CHAPTER 1

Information Security Essentials for IT Managers: Protecting Mission-Critical Systems

Albert Caballero
Terremark Worldwide, Inc.

Information security involves the protection of organizational assets from the disruption of business operations, modification of sensitive data, or disclosure of proprietary information. The protection of this data is usually described as maintaining the confidentiality, integrity, and availability (CIA) of the organization's assets, operations, and information.

1. Information Security Essentials for IT Managers, Overview

Information security management as a field is ever increasing in demand and responsibility because most organizations spend increasingly larger percentages of their IT budgets in attempting to manage risk and mitigate intrusions, not to mention the trend in many enterprises of moving all IT operations to an Internet-connected infrastructure, known as enterprise cloud computing [1]. For information security managers, it is crucial to maintain a clear perspective of all the areas of business that require protection. Through collaboration with all business units, security managers must work security into the processes of all aspects of the organization, from employee training to research and development. Security is not an IT problem; it is a business problem.

> Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction [2].

Scope of Information Security Management

Information security is a business problem in the sense that the entire organization must frame and solve security problems based on its own strategic drivers, not solely on technical controls aimed to mitigate one type of attack. As identified throughout this chapter, security goes beyond technical controls and encompasses people, technology, policy, and operations in a way that few other business objectives do. The evolution of a risk-based paradigm, as opposed to a technical solution paradigm for security, has made it clear that a secure organization does not result from securing technical infrastructure alone. Furthermore, securing the organization's technical infrastructure cannot provide the appropriate protection for these assets, nor will it protect many other information assets that are in no way dependent on technology for their existence or protection. Thus, the organization would be lulled into a false sense of security if it relied on protecting its technical infrastructure alone [3].

CISSP 10 Domains of Information Security

In the information security industry there have been several initiatives to attempt to define security management and how and when to apply it. The leader in certifying information security professionals is the Internet Security Consortium, with its CISSP (see sidebar, "CISSP 10 Domains: Common Body of Knowledge") certification [4]. In defining required skills for information security managers, the ISC has arrived at an agreement on 10 domains of information security that is known as the *Common Body of Knowledge* (CBK). Every security manager must understand and be well versed in all areas of the CBK [5].

In addition to individual certification there must be guidelines to turn these skills into actionable items that can be measured and verified according to some international standard or framework. The most widely used standard for maintaining and improving information security is ISO/IEC 17799:2005. ISO 17799 (see Figure 1.1) establishes guidelines and principles for initiating, implementing, maintaining, and improving information security management in an organization [6].

A new and popular framework to use in conjunction with the CISSP CBK and the ISO 17799 guidelines is ISMM. ISMM is a framework (see Figure 1.2) that describes a five-level evolutionary path of increasingly organized and systematically more mature security layers. It is proposed for the maturity assessment of information security management and the evaluation of the level of security awareness and practice at any organization, whether public or private. Furthermore, it helps us better understand where, and to what extent, the three main processes of security (prevention, detection, and recovery) are implemented and integrated.

ISMM helps us better understand the application of information security controls outlined in ISO 17799. Figure 1.3 shows a content matrix that defines the scope of applicability between various security controls mentioned in ISO 17799's 10 domains and the corresponding scope of applicability on the ISMM Framework [7].

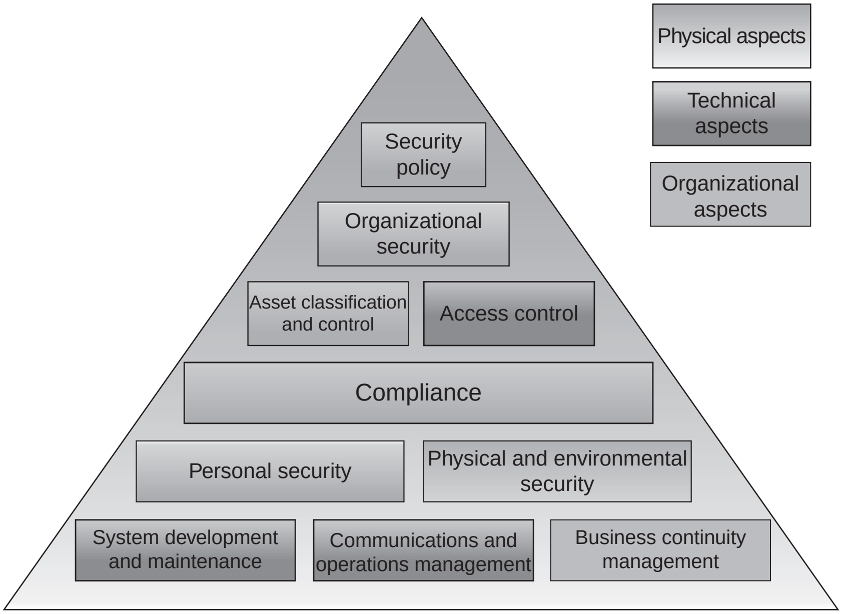

Physical aspects
Technical aspects
Organizational aspects
Security policy
Organizational security
Asset classification and control
Access control
Compliance
Personal security
Physical and environmental security
System development and maintenance
Communications and operations management
Business continuity management

Figure 1.1: ISO 17799:2005 security model [8].

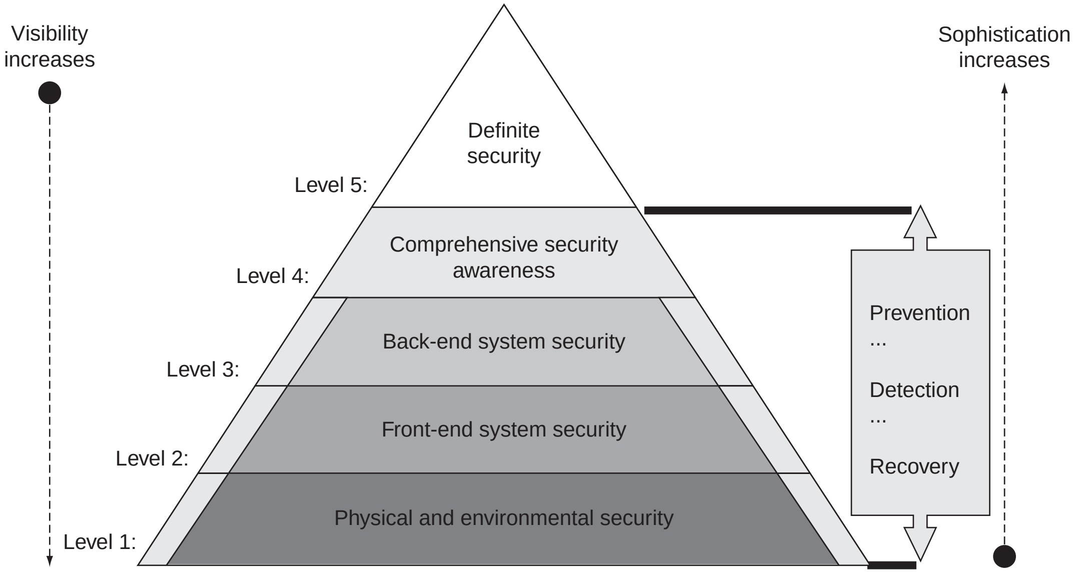


Figure 1.2: ISMM framework [9].

ISO 17799			ISMM (scope of applicability)				
Domain number	Domain name	Domain subname	Layer 1	Layer 2	Layer 3	Layer 4	Layer 5
1	Security policy	N/A	✓	✓	✓	✓	
2	Organizational security	Information security infrastructure	✓	✓	✓		
3	Asset classification and control	Security of third-party access	✓	✓	✓	✓	
		Outsourcing	✓	✓	✓	✓	
		Accountability for assets		✓	✓		
		Information classification	✓	✓	✓		
4	Personnel security	Security in job definition and resourcing	✓				
		User training	✓	✓	✓	✓	
		Responding to security incidents/malfunctions	✓	✓	✓	✓	
5	Physical and environmental security	Secure areas	✓				
		Equipment security	✓				
		General controls	✓				
6	Communications and operations management	Operational procedures and responsibilities		✓	✓		
		System planning and acceptance		✓	✓		
		Protection against malicious software		✓			
		Housekeeping		✓	✓		
		Network management			✓		
		Media handling and security	✓				
		Exchange of information and software		✓			
7	Access control	Business requirement for access control	✓	✓	✓		
		User access management		✓			
		User responsibilities		✓			
		Network access control			✓		
		Operating system access control			✓		
		Application access control		✓			
		Monitoring system access and use		✓	✓		
		Mobile computing and teleworking		✓	✓		
8	System development and maintenance	Security requirement of systems		✓	✓		
		Security in application systems		✓			
		Cryptographic controls		✓	✓		
		Security of system files			✓		
		Security in development and support processes		✓	✓		
9	Business continuity management	N/A				✓	✓
10	Compliance	Compliance with legal requirements				✓	
		Review of security policy and compliance				✓	
		System audit considerations				✓	

Figure 1.3: A content matrix for ISO 17799 and its scope of applicability.

CISSP 10 Domains: Common Body of Knowledge

- *Access control.* Methods used to enable administrators and managers to define what objects a subject can access through authentication and authorization, providing each subject a list of capabilities it can perform on each object. Important areas include access control security models, identification and authentication technologies, access control administration, and single sign-on technologies.
- *Telecommunications and network security.* Examination of internal, external, public, and private network communication systems, including devices, protocols, and remote access.
- *Information security and risk management.* Including physical, technical, and administrative controls surrounding organizational assets to determine the level of protection and budget warranted by highest to lowest risk. The goal is to reduce potential threats and money loss.
- *Application security.* Application security involves the controls placed within the application programs and operating systems to support the security policy of the organization and measure its effectiveness. Topics include threats, applications development, availability issues, security design and vulnerabilities, and application/data access control.
- *Cryptography.* The use of various methods and techniques such as symmetric and asymmetric encryption to achieve desired levels of confidentiality and integrity. Important areas include encryption protocols and applications and Public Key Infrastructures.
- *Security architecture and design.* This area covers the concepts, principles, and standards used to design and implement secure applications, operating systems, and all platforms based on international evaluation criteria such as Trusted Computer Security Evaluation Criteria (TCSEC) and Common Criteria.
- *Operations security*. Controls over personnel, hardware systems, and auditing and monitoring techniques such as maintenance of AV, training, auditing, and resource protection; preventive, detective, corrective, and recovery controls; and security and fault-tolerance technologies.
- *Business continuity and disaster recovery planning.* The main purpose of this area is to preserve business operations when faced with disruptions or disasters. Important aspects are to identify resource values; perform a business impact analysis; and produce business unit priorities, contingency plans, and crisis management.
- *Legal, regulatory, compliance, and investigations.* Computer crime, government laws and regulations, and geographic locations will determine the types of actions that constitute wrongdoing, what is suitable evidence, and what types of licensing and privacy laws your organization must abide by.
- *Physical (environmental) security.* Concerns itself with threats, risks, and countermeasures to protect facilities, hardware, data, media, and personnel. Main topics include restricted areas, authorization models, intrusion detection, fire detection, and security guards.

