Realtime publishers
"Leading the Conversation"

The Definitive Guide™ To

Service-Oriented Systems Management

sponsored by

altiris®

Dan Sullivan

Copyright Statement

Chapter 9: Improving Security with Systems Management

SOM is an approach to systems management that addresses services across platforms and across an organization. The need for information security crosses all services and all parts of an organization as well. This chapter outlines the major areas of information security management as commonly understood and practiced. Security management standards have evolved over the past decades and the most recently, widely recognized version of these efforts are the ISO-17999:2005 and ISO 27001 standards. ISO-17999:2005 is a set of best practices for the management of a wide range of information security management practices; ISO 27001 addresses the use and management of information security systems.

> 🕮 These standards are formally defined by their respective ISO committees. Full details of the standard, as published by ISO, are available at http://www.standardsdirect.org/iso17799.htm. Chapter 3 of this guide also provides details about the ISO-17799 standard.

This chapter will not simply duplicate or describe what is in the ISO but place information security management within the broad context of SOM. The goal is to understand how the areas identified by security management best practices work in conjunction with other systems management practices to improve the security of an organization's IT infrastructure.

In particular, this chapter will address:

- Security management
- Threat and vulnerability assessment
- Managing countermeasures
- Incident response
- Auditing and monitoring

Let's begin with an overview of the ISO-17799 categories and then discuss how these categories map to the common security-related tasks found in SOM.

An Overview of ISO-17799

The most recent set of best practices for information security management define 12 areas that must be addressed:

- Risk assessment and treatment
- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development, and maintenance
- Information security incident management
- Business continuity management
- Compliance

The topic areas cover the full range of information security issues, from management to technologies and from regulatory compliance to physical security. The range of topics is indicative of the nature of information security management: it is both broad and deep. For those whose primary concern is systems management, security is just one facet of their responsibilities—but it is a fundamental one. Without adequate security, the other tasks addressed in systems management cannot be met. For example, without proper access controls in place, managing users and roles is of little value. The 12 areas of information security management are high-level topics but readily map to the day-to-day activities of systems managers.

Some of the security areas, such as risk management, business continuity management, and compliance must be addressed broadly across IT management and are not limited to security management. In addition, some of the more tactical operations of systems management, such as patch management, support the general area of information systems acquisition, development, and maintenance. Let's move forward with an examination of how to improve security through systems management practices and consider tasks performed within the framework of SOM.

Security Management

Security management is the practice of establishing, coordinating, and evaluating the range of security measures put in place within an organization. Table 9.1 shows the mapping from ISO-17799 categories to SOM tasks.

ISO-17799 Category	SOM Tasks
	Security Management
Risk assessment and treatment	X
Security policy	X
Organization of information security	X
Asset management	X
Human resources security	X
Physical and environmental security	
Communications and operations management	
Access control	
Information systems acquisition, development and maintenance	
Information security incident management	
Business continuity management	X
Compliance	X

Table 9.1: SOM tasks related to security management.

Security management does not include all the factors of the ISO-17799 categories, as we will explore with later SOM tasks.

Security Management and Risk Assessment

Risk assessment is primarily a function of security management. The goal of risk management is to identify risks to IT infrastructure, prioritize those risks, and implement mitigation strategies to bring the risks within acceptable levels. As that list of tasks implies, you cannot eliminate risks, but you can reduce their likelihood. Prioritizing also implies that you might not be able to adequately reduce the potential for all risks. Risk management often entails balancing needs against limited resources.

Thinking of risk management in terms of SOM allows you to view risks in terms of services provided and not just in terms of specific pieces of infrastructure. For example,

- Data storage management is more than just providing disk space; it includes backup and archive services and access control management. Security risks in this service include breaches of access controls and theft of backup media.
- Communication services such as email, instant messaging, and voice over IP (VoIP) depend on network infrastructure and so share common risks, such as Denial of Service (DoS) attacks.
- Application services, such as Web servers and J2EE and .Net application servers, can provide a wide range of services but are subject to risks such as host intrusions, information theft, and application tampering.

Mitigation strategies within SOM should address the full service, and this often entails detailed mitigation strategies based on the particulars of an implementation. For example, standby servers in a different location being used to mitigate the risk of a compromised email server shutting down communications services. If the primary email server were to fail, email records within the domain's DNS entries could be updated and email re-routed to the alternative server. Controlling risks is closely aligned with another security management function: policy development.

