% 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
- 10% 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, information systems architecture, design, and development, physical and data security, telecommunication networks, auditing techniques, and risk management principles
- Excellent visionary skills that focus on scalability, cost-effectiveness, and ease of implementation
- 25% 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
- 25% 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-motivated

Figure I.1 (Continued) Sample information security job description.

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

Potential Career Path Opportunities

Opportunities for progression to a VP position within the company

Figure I.1 (Continued) Sample information security job description.

personnel, system operators, programmers, and the like frequently make errors that contribute directly or indirectly to this problem.

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

Common examples of information security–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.) could lead to serious problems and make up 8% of all information security–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 get the largest amount of press coverage and movies, they only account for 5% to 8% of the total picture. They are real, however, and they can cause a great deal of damage. But when attempting to allocate limited information security resources, it may be better to concentrate efforts in other areas. To be certain, conduct a risk assessment to identify what your exposure might be.

Policies and Procedures

An information security policy is the documentation of enterprise-wide 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 security 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 security policy must be part of the organization's asset management program and must be enterprise-wide.

There are as many formats, styles, and types 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 on what and how a policy is to look and who should approve the document. The key point here is that every organization needs an information security policy. According to a recent industry report on computer crime, 65% of respondents admitted that they did not have a written policy. The beginning of an information security program is the implementation of a policy. The program policy establishes the organization's attitude 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 will identify the key structural elements of policies and then review some typical policy contents. To assist you in the policy development process, an example of a recently implemented information security policy is included in Chapter 1, "Developing Policies."

Risk Management

Risk is the possibility of something adverse happening. The process of risk management is to identify risks, assess the likelihood of their occurring, and then take steps to reduce all risks to an acceptable level. All risk assessment processes use the same methodology. Determine the asset to be reviewed. Identify the threats, issues, or vulnerabilities. Assess the probability of the threat occurring, and the effect on the asset or the organization should the threat be realized (this is how a risk is determined). Then, identify controls that would bring the effect to an acceptable level.

The 2010 CRC Press book titled *Information Security Risk Analysis: Third Edition* discusses effective risk assessment methodologies. The book takes the reader through the theory of risk assessment:

1. Identify the asset
2. Identify the threats
3. Establish risk levels
4. Identify controls and safeguards

The book will help the reader understand qualitative risk analysis and then give examples of this process. To make certain that the reader gets a well-rounded exposure to risk analysis, the book presents eight different methods, finishing with the Facilitated Risk Analysis and Assessment Process (FRAAP). We will examine the FRAAP, and at the end of Chapter 4, a copy of a recent procedure on performing the FRAAP is included.

The primary function of information security risk management is the identification of appropriate controls. In every assessment of risk, there will be many areas for which the kind of controls that are appropriate will not be obvious. The goal of controls is not to have 100% 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 and productivity wins. This is not a contest, though. The goal of information security is to provide a safe and secure environment for management to meet its fiduciary duty.

When selecting controls, it is important to consider many factors, including the organization's information security policy. Legislation and regulations that govern your enterprise, along with safety, reliability, and quality requirements, must also be factored into the process. Remember that every control will affect performance requirements in some way. 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 costs 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 will need to 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 security professionals sometimes forget that the managers hired by our organizations have the responsibility to make decisions. The job of the security professional 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