What Is a Threat?

Threats to information systems come in many flavors, some with malicious intent, others with supernatural powers or unexpected surprises. Threats can be deliberate acts of espionage, information extortion, or sabotage, as in many targeted attacks between foreign nations; however, more often than not it happens that the biggest threats can be forces of nature (hurricane, flood) or acts of human error or failure. It is easy to become consumed in attempting to anticipate and mitigate every threat, but this is simply not possible. Threat agents are threats only when they are provided the opportunity to take advantage of a vulnerability, and ultimately there is no guarantee that the vulnerability will be exploited. Therefore, determining which threats are important can only be done in the context of your organization. The process by which a threat can actually cause damage to your information assets is as follows: A threat agent *gives rise to* a threat that *exploits* a vulnerability and can *lead to* a security risk that *can damage* your assets and *cause* an exposure. This can be *countermeasured by* a safeguard that *directly affects* the threat agent. Figure 1.4 shows the building blocks of the threat process.

Common Attacks

Threats are exploited with a variety of attacks, some technical, others not so much. Organizations that focus on the technical attacks and neglect items such as policies and procedures or employee training and awareness are setting up information security for

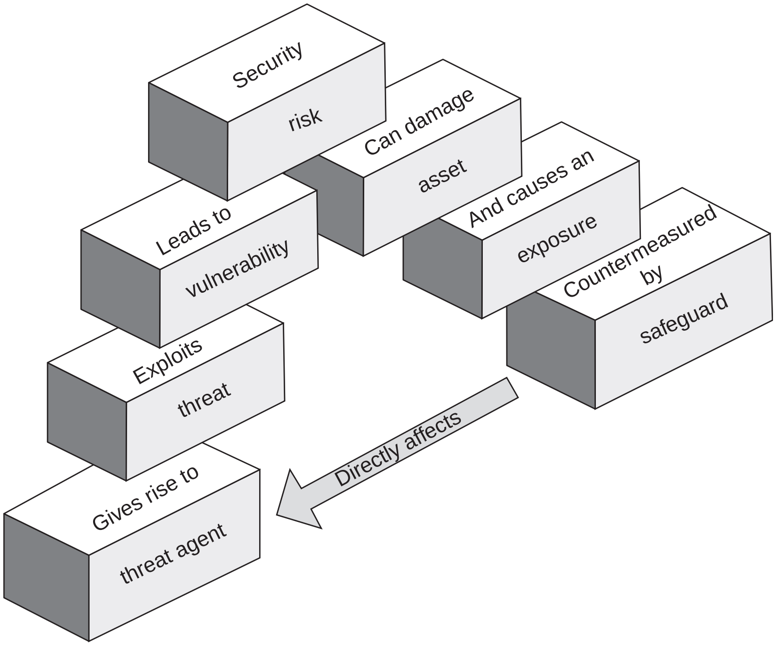


Figure 1.4: The threat process.

failure. The mantra that the IT department or even the security department, by themselves, can secure an organization is as antiquated as black-and-white television. Most threats today are a mixed blend of automated information gathering, social engineering, and combined exploits, giving the perpetrator endless vectors through which to gain access. Examples of attacks vary from a highly technical remote exploit over the Internet, social-engineering an administrative assistant to reset his password, or simply walking right through an unprotected door in the back of your building. All scenarios have the potential to be equally devastating to the integrity of the organization. Some of the most common attacks are briefly described in the sidebar titled "Common Attacks." [10]

Common Attacks

- *Malicious code (malware).* Malware is a broad category; however, it is typically software designed to infiltrate or damage a computer system without the owner's informed consent. As shown in Figure 1.5, the most commonly identifiable types of malware are viruses, worms, backdoors, and Trojans. Particularly difficult to identify are root kits, which alter the kernel of the operating system.
- *Social engineering.* The art of manipulating people into performing actions or divulging confidential information. Similar to a confidence trick or simple fraud, the term typically applies to trickery to gain information or computer system access; in most cases, the attacker never comes face to face with the victim.

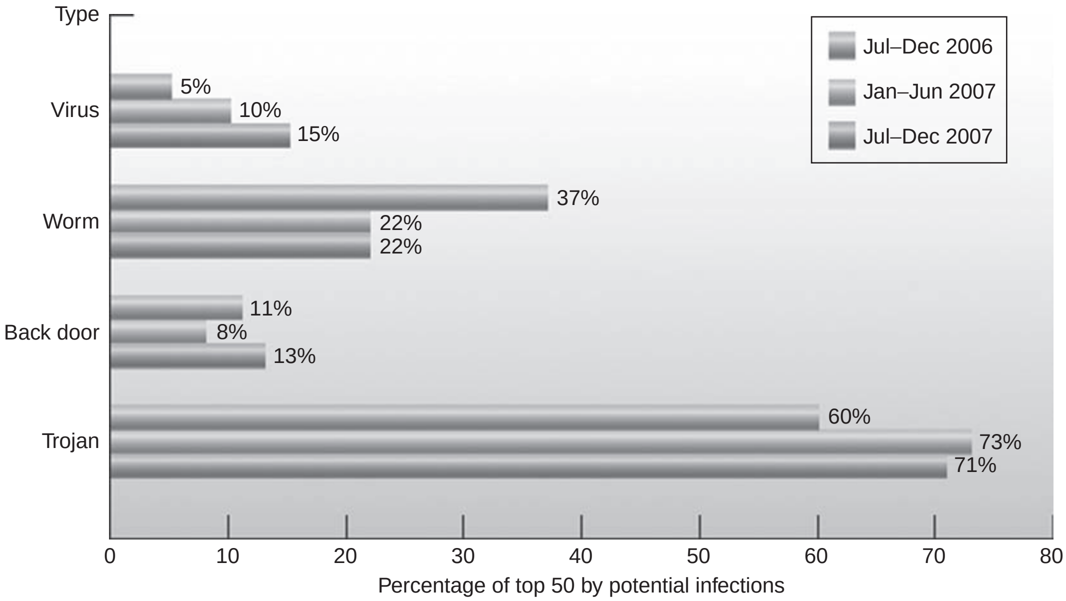


Figure 1.5: Infections by malicious code type, CSI/FBI report, 2008 [11].

Continues on next page

- *Industrial espionage.* Industrial espionage describes activities such as theft of trade secrets, bribery, blackmail, and technological surveillance as well as spying on commercial organizations and sometimes governments.
- *Spam, phishing, and hoaxes.* Spamming and phishing (see Figure 1.6), although different, often go hand in hand. Spamming is the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages, many of which contain hoaxes or other undesirable contents such as links to phishing sites. Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords, and credit-card details by masquerading as a trustworthy entity in an electronic communication.

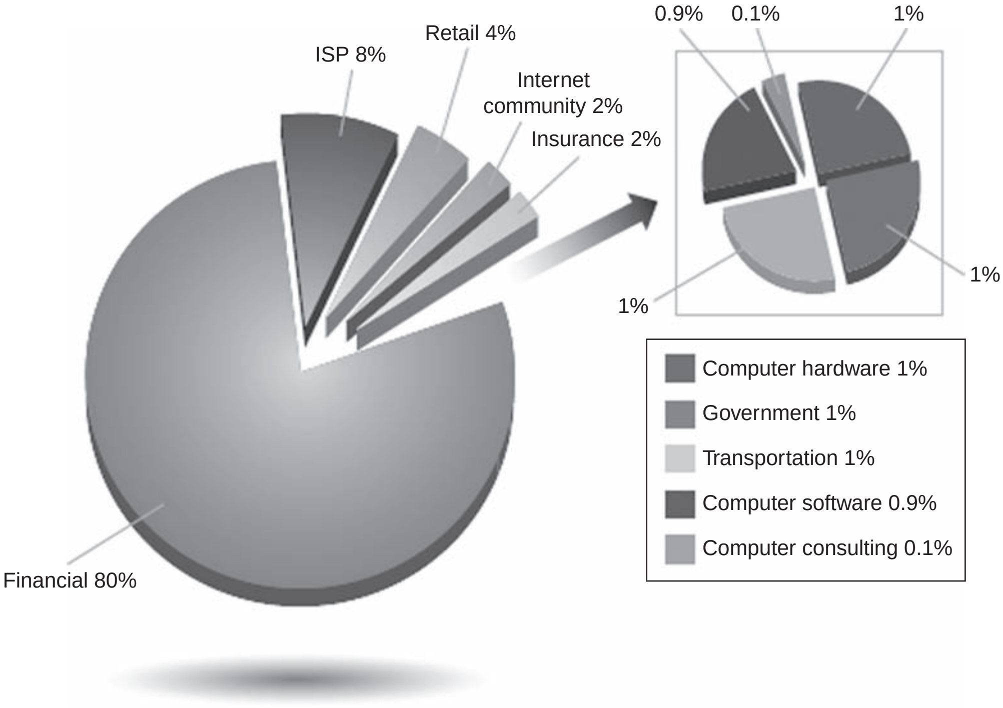


Figure 1.6: Unique brands phished by industry sectors, CSI/FBI report, 2008 [12].

- *Denial of service (DoS) and distributed denial of service (DDoS).* These are attempts to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted, malevolent efforts of a person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely.

- *Botnets*. The term *botnet* (see Figure 1.7) can be used to refer to any group of bots, or software robots, such as IRC bots, but this word is generally used to refer to a collection of compromised computers (called zombies) running software, usually installed via worms, Trojan horses, or backdoors, under a common command-and-control infrastructure. The majority of these computers are running Microsoft Windows operating systems, but other operating systems can be affected.