Security Management and Security Policy

Security policies are the foundation of an information security program. Policies are high-level descriptions of what is permitted and what is expected with regard to security. Organizations will typically have several security polices, covering:

- Acceptable use of IT infrastructure
- Access control
- Anti-malware policy
- Content-filtering policy
- Encryption policy
- Document and email retention
- Laptop and mobile device security
- Server and workstation security policy
- Wireless network access policy

Policies are generally written to clearly define the scope of the policy, the reason for the policy, and the details of the policy as well as provide the definition of technical terms if needed. An encryption policy, for example, might contain:

- A scope statement that defines the business units, employees, contractors, and business partners that need to adhere to the policy.
- An explanation for the need for the policy, such as protecting the confidentiality of customer information and proprietary company information.
- Policy details, such as a list of the categories of information that must be encrypted (for example, confidential, private, and sensitive information), the algorithms that may be used, and minimum key lengths.
- Definitions for terms such as digital signatures and public key cryptography.

Policies, such as encryption, can apply to multiple services or they may be specific to a particular service, such as email policies. In either case, policies should be aligned with the SOM model.

Organization of Information Security

The organization of information security addresses the need for governance and management of security services and functions. With regards to governance, executive management should have well-defined controls and measures in place to allow them to monitor and, if necessary, correct security operations. The governance model detailed in the Control Objectives for Information and Related Technologies (COBIT) framework provides a sound foundation for governance practices in general. The controls and measures described in COBIT are useful across the spectrum of SOM, not just security management.

> 🕮 For more information about COBIT, see the Information Systems Audit and Control Association (ISACA) Web site at https://www.isaca.org/.

Security Management and Asset Management

Like policy formation, asset management is one of the fundamental activities in security management. Asset management consists of two components: tracking hardware and software assets and classifying information.

Hardware and Software Asset Management

Assets cannot be protected if they are not managed, and they cannot be managed if they are not identified. This idea seems so obvious that it should not warrant mentioning, but tracking IT inventory is not a trivial task. Consider some of the factors that have to be accounted for when tracking inventory:

- Hardware has to be identified and inventory
- Software running on a device must be tracked
- Components within a device may be replaced or removed
- Hardware may be transferred between departments or individuals
- Some devices that access IT resources are not owned or controlled by the IT department or the organization

Hardware is one of the easiest aspects of physical inventory to manage. The location and the person or department responsible must be tracked. Movement within the organization needs to be monitored, and when the device is retired that must be noted as well. When devices are transferred or retired, operations may need to be performed to erase private or confidential data. This should be governed by information classification policy.

Software can be a challenge to track without tools. Applications are often installed, patched, and removed from users' devices as their needs change. Very few organizations can maintain a consistent set of software components on all devices across the organization even when they standardize as much as possible.

In both hardware and software management, a subunit of a device or application may be moved among devices. For example, disk drives may be moved between workstations and application server modules may be uninstalled from one server and moved to another.

To compound the challenges facing IT managers responsible for asset management, many managers now have to deal with semi-managed devices. These are often mobile devices that are owned by employees, contractors, and consultants but have some access to IT infrastructures. The most common are:

- Mobile email devices, such as Blackberrys
- PDAs
- Smartphones
- Data exchange devices, such as flash drives

The problem with these devices is that they can introduce malware or other threats to a network. Even if a complete inventory is maintained of all the software and hardware owned by an organization, security staff may still not have an accurate picture of the potential threats facing their infrastructure. Properly managing and controlling the use of semi-managed devices has emerged as a key challenge in security management.

Information Classification

Information classification is the process of labeling different types of information and establishing appropriate controls for each type. Commercial and military institutions use different classification schemes; the most common categories in commercial classifications are:

- Public
- Sensitive
- Private
- Confidential

By categorizing information, appropriate controls can be placed on information without having to apply a most-restrictive policy that protects all information as if it were equally important.

Public Information

The public classification is reserved for information that, if disclosed publicly, would not have an adverse affect on the organization. For example, information provided in press releases would not contain information that requires any unusual level of protection.

