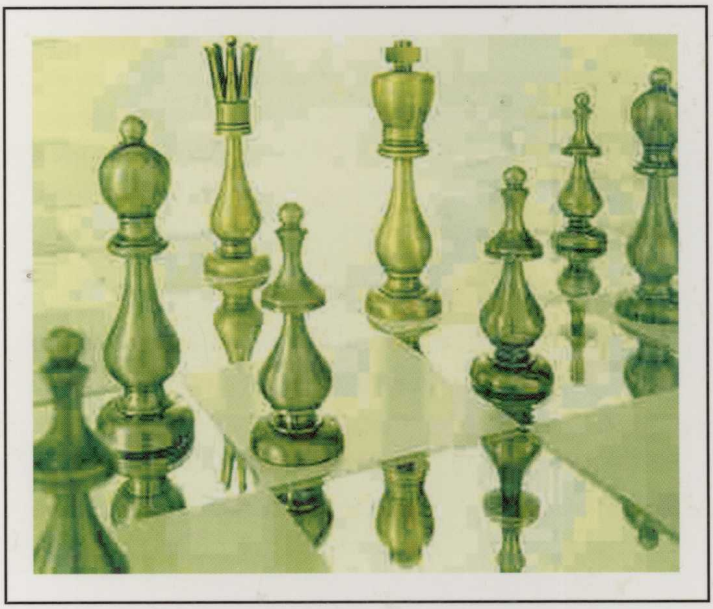
Information Security
FUNDAMENTALS



Thomas R. Peltier
Justin Peltier
John Blackley

AUERBACH

Information Security
FUNDAMENTALS

Thomas R. Peltier
Justin Peltier
John Blackley

AUERBACH PUBLICATIONS

A CRC Press Company
Boca Raton London New York Washington, D.C.

Library of Congress Cataloging-in-Publication Data

Peltier, Thomas R.
Information security fundamentals / Thomas R. Peltier, Justin Peltier, John Blackley.
p. cm.
Includes bibliographical references and index.
ISBN 0-8493-1957-9 (alk. paper)
1. Computer security. 2. Data protection. I. Peltier, Justin. II. Blackley, John A. III. Title.

QA76.9.A25P427 2004
005.8—dc22 2004051024

International Standard Book Number 0-8493-1957-9
Library of Congress Card Number 2004051024
Printed in the United States of America 1 2 3 4 5 6 7 8 9 0
Printed on acid-free paper

Acknowledgments

An organization that has moved to the forefront of creating usable information for the information security professional is the National Institute of Standards and Technology (NIST). The NIST 800 Series of Special Publications is a great source of information that many security professionals have provided over the years. Joan Hash and the other dedicated people who work at NIST have added greatly to the profession.

The Computer Security Institute (CSI) has been the leader in the information security industry since 1974 and continues to provide leadership and direction for its members and the industry as a whole. John O'Leary has been the constant in all the changes seen in this industry. The new CSI management team of Julie Hogan, Chris Keating, and Jennifer Stevens continues to provide the tools and classes that the security professional needs to be successful. The new team has blended well with the CSI seasoned veterans of Pam Salaway, Kimber Heald, Frederic Martin, Nancy Baer, and Joanna Kaufman.

No one has all of the answers to any question, so the really "smart" person cultivates good friends. Having been in the information security business for nearly 30 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 include Mike Corby, Terri Curran, Peter Stephenson, Merrill Lynch, Bob Cartwright, Pat Howard, Cheryl and Carl Jackson, Becky Herold, Ray Kaplan, Genny Burns, Anne Terwilliger, Patrice Rapalus, David Lynas, John Sherwood, Herve Schmidt, Antonio and Pietro Ruvolo, Wayne Sumida, Caroline Hamilton, Dan Erwin, Lisa Bryson, and William H. Murray.

My working buddies must also be acknowledged. My son Justin is the greatest asset any father — and more importantly, any information security team — could ever hope for. Over the past two years, we have logged

nearly 150,000 air miles together, and each day we learn something new from each other.

The other working buddy is John Blackley, a strange Scotsman who makes our life more fun and interesting. I have worked with John since 1985 and have marveled at how well he takes obtuse concepts and condenses them so that even management types 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 the industry wanted. Rich O'Hanley, not only the world's best editor and task master, but a good friend and source of knowledge. Thanks Rich!

And finally I extend a thank-you to my editor Andrea Demby. She takes the time to take the raw manuscript and put it into a logically flowing work. She sometimes has to ask me the same question more than once, but finally I get what needs to be done.

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 the 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 the 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 was 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 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.

Contents

Chapter 1

Overview

The purpose of information protection is to protect an organization's valuable resources, such as information, hardware, and software. Through the selection and application of appropriate safeguards, security helps the organization 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 roles and responsibilities, and common threats. We will also examine the need for management controls, policies and procedures, and risk analysis. Finally, we will 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 — 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 protect the assets of the enterprise and make informed business decisions. An effective information protection program will assist senior management in meeting 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 will be necessary to confirm that a significant risk exists. Implementing a timely risk analysis process can complete 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 will be necessary to publish an information protection policy statement and a 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 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 protection requires a comprehensive and integrated approach. To be as effective as possible, it will be necessary for information protection issues to be part of the system development life cycle. During the initial or analysis phase, information protection should receive as its deliverables 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 an 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 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 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 will be 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 agency's services provided to its constancy. We, as security professionals, must not lose sight of these goals and objectives.

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.

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. That activities are monitored
3. That by completing the sign-on process, the user agrees to the monitoring

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. In 1965 the idea of the "paperless office" was first introduced. The advent of third-generation computers brought about this concept. However, today the bulk of all of 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.

1.2.1 Employee Mind-Set toward Controls

Access to information and the environments that process them are dynamic. Technology and users, data and information in the systems, risks 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 "walk-about." 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

When conducting an initial "walk-about," the typical office environment will have 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 workstation. When conducting such a review, employee privacy issues must be remembered.

1.3 Roles and Responsibilities

As discussed, senior management has the ultimate responsibility for protecting the organization's information assets. One of these responsibilities

is the establishment of the function of Corporate Information Officer (CIO). The CIO directs the organization's day-to-day management of information assets. 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 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 fax.

The information protection 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 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. Quality Assurance 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 developing and conducting information protection awareness programs and in 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 protection policy.

An example of a typical job description for an information security professional is as follows:

1.3.1 *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