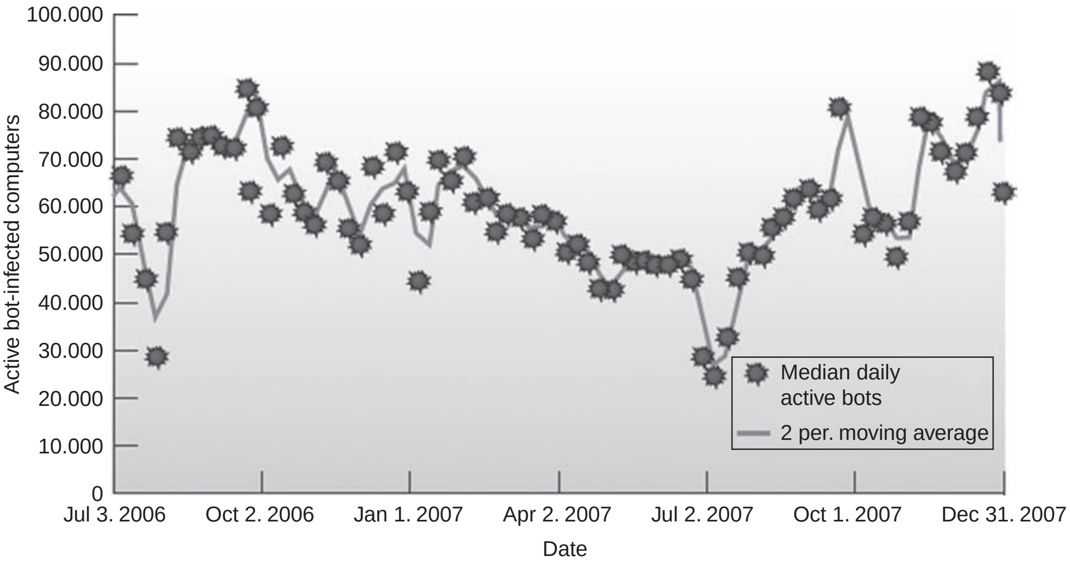


Figure 1.7: Botnet activity, CSI/FBI report, 2008 [13].

Impact of Security Breaches

The impact of security breaches on most organizations can be devastating; however, it's not just dollars and cents that are at stake. Aside from the financial burden of having to deal with a security incident, especially if it leads to litigation, other factors could severely damage an organization's ability to operate, or damage the reputation of an organization beyond recovery. Some of the preliminary key findings from the 2008 CSI/FBI Security Report [14] (see Figure 1.8) include

- Financial fraud cost organizations the most, with an average reported loss of close to $500,000.
- The second most expensive activity was dealing with bots within the network, reported to cost organizations an average of nearly $350,000.

- Virus incidents occurred most frequently, respondents said—at almost half (49%) of respondent organizations.

Some things to consider:

- How much would it cost your organization if your ecommerce Web server farm went down for 12 hours?
- What if your mainframe database that houses your reservation system was not accessible for an entire afternoon?
- What if your Web site was defaced and rerouted all your customers to a site infected with malicious Java scripts?
- Would any of these scenarios significantly impact your organization's bottom line?

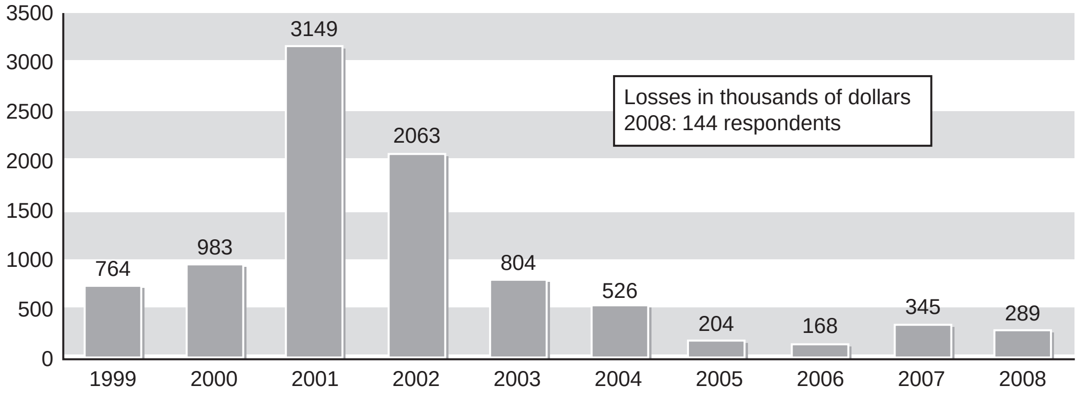


Figure 1.8: 2008 CSI/FBI Security Survey results [15].

2. Protecting Mission-Critical Systems

The IT core of any organization is its mission-critical systems. These are systems without which the mission of the organization, whether building aircraft carriers for the U.S. military or packaging Twinkies to deliver to food markets, could not operate. The major components to protecting these systems are detailed throughout this chapter; however, with special emphasis on the big picture an information security manager must keep in mind, there are some key components that are crucial for the success and continuity of any organization. These are information assurance, information risk management, defense in depth, and contingency planning.

Information Assurance

Information assurance is achieved when information and information systems are protected against attacks through the application of security services such as availability, integrity, authentication, confidentiality, and nonrepudiation. The application of these services should be based on the protect, detect, and react paradigm. This means that in addition to incorporating protection mechanisms, organizations need to expect attacks and include attack detection tools and procedures that allow them to react to and recover from these unexpected attacks [16].

Information Risk Management

Risk is, in essence, the likelihood of something going wrong and damaging your organization or information assets. Due to the ramifications of such risk, an organization should try to reduce the risk to an acceptable level. This process is known as *information risk management*. Risk to an organization and its information assets, similar to threats, comes in many different forms. Some of the most common risks and/or threats are

- *Physical damage*. Fire, water, vandalism, power loss, and natural disasters.
- *Human interaction*. Accidental or intentional action or inaction that can disrupt productivity.
- *Equipment malfunctions*. Failure of systems and peripheral devices.
- *Internal or external attacks*. Hacking, cracking, and attacking.
- *Misuse of data*. Sharing trade secrets; fraud, espionage, and theft.
- *Loss of data*. Intentional or unintentional loss of information through destructive means.
- *Application error*. Computation errors, input errors, and buffer overflows.

The idea of risk management is that threats of any kind must be identified, classified, and evaluated to calculate their damage potential [17]. This is easier said than done.

Administrative, Technical, and Physical Controls

For example, administrative, technical, and physical controls, are as follows:

- Administrative controls consist of organizational policies and guidelines that help minimize the exposure of an organization. They provide a framework by which a business can manage and inform its people how they should conduct themselves while at the workplace and provide clear steps employees can take when they're confronted with a potentially risky situation. Some examples of administrative controls include the corporate security policy, password policy, hiring policies, and disciplinary policies that form the basis for the selection and implementation of logical and physical controls. Administrative controls are of paramount importance because technical and physical controls are manifestations of the administrative control policies that are in place.

- Technical controls use software and hardware resources to control access to information and computing systems, to help mitigate the potential for errors and blatant security policy violations. Examples of technical controls include passwords, network- and host-based firewalls, network intrusion detection systems, and access control lists and data encryption. Associated with technical controls is the *Principle of Least Privilege*, which requires that an individual, program, or system process is not granted any more access privileges than are necessary to perform the task.
- Physical controls monitor and protect the physical environment of the workplace and computing facilities. They also monitor and control access to and from such facilities. Separating the network and workplace into functional areas are also physical controls. An important physical control is also separation of duties, which ensures that an individual cannot complete a critical task by herself.

Risk Analysis

During risk analysis there are several units that can help measure risk. Before risk can be measured, though, the organization must identify the vulnerabilities and threats against its mission-critical systems in terms of business continuity. During risk analysis, an organization tries to evaluate the cost for each security control that helps mitigate the risk. If the control is cost effective relative to the exposure of the organization, then the control is put in place. The measure of risk can be determined as a product of threat, vulnerability, and asset values—in other words:

$$\text{Risk} = \text{Asset} \times \text{Threat} \times \text{Vulnerability}$$

There are two primary types of risk analysis: quantitative and qualitative. *Quantitative risk analysis* attempts to assign meaningful numbers to all elements of the risk analysis process. It is recommended for large, costly projects that require exact calculations. It is typically performed to examine the viability of a project's cost or time objectives. Quantitative risk analysis provides answers to three questions that cannot be addressed with deterministic risk and project management methodologies such as traditional cost estimating or project scheduling [18]:

- What is the probability of meeting the project objective, given all known risks?
- How much could the overrun or delay be, and therefore how much contingency is needed for the organization's desired level of certainty?
- Where in the project is the most risk, given the model of the project and the totality of all identified and quantified risks?

Qualitative risk analysis does not assign numerical values but instead opts for general categorization by severity levels. Where little or no numerical data is available for a risk assessment, the qualitative approach is the most appropriate. The qualitative approach does not require heavy mathematics; instead, it thrives more on the people participating and their backgrounds. Qualitative analysis enables classification of risk that is determined by people's wide experience and knowledge captured within the process. Ultimately, it is not an exact science, so the process will count on expert opinions for its base assumptions. The assessment process uses a structured and documented approach and agreed likelihood and consequence evaluation tables. It is also quite common to calculate risk as a single loss expectancy (SLE) or annual loss expectancy (ALE) by project or business function.

Defense in Depth

The principle of *defense in depth* is that layered security mechanisms increase security of a system as a whole. If an attack causes one security mechanism to fail, other mechanisms may still provide the necessary security to protect the system [19]. This is a process that involves people, technology, and operations as key components to its success; however, those are only part of the picture. These organizational layers are difficult to translate into specific technological layers of defenses, and they leave out areas such as security monitoring and metrics. Figure 1.9 shows a mind map that organizes the major categories from both the organizational and technical aspects of defense in depth and takes into account people, policies, monitoring, and security metrics.

Contingency Planning

Contingency planning is necessary in several ways for an organization to be sure it can withstand some sort of security breach or disaster. Among the important steps required to make sure an organization is protected and able to respond to a security breach or disaster are business impact analysis, incident response planning, disaster recovery planning, and business continuity planning. These contingency plans are interrelated in several ways and need to stay that way so that a response team can change from one to the other seamlessly if there is a need. Figure 1.10 shows the relationship between the four types of contingency plans with the major categories defined in each.

Business impact analysis must be performed in every organization to determine exactly which business process is deemed mission critical and which processes would not seriously hamper business operations should they be unavailable for some time. An important part of a business impact analysis is the recovery strategy that is usually defined at the end of the process. If a thorough business impact analysis is performed, there should be a clear picture of the priority of each organization's highest-impact, therefore risky, business processes and assets as well as a clear strategy to recover from an interruption in one of these areas [20].