Sensitive Information

Sensitive information should not be publicly disclosed, but if it were, the disclosure would not have serious adverse affects on the organization. Information about project plans, work schedules, orders, inventory levels, and other operational data by itself could not be used against an organization. It is conceivable that a competitor could piece together competitive intelligence about a firm by examining large amounts of such operational information.

Private Information

Private information is about customers, clients, patients, employees, and other persons who have dealings with an organization. The disclosure of private information could adversely affect those individuals; organizations may be subject to fines or other legal proceedings for violating regulations regarding the protection of private information. Examples of private information include:

- Employee records
- Protected healthcare information
- Financial records
- Social Security numbers, driver's license numbers, and other identifying information

Depending on the industry, organizations could be subject to a range of regulations governing the protection of private information. The health care and financial services industries are subject to comprehensive regulations in the United States; the European Union (EU) has established broad privacy protections that apply to all businesses.

Confidential Information

Confidential information requires significant controls because the disclosure of this information could have a significant impact on an organization. Some of the typical types of confidential information include:

- Trade secrets
- Negotiation details
- Strategic plans
- Intellectual property, such as algorithms and product designs

Like private information, confidential information should be protected with well-defined access controls and clear lines of responsibility.

Although many of the same measures may be used to protect confidential and private information, they are fundamentally different and should not be linked with regards to security policies and procedures. Private information, for example, may be subject to specific audit requirements that are not relevant to protecting confidential information. Similarly, some confidential information may be protected with stronger, and more costly, measures than required for private information. These two categories should always be managed as separate entities.

Security Management and Human Resources Management

Within the realm of human resource management, the key areas from a security perspective are:

- Screening employees, contractors, and consultants and having procedures in place to monitor their activities relative to information security.
- Providing training to employees, contractors, and consultants about information security practices. Training should include basics about the technical issues of information security, such as the different types of malware threats and how to counter them as well as training on social engineering tactics, such as those used by phishers.
- Establishing procedures and educating employees and others about appropriate incident response measures.

Another area that IT managers must address is business continuity.

Security Management and Business Continuity Management

Information security is often described in terms of three characteristics: confidentiality, integrity, and availability. It is the last characteristic that is the subject of business continuity. From a SOM perspective, business continuity is a broad topic that includes information security but is not limited to it.

Security professionals should contribute to business continuity plans for a number of reasons:

- Systems availability is subject to threats such as DoS attacks; business continuity planning should take into account countermeasure to mitigate the impact of a such an attack.
- Business continuity often includes plans for redeploying operations to an alternative site; electronic and physical security measures must be in place at these sites as well as at the primary site.
- During a business disruption, data may be moved between servers or entire facilities. The data must be protected in transit.

Another area in which security professionals are required is compliance with government regulations.

Security Management and Compliance

Adequate protection of private and confidential information plays a role in many government regulations. Some of the most well known include:

- Sarbanes-Oxley Act—publicly traded companies
- Gramm-Leach-Bliley Act—financial service firms
- Health Insurance Portability and Accountability Act (HIPAA)—health care firms
- BASEL II—financial services
- 21 CFR Part 11—pharmaceutical companies
- Federal Information Security Management Act (FISMA)—federal government
- California State Bill (SB) 1386—business with customers in California
- EU Directives on Privacy—companies doing business in the EU
- Personal Information Protection and Electronic Documents Act (PIPEDA)—companies doing business in Canada

Responsibility for complying with the array of regulations in existence is likely spread across a number of departments. Fortunately for IT practitioners, sound security management practices often contribute significantly to meeting compliance requirements. With proper controls, such as information classification, access controls, network and host defenses, and proper monitoring and auditing, IT departments can meet the requirements of many regulations by continuing their security best practices.

Security management spans the full range of information protection activities. Other areas of information security management are more focused, such as threat assessment.

Threat and Vulnerability Assessment

As part of SOM, one of the key security tasks is to understand the threats to IT infrastructure and to information housed within that infrastructure as well as systemic vulnerabilities that may be exploited. Unfortunately, there is no shortage of threats, including:

- Malware
- System attacks
- Information theft
- Resource theft

These threats are not necessarily distinct. Malware may be used to steal information or resources and system attacks may be combined with information theft. Although each of these will be discussed separately, it is useful to keep in mind that these threats may be combined when used by attackers.