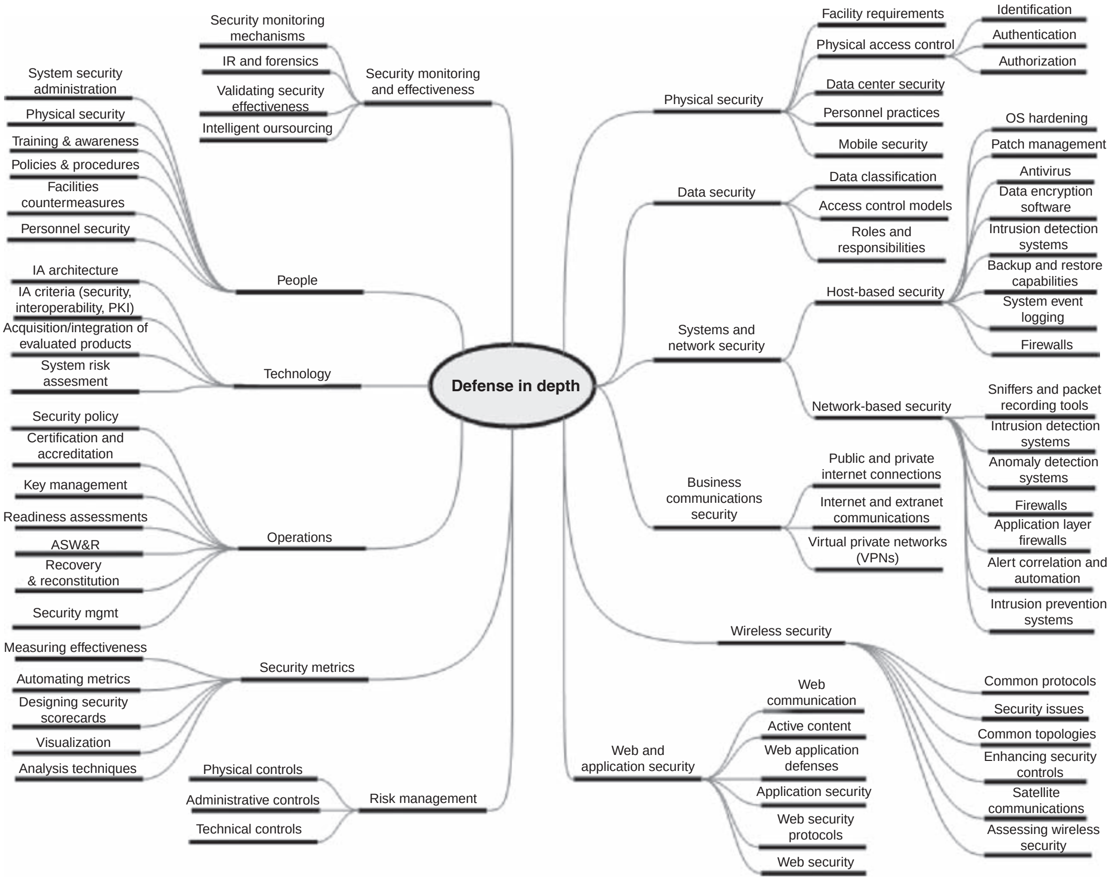


Figure 1.9: Defense-in-depth mind map.

An Incident Response (IR) Plan

An incident response (IR) plan is a detailed set of processes and procedures that anticipate, detect, and mitigate the impact of an unexpected event that might compromise information resources and assets. Incident response plans are composed of six major phases:

1. *Preparation*. This phase involves planning and readying in the event of a security incident.
2. *Identification*. This phase involves identifying a set of events that have some negative impact on the business and can be considered a security incident.
3. *Containment*. During this phase the security incident has been identified and action is required to mitigate its potential damage.
4. *Eradication*. After it's contained, the incident must be eradicated and studied to make sure it has been thoroughly removed from the system.

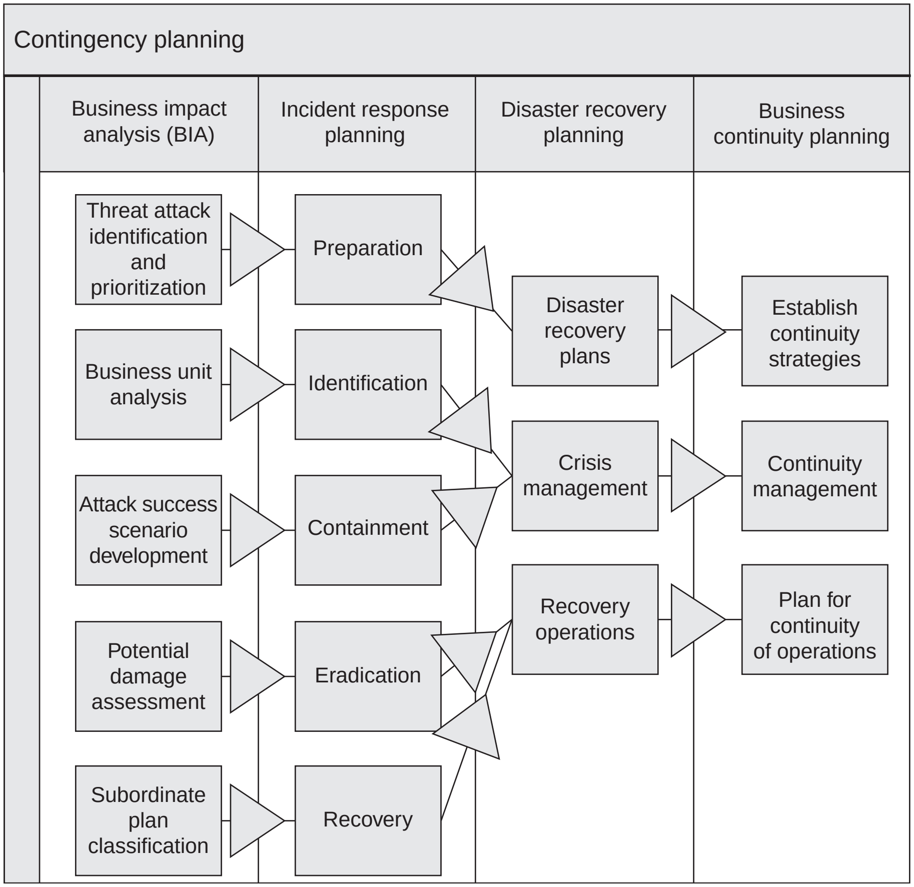

Contingency planning
Business impact analysis (BIA)
Incident response planning
Disaster recovery planning
Business continuity planning
Threat attack identification and prioritization
Business unit analysis
Attack success scenario development
Potential damage assessment
Subordinate plan classification
Preparation
Identification
Containment
Eradication
Recovery
Disaster recovery plans
Crisis management
Recovery operations
Establish continuity strategies
Continuity management
Plan for continuity of operations

Figure 1.10: The relationship between the four types of contingency plans.

5. *Recovery*. This phase involves bringing the business and assets involved in the security incident back to normal operations.
6. *Lessons learned*. A thorough review of how the incident occurred and the actions taken to respond to it where the lessons learned get applied to future incidents.

When a threat becomes a valid attack, it is classified as an information security incident if [21]

- It is directed against information assets.
- It has a realistic chance of success.
- It threatens the confidentiality, integrity, or availability of information assets.

Business Continuity Planning (BCP)

Business continuity planning ensures that critical business functions can continue during a disaster and is most properly managed by the CEO of the organization. The BCP is usually activated and executed concurrently with *disaster recovery planning* (DRP) when needed and re-establishes critical functions at alternate sites (DRP focuses on re-establishment at the primary site). BCP relies on identification of critical business functions and the resources to support them using several continuity strategies, such as exclusive-use options like hot, warm, and cold sites or shared-use options like timeshare, service bureaus, or mutual agreements [22].

Disaster recovery planning is the preparation for and recovery from a disaster. Whether natural or manmade, it is an incident that has become a disaster because the organization is unable to contain or control its impact, or the level of damage or destruction from the incident is so severe that the organization is unable to recover quickly. The key role of DRP is defining how to re-establish operations at the site where the organization is usually located [23]. Key points in a properly designed DRP are

- Clear delegation of roles and responsibilities
- Execution of alert roster and notification of key personnel
- Clear establishment of priorities
- Documentation of the disaster
- Action steps to mitigate the impact
- Alternative implementations for various systems components
- Regular testing of the DRP

3. Information Security from the Ground Up

The core concepts of information security management and protecting mission-critical systems have been explained. Now, how do you actually apply these concepts to your organization from the ground up? You literally start at the ground (physical) level and work yourself up to the top (application) level. This model can be applied to many IT frameworks, ranging from networking models such as OSI or TCP/IP stacks to operating systems or other problems such as organizational information security and protecting mission-critical systems.

There are many areas of security, all of which are interrelated. You can have an extremely hardened system running your ecommerce Web site and database; however, if physical access to the system is obtained by the wrong person, a simple yanking of the right power plug can be game over. In other words, to think that any one of the following components is not important to the overall security of your organization is to provide malicious attackers the

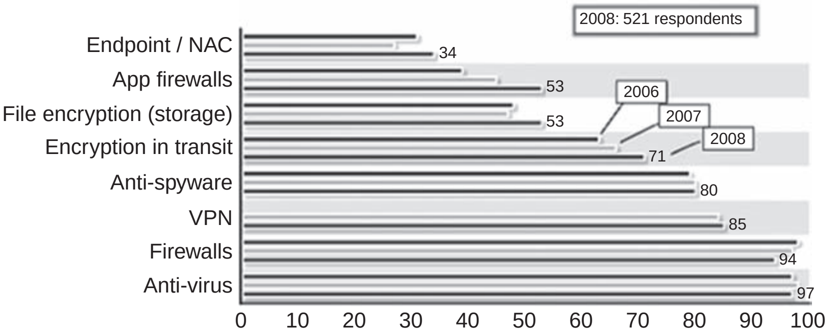


Figure 1.11: Security technologies used by organizations, CSI/FBI report, 2008.

only thing they need to be successful—that is, the path of least resistance. The following parts of this chapter contain an overview of the technologies (see Figure 1.11) and processes of which information security managers must be aware to successfully secure the assets of any organization:

- Physical security
- Data security
- Systems and network security
- Business communications security
- Wireless security
- Web and application security
- Security policies and procedures
- Security employee training and awareness

Physical Security

Physical security as defined earlier concerns itself with threats, risks, and countermeasures to protect facilities, hardware, data, media and personnel. Main topics include restricted areas, authorization models, intrusion detection, fire detection, and security guards. Therefore, physical safeguards must be put in place to protect the organization from damaging consequences. The security rule defines physical safeguards as "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion." [24] A brief description of the baseline requirements to implement these safeguards at your facility follows.

Facility Requirements

Entering and accessing information systems to any degree within any organization must be controlled. What's more, it is necessary to understand what is allowed and what is not; if those parameters are clearly defined, the battle is half won. Not every building is a high-security facility, so it's understandable that some of the following items might not apply to your organization; however, there should be a good, clear reason as to why they don't. Here are sample questions to consider: [25]

- Are policies and procedures developed and implemented that address allowing authorized and limiting unauthorized physical access to electronic information systems and the facility or facilities in which they are housed?
- Do the policies and procedures identify individuals (workforce members, business associates, contractors, etc.) with authorized access by title and/or job function?
- Do the policies and procedures specify the methods used to control physical access, such as door locks, electronic access control systems, security officers, or video monitoring?

The facility access controls standard has four implementation specifications [26]:

- *Contingency operations.* Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
- *Facility security plan.* Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
- *Access control and validation procedures.* Implement procedures to control and validate a person's access to facilities based on her role or function, including visitor control and control of access to software programs for testing and revision.
- *Maintenance records.* Implement policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks).

Administrative, Technical, and Physical Controls

Understanding what it takes to secure a facility is the first step in the process of identifying exactly what type of administrative, technical, and physical controls will be necessary for your particular organization. Translating the needs for security into tangible examples, here are some of the controls that can be put in place to enhance security:

- *Administrative controls.* These include human resources exercises for simulated emergencies such as fire drills or power outages as well as security awareness training and security policies.

- *Technical controls*. These include physical intrusion detection systems and access control equipment such as biometrics.
- *Physical controls*. These include video cameras, guarded gates, man traps, and car traps.

Data Security

Data security is at the core of what needs to be protected in terms of information security and mission-critical systems. Ultimately, it is the data that the organization needs to protect in many cases, and usually data is exactly what perpetrators are after, whether trade secrets, customer information, or a database of Social Security numbers—the data is where it's at!

To be able to properly classify and restrict data, one first needs to understand how data is accessed. Data is accessed by a *subject*, whether that is a person, process, or another application, and what is accessed to retrieve the data is called an *object*. Think of an object as a cookie jar with valuable information in it, and only select subjects have the permissions necessary to dip their hands into the cookie jar and retrieve the data or information that they are looking for. Both subjects and objects can be a number of things acting in a network, depending on what action they are taking at any given moment, as shown in Figure 1.12.

Data Classification

Various *data classification* models are available for different environments. Some security models focus on the confidentiality of the data (such as Bell-La Padula) and use different classifications. For example, the U.S. military uses a model that goes from most confidential (Top Secret) to least confidential (Unclassified) to classify the data on any given system. On the other hand, most corporate entities prefer a model whereby they classify data by business

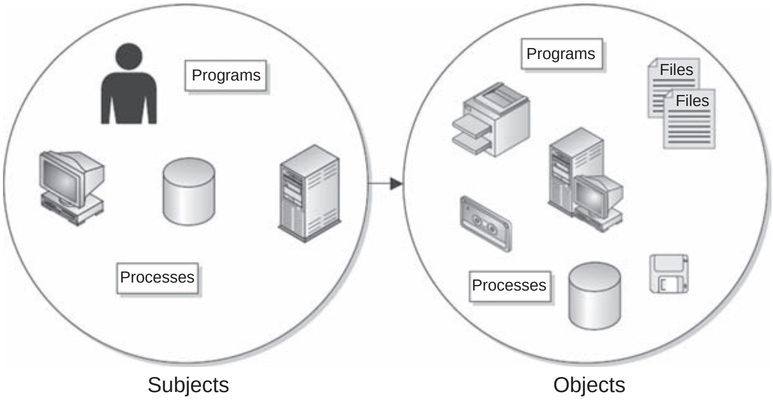


Figure 1.12: Subjects access objects.

unit (HR, Marketing, R&D, etc.) or use terms such as *Company Confidential* to define items that should not be shared with the public. Other security models focus on the integrity of the data (for example, Bipa); yet others are expressed by mapping security policies to data classification (for example, Clark-Wilson). In every case there are areas that require special attention and clarification.

Access Control Models

Three main *access control models* are in use today: RBAC, DAC, and MAC. In Role-Based Access Control (RBAC), the job function of the individual determines the group he is assigned to and determines the level of access he can attain on certain data and systems. The level of access is usually defined by IT personnel in accordance with policies and procedures. In Discretionary Access Control (DAC), the end user or creator of the data object is allowed to define who can and who cannot access the data; this model has become less popular in recent history. Mandatory Access Control (MAC) is more of a militant style of applying permissions, where permissions are the same across the board to all members of a certain level or class within the organization.

The following are data security "need-to-knows":

- *Authentication versus authorization.* It's crucial to understand that simply because someone becomes authenticated does not mean that she is authorized to view certain data. There needs to be a means by which a person, after gaining access through authentication, is limited in the actions she is authorized to perform on certain data (such as read-only permissions).
- *Protecting data with cryptography* is important for the security of both the organization and its customers. Usually, the most important item that an organization needs to protect, aside from trade secrets, is its customers' personal data. If there is a security breach and the data that is stolen or compromised was previously encrypted, the organization can feel more secure in that the collateral damage to its reputation and customer base will be minimized.
- *Data leakage prevention and content management* is an up-and-coming area of data security that has proven extremely useful in preventing sensitive information from leaving an organization. With this relatively new technology, a security administrator can define the types of documents, and further define the content within those documents, that cannot leave the organization and quarantine them for inspection before they hit the public Internet.
- *Securing email systems* is one of the most important and overlooked areas of data security. With access to the mail server, an attacker can snoop through anyone's email, even the company CEO's! Password files, company confidential documents,

and contacts for all address books are only some of the things that a compromised mail server can reveal about an organization, not to mention root/administrator access to a system in the internal network.

Systems and Network Security

Systems and network security [27] is at the core of information security. Though physical security is extremely important and a breach could render all your systems and network security safeguards useless, without hardened systems and networks, anyone from the comfort of her own living room can take over your network, access your confidential information, and disrupt your operations at will. Data classification and security are also quite important, if for nothing else but to be sure that only those who need to access certain data can and those who do not need access cannot; however, that usually works well for people who play by the rules. In many cases when an attacker gains access to a system, the first order of business is escalation of privileges. This means that the attacker gets in as a regular user and attempts to find ways to gain administrator or root privileges.

The following are brief descriptions of each of the components that make for a complete security infrastructure for all host systems and network-connected assets.

Host-Based Security

The host system is the core place where data sit and are accessed, so it is therefore also the main target of many intruders. Regardless of the operating system platform that is selected to run certain applications and databases, the principles of hardening systems are the same and apply to host systems as well as network devices, as we will see in the upcoming sections. Steps required to maintain host systems in as secure a state as possible are as follows:

1. *OS hardening*. Guidelines by which a base operating system goes through a series of checks to make sure no unnecessary exposures remain open and that security features are enabled where possible. There is a series of organizations that publish OS hardening guides for various platforms of operating systems.

2. *Removing unnecessary services*. In any operating system there are usually services that are enabled but have no real business need. It is necessary to go through all the services of your main corporate image, on both the server side and client side, to determine which services are required and which would create a potential vulnerability if left enabled.

3. *Patch management*. All vendors release updates for known vulnerabilities on some kind of schedule. Part of host-based security is making sure that all required vendor

patches, at both the operating system and the application level, are applied as quickly as business operations allow on some kind of regular schedule. There should also be an emergency patch procedure in case there is an outbreak and updates need to be pushed out of sequence.

4. *Antivirus*. Possibly more important than patches are antivirus definitions, specifically on desktop and mobile systems. Corporate antivirus software should be installed and updated frequently on all systems in the organization.
5. *Intrusion detection systems (IDSs)*. Although many seem to think IDSs are a network security function, there are many good host-based IDS applications, both commercial and open source, that can significantly increase security and act as an early warning system for possibly malicious traffic and/or files for which the AV does not have a definition.
6. *Firewalls*. Host-based firewalls are not as popular as they once were because many big vendors such as Symantec, McAfee, and Checkpoint have moved to a host-based client application that houses all security functions in one. There is also another trend in the industry to move toward application-specific host-based firewalls like those specifically designed to run on a Web or database server, for example.
7. *Data encryption software*. One item often overlooked is encryption of data while at rest. Many solutions have recently come onto the market that offer the ability to encrypt sensitive data such as credit-card and Social Security numbers that sit on your file server or inside the database server. This is a huge protection in the case of information theft or data leakage.
8. *Backup and restore capabilities*. Without the ability to back up and restore both servers and clients in a timely fashion, an issue that could be resolved in short order can quickly turn into a disaster. Backup procedures should be in place and restored on a regular basis to verify their integrity.
9. *System event logging*. Event logs are significant when you're attempting to investigate the root cause of an issue or incident. In many cases, logging is not turned on by default and needs to be enabled after the core installation of the host operating system. The OS hardening guidelines for your organization should require that logging be enabled.

Network-Based Security

The network is the communication highway for everything that happens between all the host systems. All data at one point or another pass over the wire and are potentially vulnerable to snooping or spying by the wrong person. The controls implemented on the network are similar in nature to those that can be applied to host systems; however, network-based security can be more easily classified into two main categories: detection and prevention.

We will discuss security monitoring tools in another section; for now the main functions of network-based security are to either detect a potential incident based on a set of events or prevent a known attack.

Most network-based security devices can perform detect or protect functions in one of two ways: signature-based or anomaly-based. Signature-based detection or prevention is similar to AV signatures that look for known traits of a particular attack or malware. Anomaly-based systems can make decisions based on what is expected to be "normal" on the network or per a certain set of standards (for example, RFC), usually after a period of being installed in what is called "learning" or "monitor" mode.

Intrusion Detection

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents that are violations or imminent threats of violation of computer security policies, acceptable-use policies, or standard security practices. Incidents have many causes, such as malware (e.g., worms, spyware), attackers gaining unauthorized access to systems from the Internet, and authorized system users who misuse their privileges or attempt to gain additional privileges for which they are not authorized [28]. The most common detection technologies and their security functions on the network are as follows:

- *Packet sniffing and recording tools.* These tools are used quite often by networking teams to troubleshoot connectivity issues; however, they can be a security professional's best friend during investigations and root-cause analysis. When properly deployed and maintained, a packet capture device on the network allows security professionals to reconstruct data and reverse-engineer malware in a way that is simply not possible without a full packet capture of the communications.

- *Intrusion detection systems.* In these systems, appliances or servers monitor network traffic and run it through a rules engine to determine whether it is malicious according to its signature set. If the traffic is deemed malicious, an alert will fire and notify the monitoring system.

- *Anomaly detection systems.* Aside from the actual packet data traveling on the wire, there are also traffic trends that can be monitored on the switches and routers to determine whether unauthorized or anomalous activity is occurring. With Net-flow and S-flow data that can be sent to an appliance or server, aggregated traffic on the network can be analyzed and can alert a monitoring system if there is a problem. Anomaly detection systems are extremely useful when there is an attack for which the IDS does not have a signature or if there is some activity occurring that is suspicious.

Intrusion Prevention

Intrusion prevention is a system that allows for the active blocking of attacks while they are inline on the network, before they even get to the target host. There are many ways to prevent attacks or unwanted traffic from coming into your network, the most common of which is known as a firewall. Although a firewall is mentioned quite commonly and a lot of people know what a firewall is, there are several different types of controls that can be put in place in addition to a firewall that can seriously help protect the network. Here are the most common prevention technologies:

- *Firewalls.* The purpose of a firewall is to enforce an organization's security policy at the border of two networks. Typically, most firewalls are deployed at the edge between the internal network and the Internet (if there is such a thing) and are configured to block (prevent) any traffic from going in or out that is not allowed by the corporate security policy. There are quite a few different levels of protection a firewall can provide, depending on the type of firewall that is deployed, such as these:

  Packet filtering. The most basic types of firewalls perform what is called *stateful packet filtering*, which means that they can remember which side initiated the connection, and rules (called access control lists, or ACLs) can be created based not only on IPs and ports but also depending on the state of the connection (meaning whether the traffic is going into or out of the network).