Within the ISO-17799 framework, a number of areas address threat and vulnerability assessment (see Table 9.2).

ISO-17799 Category	SOM Tasks
	Security Management
Risk assessment and treatment	X
Security policy	X
Organization of information security	
Asset management	X
Human resources security	
Physical and environmental security	X
Communications and operations management	X
Access control	
Information systems acquisition, development and maintenance	
Information security incident management	X
Business continuity management	
Compliance	

Table 9.2: Threat assessment categories of ISO-17799.

Malware Threat

The malware threat has evolved from disruptive and annoying viruses written to demonstrate an attacker's ability to circumvent normal OS operations to financially motivated, sophisticated blend threats designed to steal information and compromise hosts. There are several distinct types of malware:

- Viruses and worms
- Keyloggers and video frame grabbers
- Trojan horses
- Botnets
- Rootkits

These different types of malware are used for carrying out different aspects of an attack and may be blended to create a more serious threat than posed by any single type of malware on its own.

Viruses and Worms

Viruses and worms are the most well-known forms of malware. Viruses consist of a payload, the part of the virus that carries out its malicious activity, and propagation code, which allows the program to spread by attaching itself to other programs. More sophisticated forms of viruses include encryption modules used to mask the viruses from antivirus detection. In practice, encryption is not protection enough because signature-based detection methods can still be used to identify encryption modules even when the payload is encrypted.

Polymorphic viruses change the structure of the program without changing its functions. These kinds of viruses include a module known as the polymorphic engine that introduces operations that have no effect on the functioning of the program, such as an instruction to add 0 to a number or to concatenate two strings into a variable that is never used in the control or output of the program.

Worms are similar to viruses but propagate on their own by exploiting vulnerabilities in applications and network systems. The SQL Slammer worm, for example, spread by using a vulnerability in SQL Server communications that allowed it to find other SQL Server instances by searching random IP addresses. The worm spread rapidly and within minutes had slowed traffic on large segments of the Internet when it struck in 2003.

The SQL Slammer incident is one of those cases that did not have to happen. Microsoft had patched the vulnerability exploited by SQL Slammer months before the worm struck. Part of the problem was that database administrators had not patched SQL Server instances, and part of the problem was due to users not knowing they were running a desktop version of SQL Server that had been embedded in some applications. This is one of the reasons asset management is so important to information security—you must know what software you are running and how it is patched.

Keyloggers and Video Frame Grabbers

Another type of malware that is a growing concern is malware designed to electronically eavesdrop and steal information. Keyloggers are programs or hardware devices that intercept keystrokes from a keyboard and log them to a file. The file is then sent to an attacker, in the case of software-based keyloggers, or retrieved by an attacker, in the case of a hardware keyloggers. It is easy to imagine a scenario in which a keylogger could be used to collect useful information for a thief. Consider the following sequence of events in which a user

- Opens a browser and enters a URL for a popular online auction
- Searches for an electronic devices and makes a purchase
- Opens her payment service account by entering a username and password
- Navigates to her bank's Web site
- Logs into her accounts using her bank username and password
- Transfers funds from her savings account to checking account
- Navigates to several news sites

Logging every keystroke can lead to a great deal of useless information from the attacker's point of view; however, by scanning for text patterns found in known sites, such as the names of online auctions, banks, and retailers, the attackers can quickly identify parts of the log files that will most likely have usernames, passwords, and account numbers.

For example, the attacker may scan the file looking for text such as "www.mybankwebsite.com" or "www.someonlineauction.com" and then search for a single term 4 to 12 characters long, such as "JaneDoeNYC" followed by another word 6 to 15 characters long, such as "P2sSw5rd!" to retrieve usernames and passwords. Similar scanning techniques can be used to find Social Security numbers, driver's license numbers, bank account numbers, and so on. Of course, there is more useful information than just the text that passes through the keyboard.

A Picture, A Thousand Words, and Video Frame Grabbers

One way to avoid having passwords captured by keyloggers is to display a virtual keyboard on the screen and have users mouse over and click each character in a password. This can circumvent a keylogger, but as you should expect, attackers have devised ways to continue to steal information in spite of this countermeasure.