  Proxies. The main difference between proxies and stateful packet-filtering firewalls is that proxies have the capability to terminate and re-establish connections between two end hosts, acting as a proxy for all communications and adding a layer of security and functionality to the regular firewalls.

  Application layer firewalls. The app firewalls have become increasingly popular; they are designed to protect certain types of applications (Web or database) and can be configured to perform a level of blocking that is much more intuitive and granular, based not only on network information but also application-specific variables so that administrators can be much more precise in what they are blocking. In addition, app firewalls can typically be loaded with server-side SSL certificates, allowing the appliance to decrypt encrypted traffic, a huge benefit to a typical proxy or stateful firewall.

- *Intrusion prevention systems.* An intrusion prevention system (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents using a set of conditions based on signatures or anomalies.

Business Communications Security

Businesses today tend to communicate with many other business entities, not only over the Internet but also through private networks or guest access connections directly to the organization's network, whether wired or wireless. Business partners and contractors conducting business communications obviously tend to need a higher level of access than public users but not as extensive as permanent employees, so how does an organization handle this phenomenon? External parties working on internal projects are also classed as business partners. Some general rules for users to maintain security control of external entities are shown in Figure 1.13.

General Rules for Self-Protection

The general rules for self-protection are as follows:

- Access to a user's own IT system must be protected in such a way that system settings (e.g., in the BIOS) can be changed only subject to authentication.
- System start must always be protected by requiring appropriate authentication (e.g., requesting the boot password). Exceptions to this rule can apply if:

  Automatic update procedures require this, and the system start can take place only from the built-in hard disk.

  The system is equipped for use by a number of persons with their individual user profiles, and system start can take place only from the built-in hard disk.

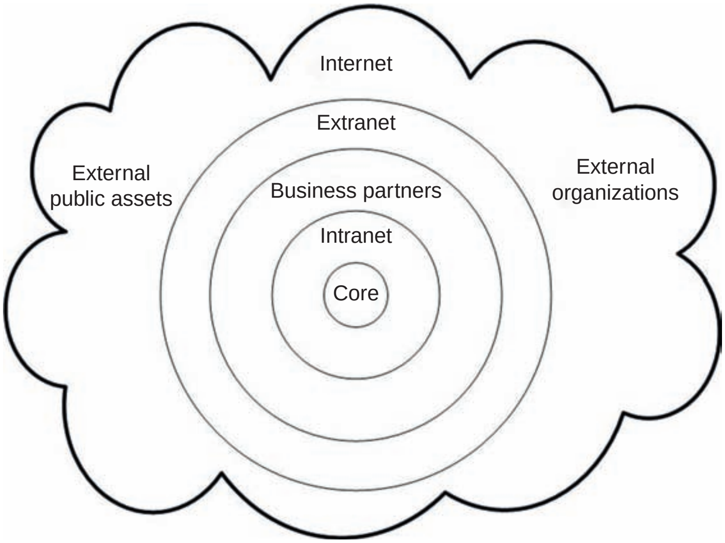


Figure 1.13: The business communications cloud.

- Unauthorized access to in-house resources including data areas (shares, folders, mailboxes, calendar, etc.) must be prevented in line with their need for protection. In addition, the necessary authorizations for approved data access must be defined.
- Users are not permitted to operate resources without first defining any authorizations (such as no global sharing). This rule must be observed particularly by those users who are system managers of their own resources.
- Users of an IT system must lock the access links they have opened (for example, by enabling a screensaver or removing the chip card from the card reader), even during short periods of absence from their workstations.
- When work is over, all open access links must be properly closed or protected against system/data access (such as if extensive compilation runs need to take place during the night).
- Deputizing rules for access to the user's own system or data resources must be made in agreement with the manager and the acting employee.

Handling Protection Resources

The handling of protection resources is as follows:

- Employees must ensure that their protection resources cannot be subject to snooping while data required for authentication are being entered (e.g., password entry during login).
- Employees must store all protection resources and records in such a way that they cannot be subjected to snooping or being stolen.
- Personal protection resources must never be made available to third parties.
- In the case of chip cards, SecurID tokens, or other protection resources requiring a PIN, the associated PIN (PIN letter) must be stored separately.
- Loss, theft, or disclosure of protection resources is to be reported immediately.
- Protection resources subject to loss, theft, or snooping must be disabled immediately.

Rules for Mobile IT Systems

In addition to the general rules for users, the following rules may also apply for mobile IT systems:

- There is extended self-protection.
- A mobile IT system must be safeguarded against theft (that is, secured with a cable lock, locked away in a cupboard).

- The data from a mobile IT system using corporate proprietary information must be safeguarded as appropriate (e.g., encryption). In this connection, CERT rules in particular are to be observed.
- The software provided by the organization for system access control may be used only on the organization's own mobile IT systems.

Operation on Open Networks

Rules for operation on open networks are as follows:

- The mobile IT system must be operated in open network environments using a personal firewall.
- The configuration of the personal firewall must be in accordance with the corporate policy or, in the case of other personal firewall systems, must be subject to restrictive settings.
- A mobile IT system must be operated in an unprotected open network only for the duration of a secure access link to the organization's own network. The connection establishment for the secure access link must be performed as soon as possible, at least within five minutes.
- Simultaneous operation on open networks (protected or unprotected) and the organization's own networks is forbidden at all times.
- Remote access to company internal resources must always be protected by means of strong authentication.
- For the protection of data being transferred via a remote access link, strong encryption must always be used.

Additional Business Communications Guidelines

Additional business communications guidelines should be defined for the following:

- External IT systems may not be connected directly to the intranet. Transmission of corporate proprietary data to external systems should be avoided wherever possible, and copies of confidential or strictly confidential data must never be created on external IT systems.
- Unauthorized access to public data areas (shares, folders, mailboxes, calendars, etc.) is to be prevented. The appropriate authentication checks and authorization requirements must be defined, and the operation of resources without such requirements is not permitted (e.g., no global sharing).
- Remote data access operations must be effected using strong authentication and encryption, and managers must obtain permission from the owner of the resources to access.

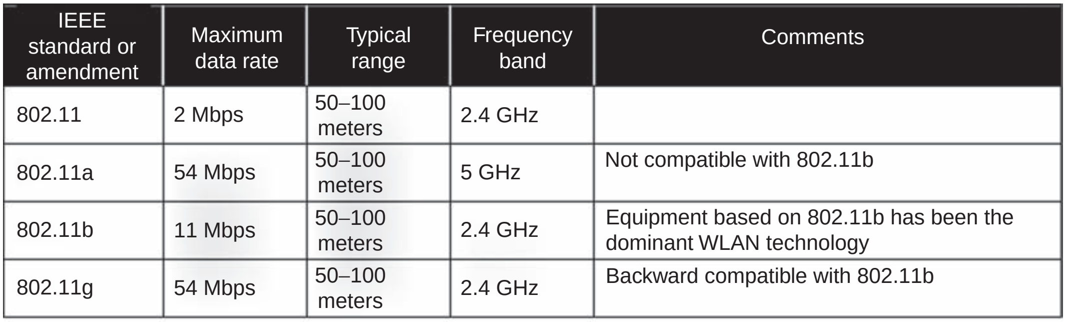
- For secure remote maintenance by business partners, initialization of the remote maintenance must take place from an internal system, such as via an Internet connection protected by strong encryption. An employee must be present at the system concerned during the entire remote maintenance session to monitor the remote maintenance in accordance with the policy, and the date, nature, and extent of the remote maintenance must be logged at a minimum.

Wireless Security

Wireless networking enables devices with wireless capabilities to use information resources without being physically connected to a network. A wireless local area network (WLAN) is a group of wireless networking nodes within a limited geographic area that is capable of radio communications. WLANs are typically used by devices within a fairly limited range, such as an office building or building campus, and are usually implemented as extensions to existing wired local area networks to provide enhanced user mobility. Since the beginning of wireless networking, many standards and technologies have been developed for WLANs. One of the most active standards organizations that address wireless networking is the Institute of Electrical and Electronics Engineers (IEEE), as outlined in Figure 1.14 [29]. Like other wireless technologies, WLANs typically need to support several security objectives. This is intended to be accomplished through a combination of security features built into the wireless networking standard.

The most common security objectives for WLANs are as follows:

- *Access control*. Restrict the rights of devices or individuals to access a network or resources within a network.
- *Confidentiality*. Ensure that communication cannot be read by unauthorized parties.
- *Integrity*. Detect any intentional or unintentional changes to data that occur in transit.



IEEE standard or amendment	Maximum data rate	Typical range	Frequency band	Comments
802.11	2 Mbps	50–100 meters	2.4 GHz	
802.11a	54 Mbps	50–100 meters	5 GHz	Not compatible with 802.11b
802.11b	11 Mbps	50–100 meters	2.4 GHz	Equipment based on 802.11b has been the dominant WLAN technology
802.11g	54 Mbps	50–100 meters	2.4 GHz	Backward compatible with 802.11b

Figure 1.14: IEEE Common Wireless Standards: NIST SP800-97 [30].

- *Availability*. Ensure that devices and individuals can access a network and its resources whenever needed.

Access Control

Typically, there are two means by which to validate the identities of wireless devices attempting to connect to a WLAN: open system authentication and shared-key authentication. Neither of these alternatives is secure. The security provided by the default connection means is unacceptable; all it takes for a host to connect to your system is a Service Set Identifier (SSID) for the AP (which is a name that is broadcast in the clear) and, optionally, a MAC address. The SSID was never intended to be used as an access control feature.

A MAC address is a unique 48-bit value that is permanently assigned to a particular wireless network interface. Many implementations of IEEE 802.11 allow administrators to specify a list of authorized MAC addresses; the AP will permit devices with those MAC addresses only to use the WLAN. This is known as *MAC address filtering*. However, because the MAC address is not encrypted, it is simple to intercept traffic and identify MAC addresses that are allowed past the MAC filter. Unfortunately, almost all WLAN adapters allow applications to set the MAC address, so it is relatively trivial to spoof a MAC address, meaning that attackers can easily gain unauthorized access. Additionally, the AP is not authenticated to the host by open system authentication. Therefore, the host has to trust that it is communicating to the real AP and not an impostor AP that is using the same SSID. Therefore, open system authentication does not provide reasonable assurance of any identities and can easily be misused to gain unauthorized access to a WLAN or to trick users into connecting to a malicious WLAN [31].

Confidentiality

The WEP protocol attempts some form of confidentiality by using the RC4 stream cipher algorithm to encrypt wireless communications. The standard for WEP specifies support for a 40-bit WEP key only; however, many vendors offer nonstandard extensions to WEP that support key lengths of up to 128 or even 256 bits. WEP also uses a 24-bit value known as an *initialization vector* (IV) as a seed value for initializing the cryptographic keystream. Ideally, larger key sizes translate to stronger protection, but the cryptographic technique used by WEP has known flaws that are not mitigated by longer keys. WEP is not the secure alternative you’re looking for.

A possible threat against confidentiality is network traffic analysis. Eavesdroppers might be able to gain information by monitoring and noting which parties communicate at particular times. Also, analyzing traffic patterns can aid in determining the content of communications; for example, short bursts of activity might be caused by terminal emulation or instant messaging, whereas steady streams of activity might be generated by videoconferencing.

More sophisticated analysis might be able to determine the operating systems in use based on the length of certain frames. Other than encrypting communications, IEEE 802.11, like most other network protocols, does not offer any features that might thwart network traffic analysis, such as adding random lengths of padding to messages or sending additional messages with randomly generated data [32].

Integrity

Data integrity checking for messages transmitted between hosts and APs exists and is designed to reject any messages that have been changed in transit, such as by a man-in-the-middle attack. WEP data integrity is based on a simple encrypted checksum—a 32-bit cyclic redundancy check (CRC-32) computed on each payload prior to transmission. The payload and checksum are encrypted using the RC4 keystream and then transmitted. The receiver decrypts them, recomputes the checksum on the received payload, and compares it with the transmitted checksum. If the checksums are not the same, the transmitted data frame has been altered in transit, and the frame is discarded. Unfortunately, CRC-32 is subject to bit-flipping attacks, which means that an attacker knows which CRC-32 bits will change when message bits are altered. WEP attempts to counter this problem by encrypting the CRC-32 to produce an integrity check value (ICV). WEP's creators believed that an enciphered CRC-32 would be less subject to tampering. However, they did not realize that a property of stream ciphers such as WEP's RC4 is that bit flipping survives the encryption process: The same bits flip whether or not encryption is used. Therefore, the WEP ICV offers no additional protection against bit flipping [33].

Availability

Individuals who do not have physical access to the WLAN infrastructure can cause a denial of service for the WLAN. One threat is known as jamming, which involves a device that emits electromagnetic energy on the WLAN's frequencies. The energy makes the frequencies unusable by the WLAN, causing a denial of service. Jamming can be performed intentionally by an attacker or unintentionally by a non-WLAN device transmitting on the same frequency. Another threat against availability is flooding, which involves an attacker sending large numbers of messages to an AP at such a high rate that the AP cannot process them, or other STAs cannot access the channel, causing a partial or total denial of service. These threats are difficult to counter in any radio-based communications; thus, the IEEE 802.11 standard does not provide any defense against jamming or flooding. Also, attackers can establish rogue APs; if STAs mistakenly attach to a rogue AP instead of a legitimate one, this could make the legitimate WLAN effectively unavailable to users. Although 802.11i protects data frames, it does not offer protection to control or management frames. An attacker can exploit the fact that management frames are not authenticated to deauthenticate a client or to disassociate a client from the network [34].

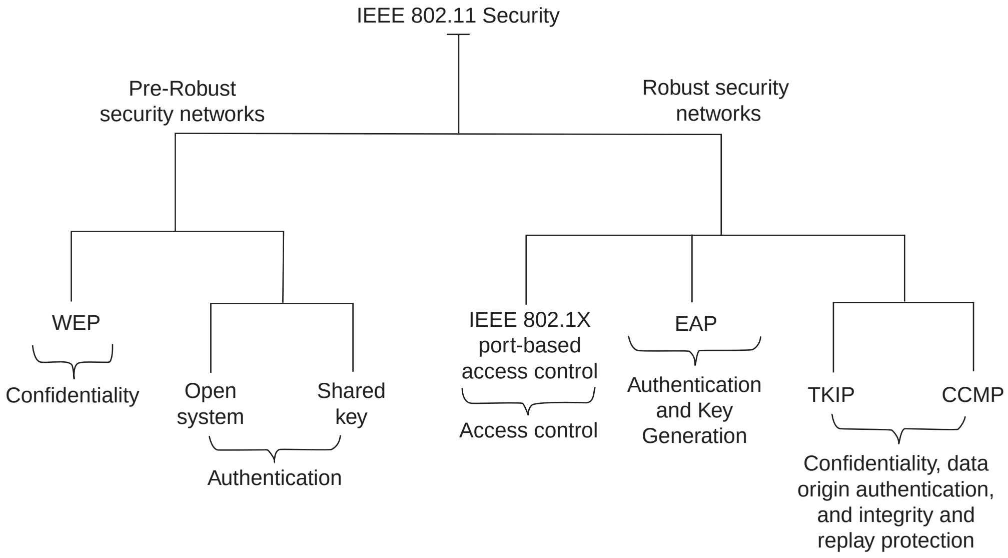

IEEE 802.11 Security
Pre-Robust security networks
Robust security networks
WEP
Confidentiality
Open system
Shared key
Authentication
IEEE 802.1X port-based access control
Access control
EAP
Authentication and Key Generation
TKIP
CCMP
Confidentiality, data origin authentication, and integrity and replay protection

Figure 1.15: High-level taxonomy of the major pre-RSN and RSN security mechanisms [35].

Enhancing Security Controls

The IEEE 802.11i amendment allows for enhanced security features beyond WEP and the simple IEEE 802.11 shared-key challenge-response authentication. The amendment introduces the concepts of Robust Security Networks (RSNs) (see Figure 1.15) and Robust Security Network Associations (RSNAs). There are two RSN data confidentiality and integrity protocols defined in IEEE 802.11i: Temporal Key Integrity Protocol (TKIP) and Counter Mode with Cipher-Block Chaining Message Authentication Code Protocol (CCMP).

At a high level, RSN includes IEEE 802.1x port-based access control, key management techniques, and the TKIP and CCMP data confidentiality and integrity protocols. These protocols allow for the creation of several diverse types of security networks because of the numerous configuration options. RSN security is at the link level only, providing protection for traffic between a wireless host and its associated AP or between one wireless host and another. It does not provide end-to-end application-level security, such as between a host and an email or Web server, because communication between these entities requires more than just one link. For infrastructure mode, additional measures need to be taken to provide end-to-end security.

The IEEE 802.11i amendment defines an RSN as a wireless network that allows the creation of RSN Associations (RSNAs) only. An RSNA is a security relationship established by the IEEE 802.11i 4-Way Handshake. The 4-Way Handshake validates that the parties to the protocol instance possess a pairwise master key (PMK), synchronize the installation of temporal keys, and confirm the selection of cipher suites. The PMK is the cornerstone of a number of security features absent from WEP. Complete robust security is considered possible only when all devices in the network use RSNAs. In practice, some networks have a mix of RSNAs and non-RSNA connections. A network that allows the creation of both pre-RSN associations (pre-RSNA) and RSNAs is referred to as a Transition Security Network (TSN). A TSN is intended to be an interim means to provide connectivity while an organization migrates to networks based exclusively on RSNAs. RSNAs enable the following security features for IEEE 802.11 WLANs:

- Enhanced user authentication mechanisms
- Cryptographic key management
- Data confidentiality
- Data origin authentication and integrity
- Replay protection

An RSNA relies on IEEE 802.1x to provide an authentication framework. To achieve the robust security of RSNAs, the designers of the IEEE 802.11i amendment used numerous mature cryptographic algorithms and techniques. These algorithms can be categorized as being used for confidentiality, integrity (and data origin authentication), or key generation. All the algorithms specifically referenced in the IEEE 802.11 standard (see Figure 1.16) are symmetric algorithms, which use the same key for two different steps of the algorithm, such as encryption and decryption.

TKIP is a cipher suite for enhancing WEP on pre-RSN hardware without causing significant performance degradation. TKIP works within the processing constraints of first-generation hosts and APs and therefore enables increased security without requiring hardware replacement. TKIP provides the following fundamental security features for IEEE 802.11 WLANs:

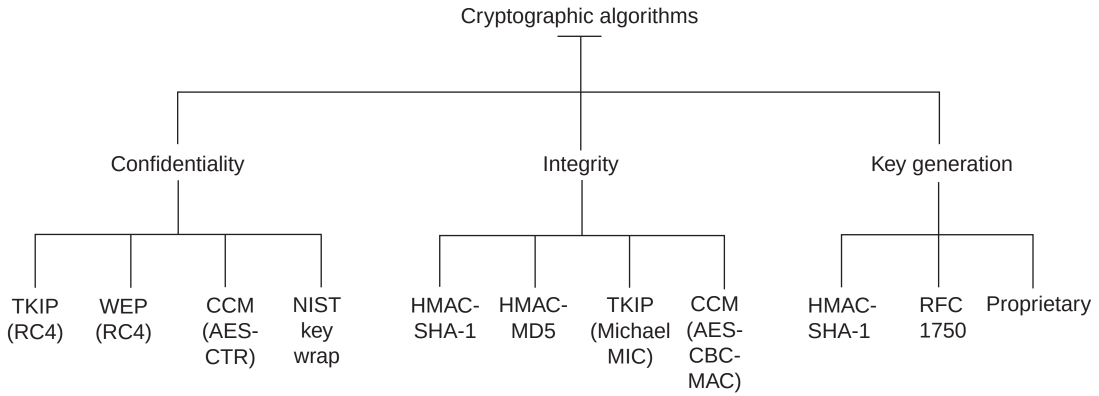


Figure 1.16: Taxonomy of the cryptographic algorithms included in the IEEE 802.11 standard [36].

- Confidentiality protection using the RC4 algorithm [38].
- Integrity protection against several types of attacks [39] using the Michael message digest algorithm (through generation of a message integrity code [MIC]) [40]
- Replay prevention through a frame-sequencing technique
- Use of a new encryption key for each frame to prevent attacks, such as the Fluhrer-Mantin-Shamir (FMS) attack, which can compromise WEP-based WLANs [41]
- Implementation of countermeasures whenever the STA or AP encounters a frame with a MIC error, which is a strong indication of an active attack

Web and Application Security

Web and application security has come to center stage because Web sites and other public-facing applications have had so many vulnerabilities reported that it is often trivial to find some part of the application that is vulnerable to one of the many exploits out there. When an attacker compromises a system at the application level, often it is too trivial to take advantage of all the capabilities said application has to offer, including querying the back-end database or accessing proprietary information. In the past it was not necessary to implement security during the development phase of an application, and since most security professionals are not programmers, that worked out just fine; however, due to factors such as rushing software releases and a certain level of complacency where end users expect buggy software and apply patches, the trend of inserting security earlier in the development process is catching steam.