A video frame grabber makes copies of the contents of video memory, and so can capture a wide array of information such as:

- Virtual keyboards used to enter passwords
- Email messages displayed on the screen
- Spreadsheets and documents displayed on the screen
- Instant message discussions
- Account information displayed by database applications

Both keyloggers and video frame grabbers are especially threatening when unmanaged devices are used to access information. Unmanaged devices include home computers used by customers to access their account information as well as public access computers, such as in hotels, which may be infected with malware, including keyloggers and video frame grabbers.

Trojan Horses

Trojan horses are programs that appear to serve one purpose but actually contain malware. Trojan horses may be found in:

- Browser add-ons
- Utility programs, such as clock synchronizers
- File-sharing utilities
- Programs and files sent through email and instant messaging

Trojan horses are a mechanism for distributing malicious code. They are often used with multiple forms of malware, known as blended threats, which can include keyloggers, communications programs, file transfer programs, and command and control programs that allow remote control or remote execution of code. The ability to execute programs on compromised hosts gives attackers the means to create networks of compromised computers, sometimes called "zombies" but more commonly known as bots.

Remote Control and Botnets

A bot is a program that may be controlled by an attacker. Bots have been used to distribute spam, phishing attacks, and click fraud as well as launch distributed DoS (DDoS) attacks. A compromised host typically listens for commands on an Internet Relay Chat (IRC) channel or instant messaging service. Botnet controllers can send commands to execute scripts, send spam, or download updates to the botnet software. Identifying and eradicating botnets, Trojan horses, keyloggers, video frame grabbers, viruses, worms, and other malware is more difficult when a device is also compromised because of the presence of a rootkit.

Hiding Malware with Rootkits

A rootkit is a program that masks the presence of other programs and files and makes the activities of those programs more difficult to detect. Rootkits may modify OS or application code so that it

- Intercepts low-level system calls for file information
- Prevents the display of information about processes executing
- Loads rootkit code instead of OS code
- Substitutes legitimate application code with compromised versions of code

Because rootkits compromise the OS, there is not necessarily a trusted computing base. Any information returned by the OS kernel (for example, what processes are executing? What is the size of a particular binary file?) may not be accurate because the code that executes the requested service may be compromised.

Some tools have been developed to detect patterns indicative of the presence of a rootkit. For example, a rootkit detector might compare file system information returned by the OS with information returned by low-level analysis of the disk system; any discrepancies could indicate the presence of a rootkit. Another technique is to boot a device from a trusted source, such as an OS CD and scan for rootkits.

> 🕮 Rootkits may become even more difficult to detect, especially if vulnerabilities in BIOS are exploited. See Robert Lemos' "Researchers: Rootkits Headed for BIOS" at http://www.securityfocus.com/news/11372 for more information.

The best response to the threat of malware attacks is to use a defense-in-depth strategy. This approach recognizes that no one countermeasure or policy will fully mitigate the risks of an attack. It also recognizes that anti-malware programs and related systems are themselves complex programs with their own limits and vulnerabilities. A defense-in-depth approach to malware protection will include:

- Antivirus and personal firewalls on client devices
- Network-based content filtering to block malicious content before it reaches the client
- Intrusion prevention monitoring to detect unusual network activity, such as large volumes of network traffic outside of normal patterns
- Host-based intrusion prevention that detects changes to OS files
- Regular monitoring of logs and audits of security measures
- End user training, especially on the threat of social engineering techniques
- Comprehensive set of policies that define an organization's strategy for managing the risks of malware attacks

Unfortunately, malware is not the only kind of information security threat.

System Attacks

System attacks are those targeted to particular applications or hosts. The purpose of such attacks may be to disrupt services or steal information. As the economic motives behind attacks have grown to dominate the reasons for serious attacks, more attacks targeted to specific applications and hosts are likely to emerge. Attacks may include:

- DoS attacks attempting to disrupt the operations of an organization
- Database breaches in attempt to steal private but profitable customer information
- Applications-specific attacks, such as attacks on enterprise management systems that contain sensitive and confidential information about an organizations operations

Systems attacks are often not ends in themselves but rather a means to an end: information and resource theft.

Information and Resource Theft

An underground economy of stolen information and compromised computers is supporting attackers who can gain access to customer information, such as names, addresses, bank account numbers, Social Security numbers, and personally identifying information. Although phishing is one way to con information from a number of victims, cracking databases can yield large volumes of data in a single theft.

As noted earlier in the discussion of botnets, computers themselves are also resources for attackers. For example, security researchers reported a botnet with nearly one million compromised devices in the fall of 2006. The purpose of the botnet is not known at the this time but one likely use is a massive phishing campaign.

> 🕮 For more information about the unusually large botnet discovered in the fall of 2006, see Andrew Charlseworth's "Million PC Botnet Threatens Consumers" at http://www.vnunet.com/vnunet/news/2167474/million-pc-botnet-threatens.

There are a range of threats and vulnerabilities that face systems administrators and information security professionals. From malware and system attacks to the growing threat of information and resource theft, there is a an increasing need for effective and coordinated countermeasures.

Managing Countermeasures

The defense-in-depth approach is considered a security best practice but it comes at a price: multiple security solutions must be managed. In addition, to gain the most from these point solutions, the information from them should be coordinated. As Table 9.3 shows, the tasks of managing countermeasures cross several ISO-17799 categories.

ISO-17799 Category	**SOM Tasks**
	Security Management
Risk assessment and treatment	
Security policy	
Organization of information security	
Asset management	
Human resources security	
Physical and environmental security	
Communications and operations management	X
Access control	X
Information systems acquisition, development and maintenance	X
Information security incident management	X
Business continuity management	
Compliance	

Table 9.3: Managing countermeasures falls into several ISO-17799 categories.

The key activities within this area include:

- Ensuring both network and host-based defenses are kept up to date with signature files and patches
- Coordinating information from multiple sources, such as perimeter defenses and host-base defenses
- Ensuring procedures dictated by security policies are in place and enforced across countermeasures
- Configuring new devices and software properly during the implementation phase of a project
- Putting in place mechanisms to support incident response

The last example is one in which systems managers may be asked to play a major role because incident response can require a rapidly executed and well-coordinated plan to contain the impact of a security breach.

Incident Response

An incident response plan is like an insurance policy: no one wants to have to use it, but everyone is glad to have one when it is needed. A security incident can take on many forms, including:

- A virus infection of multiple devices or critical servers
- The discovery of a significant number of Trojan horse programs
- Infections with keyloggers
- A DoS attack on a network device
- An attempt to break into a server
- An attempt to steal information for a database
- The discovery of a botnet within an organization's network
- Loss of a laptop or other mobile device containing sensitive, private, or confidential information

Incident response planning has two dimensions—one addresses procedures and the other addresses the human resources element of the problem.

Incident Response Procedures

When an event occurs, the logical challenge is to determine how to respond. The solution should be governed by an incident response policy that includes:

- Guidelines on containing the potential damage of the incident
- Persons to notify, including both IT and business executives and managers
- Procedures for contacting information security personnel with knowledge of forensic procedures who can help gather evidence
- Procedures for securing compromised devices and preserving evidence

Incident handling and its relation to ISO-17799 is shown in Table 9.4.

ISO-17799 Category	**SOM Tasks**
	Security Management
Risk assessment and treatment	
Security policy	
Organization of information security	
Asset management	
Human resources security	X
Physical and environmental security	
Communications and operations management	
Access control	
Information systems acquisition, development and maintenance	
Information security incident management	X
Business continuity management	
Compliance	

Table 9.4: In addition to the incident management category, there is a human resources element to incident response.

Human Resources Issues in Incident Response

There are a few issues related to human resources that should be kept in mind when designing an incident response plan:

- The need for incident response training
- The need for separation of duties
- The benefits of post-incident analysis

Training and Incident Response

Users, technical staff, and management should all be trained in incident response procedures. For many, it may be as simple as directing them to call the service desk when something suspicious appears. This suspicious activity could be something as clear as a warning from a local antivirus program indicating malware has been detected to something less obvious, such as sluggish performance from a device for no apparent reason (this could indicate a spyware or Trojan horse infection that is using the device for other purposes).

Technical staff, especially front-line service desk support and systems administrators should be trained on how to respond according to the severity of an incident. For example, minor incidents, such as a virus infection on a single device, might call for a basic response using a procedure defined for relatively predictable incidents. For major incidents, such as a DoS attack that is blocking access to critical servers, front-line technical staff should know how to enlist additional help to deal with the problem.

Executives and managers should understand the implications of various types of attacks with regard to the impact on business operations as well as legal responsibilities with regards to reporting the incident and complying with government regulations.

Separation of Duties

There is something strange about the fact that it is more prudent to trust two or more individuals than it is to trust one, but that is the idea behind separation of duties. This is especially important when responding to security incidents. One of the activities of incident response is to collect and preserve evidence. It is not unheard of for someone working for an organization to be involved with crimes against that organization. If an employee or contractor perpetrated an incident, that person may be involved with the incident response.

For example, a database administrator is someone with the keys to the proverbial kingdom when it comes to large volumes of business information. If someone were stealing customer credit card data from a database and a security monitor on the network detected unusual activity on a database server, the first person to call would be the database administrator. The potential problem is clear; the solution is to have at least two knowledgeable individuals respond to an incident.

Response Evaluation

Security breaches are disruptive and potentially costly, but they are also opportunities to improve security measures. A post-incident evaluation can provide valuable information about:

- How attackers breached security mechanisms
- Which security mechanisms worked and which did not
- If attack techniques were not anticipated
- Whether monitoring and logging were adequate to diagnose the incident
- Vulnerabilities in applications, OSs, or network devices
- Vulnerabilities in policies and procedures

The goal of the post-incident evaluation is to improve the quality of security, not simply to place blame. Managing information security is difficult and a breach does not necessarily imply negligence or disregard for policies and procedures. Another aspect of information security management that can help improve security quality is regular auditing.

Security Auditing and Monitoring

IT auditing became much more common with the advent of the Sarbanes-Oxley Act. The goal of this and related regulations is to preserve the integrity of business information. To meet that objective, you must have procedures and systems in place that protect information and you must periodically review those systems and procedures to ensure they are functioning adequately. Thus, regular IT audits are much more thorough than may have been conducted in the past. As Table 9.5 shows, auditing spans a number or areas within the ISO-17799 framework.

ISO-17799 Category	**SOM Tasks**
	Security Management
Risk assessment and treatment	
Security policy	X
Organization of information security	
Asset management	
Human resources security	X
Physical and environmental security	
Communications and operations management	
Access control	X
Information systems acquisition, development and maintenance	
Information security incident management	X
Business continuity management	
Compliance	X

Table 9.5: Auditing spans a number of security areas; it is not as limited as often understood.

Audit Controls

Auditing begins with policies. Policies may be defined by an organization on it own or as part of compliance with regulations. Regardless of the motivation for policies, the role of auditing is to ensure that they are appropriate for the objective and sufficiently implemented. Some of the most important areas that should be verified in audits include:

- Information classification
- Access controls appropriate for information classifications
- Adequate perimeter and network defenses
- Adequate host defenses
- Adequate review of content, both entering and leaving the network
- Sufficient training on security measures
- Backup and recovery procedures
- Appropriate security management practices, such as separation of duties and rotation of duties

Auditing is an in-depth review of security policies and procedures. Auditing may be regular but is still infrequent; day-to-day monitoring is also required.

Security Monitoring

Monitoring can be time consuming unless tools are used to help sift through the volumes of log data that can be generated in even a moderate-sized network. The difficulties arise from the range of events that should be monitored, including system events, application events, and user events. Some of the most common are:

- System performance metrics, such as number of processes, CPU utilization, storage utilization
- Login attempts and failures
- Applications executed and functions executed within enterprise applications
- Changes to OS configurations
- Errors generated by applications
- Files read, modified, and deleted
- Attempts to access unauthorized resources

In isolation, any one of these events may not be indicative of a serious breach. However, in conjunction with other events, these may warrant closer examination and may indicate a breach. One of the greatest challenges in information security today is integrating data from the variety of security mechanisms already in place. Firewalls, routers, intrusion prevention devices, access control systems, OSs, anti-malware solutions, and content-filtering applications can all generate large quantities of data, some of which can be quite useful if it is identified and integrated with other information in a timely manner.

Summary

Security management is one of the most multi-faceted areas of systems management. It ranges from the broad issues of managing security information down to the detailed practice of threat and vulnerability assessment. In addition to day-to-day activities such as monitoring systems, applications, and users, systems administrators and security professionals must manage an array of security mechanisms deployed in such a way as to provide multiple layers of defense.

Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit http://nexus.realtimepublishers.com.