Web Security

Web security is unique to every environment; any application and service that the organization wants to deliver to the customer will have its own way of performing transactions. Static Web sites with little content or searchable areas of course pose the least risk, but they also offer the least functionality. Who wants a Web site they can't sell anything from? Implementing something like a shopping cart or content delivery on your site opens up new, unexpected aspects of Web security. Among the things that need to be considered are whether it is worth developing the application in-house or buying one off the shelf and rely on someone else for the maintenance ad patching. With some of these thoughts in mind, here are some of the biggest threats associated with having a public-facing Web site:

- Vandalism
- Financial fraud
- Privileged access

- Theft of transaction information
- Theft of intellectual property
- Denial-of-service (DoS) attacks
- Input validation errors
- Path or directory traversal
- Unicode encoding
- URL encoding

Some Web application defenses that can be implemented have already been discussed; they include

- Web application firewalls
- Intrusion prevention systems
- SYN proxies on the firewall

Application Security

An integrated approach to application security (see Figure 1.17) in the organization is required for successful deployment and secure maintenance of all applications.

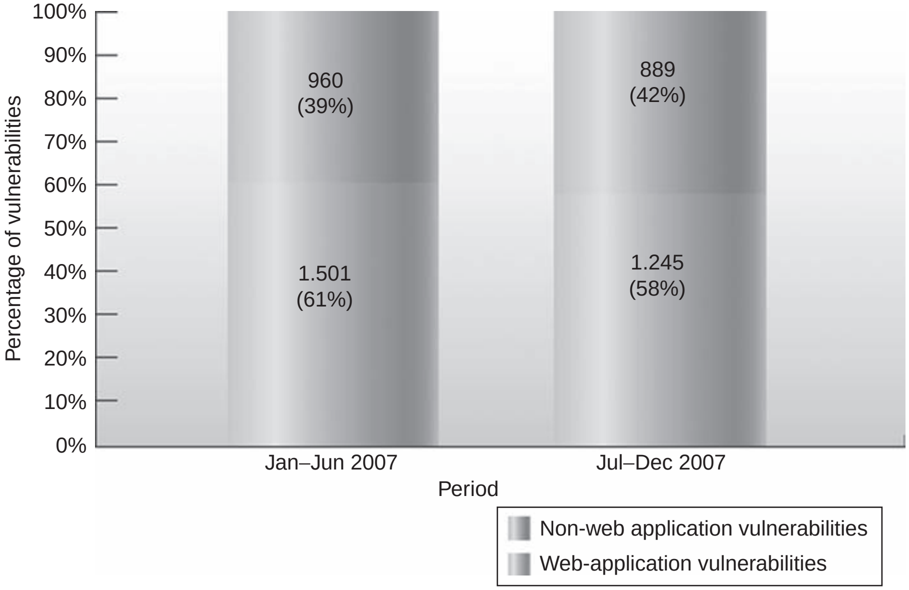


Figure 1.17: Symantec Web application vulnerabilities by share.

A corporate initiative to define, promote, assure, and measure the security of critical business applications would greatly enhance an organization's overall security. Some of the biggest obstacles, as mentioned in the previous section, are that security professionals are not typically developers, so this means that often application security is left to IT or R&D personnel, which can lead to gaping holes. Components of an application security program consist of [37].

- *People.* Security architects, managers, technical leads, developers, and testers.
- *Policy.* Integrate security steps into your SDLC and ADLC; have security baked in, not bolted on. Find security issues early so that they are easier and cheaper to fix. Measure compliance; are the processes working? Inventory and categorize your applications.
- *Standards.* Which controls are necessary, and when and why? Use standard methods to implement each control. Provide references on how to implement and define requirements.
- *Assessments.* Security architecture/design reviews, security code reviews, application vulnerability tests, risk acceptance review, external penetration test of production applications, white-box philosophy. Look inside the application, and use all the advantages you have such as past reviews, design documents, code, logs, interviews, and so on. Attackers have advantages over you; don't tie your hands.
- *Training.* Take awareness and training seriously. All developers should be performing their own input validation in their code and need to be made aware of the security risks involved in sending unsecure code into production.

Security Policies and Procedures

A quality information security program begins and ends with the correct information security policy (see Figure 1.18). Policies are the least expensive means of control and often the most difficult to implement.

An information security policy is a plan that influences and determines the actions taken by employees who are presented with a policy decision regarding information systems. Other components related to a security policy are practices, procedures, and guidelines, which attempt to explain in more detail the actions that are to be taken by employees in any given situation. For policies to be effective, they must be properly disseminated, read, understood, and agreed to by all employees as well as backed by upper management. Without upper management support, a security policy is bound to fail. Most information security policies should contain at least the following:

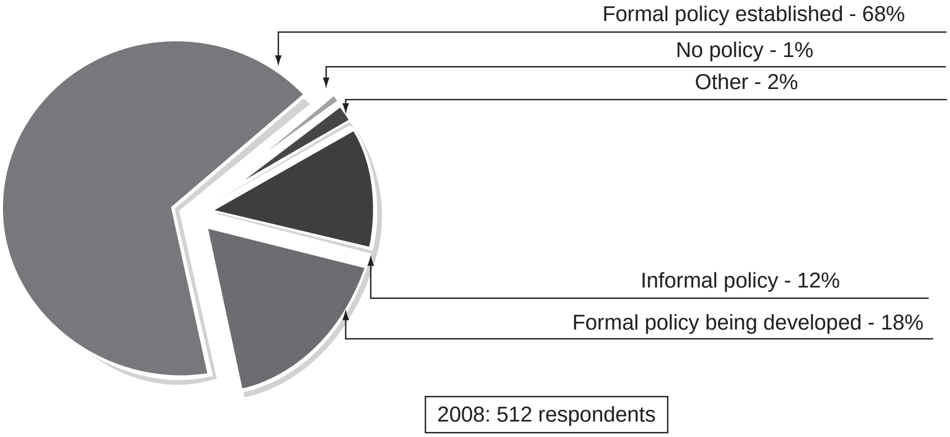


Figure 1.18: Information security policy within your organization, CSI/FBI report, 2008.

- An overview of the corporate philosophy on security
- Information about roles and responsibilities for security shared by all members of the organization
- Statement of purpose
- Information technology elements needed to define certain controls or decisions
- The organization's security responsibilities defining the security organization structure
- References to IT standards and guidelines, such as Government Policies and Guidelines, FISMA, http://iase.disa.mil/policy-guidance/index.html #FISMA and NIST Special Publications (800 Series), and http://csrc.nist.gov/publications/PubsSPs.html.

Some basic rules must be followed when you're shaping a policy:

- Never conflict with the local or federal law.
- Your policy should be able to stand up in court.
- It must be properly supported and administered by management.
- It should contribute to the success of the organization.
- It should involve end users of information systems from the beginning.

Security Employee Training and Awareness

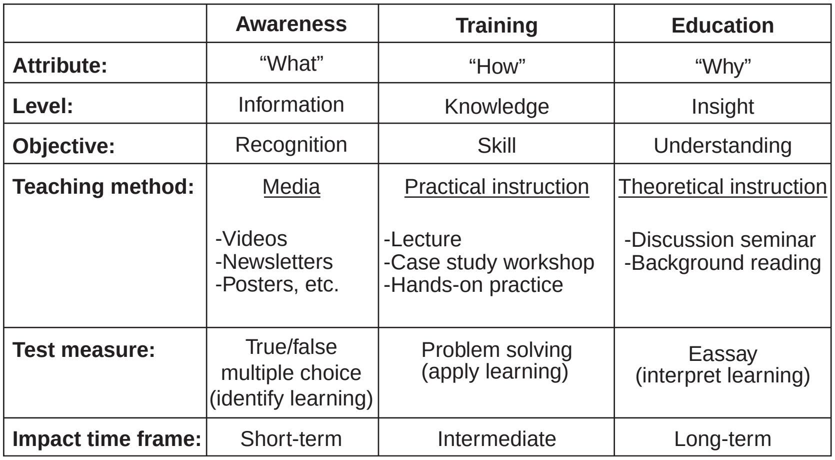
The Security Employee Training and Awareness (SETA) program is a critical component of the information security program. It is the vehicle for disseminating security information that the workforce, including managers, need to do their jobs. In terms of the total security solution, the importance of the workforce in achieving information security goals and the importance of training as a countermeasure cannot be overstated. Establishing and maintaining a robust and relevant information security awareness and training program as part of the overall information security program is the primary conduit for providing employees with the information and tools needed to protect an agency's vital information resources. These programs will ensure that personnel at all levels of the organization understand their information security responsibilities to properly use and protect the information and resources entrusted to them. Agencies that continually train their workforces in organizational security policy and role-based security responsibilities will have a higher rate of success in protecting information [38].

As cited in audit reports, periodicals, and conference presentations, people are arguably the weakest element in the security formula that is used to secure systems and networks. The people factor, not technology, is a critical one that is often overlooked in the security equation. It is for this reason that the Federal Information Security Management Act (FISMA) and the Office of Personnel Management (OPM) have mandated that more and better attention must be devoted to awareness activities and role-based training, since they are the only security controls that can minimize the inherent risk that results from the people who use, manage, operate, and maintain information systems and networks. Robust and enterprisewide awareness and training programs are needed to address this growing concern [39].

The 10 Commandments of SETA

The 10 Commandments of SETA consist of the following:

1. Information security is a people, rather than a technical, issue.
2. If you want them to understand, speak their language.
3. If they cannot see it, they will not learn it.
4. Make your point so that you can identify it and so can they.
5. Never lose your sense of humor.
6. Make your point, support it, and conclude it.
7. Always let the recipients know how the behavior that you request will affect them.
8. Ride the tame horses.
9. Formalize your training methodology.
10. Always be timely, even if it means slipping schedules to include urgent information.



	Awareness	Training	Education
Attribute:	"What"	"How"	"Why"
Level:	Information	Knowledge	Insight
Objective:	Recognition	Skill	Understanding
Teaching method:	Media -Videos -Newsletters -Posters, etc.	Practical instruction -Lecture -Case study workshop -Hands-on practice	Theoretical instruction -Discussion seminar -Background reading
Test measure:	True/false multiple choice (identify learning)	Problem solving (apply learning)	Eassay (interpret learning)
Impact time frame:	Short-term	Intermediate	Long-term

Figure 1.19: Matrix of security teaching methods and measures that can be implemented.

Depending on the level of targeted groups within the organization, the goal is first awareness, then training, and eventually the education of all users as to what is acceptable security. Figure 1.19 shows a matrix of teaching methods and measures that can be implemented at each level.

Targeting the right people and providing the right information are crucial when you're developing a security awareness program. Therefore, some of the items that must be kept in mind are focusing on people, not so much on technologies; refraining from using technical jargon; and using every available venue, such as newsletters or memos, online demonstrations, and in-person classroom sessions. By not overloading users and helping them understand their roles in information security, you can establish a program that is effective, identifies target audiences, and defines program scope, goals, and objectives. Figure 1.20 presents a snapshot according to the 2008 CSI/FBI Report, showing where the SETA program stands in 460 different U.S. organizations.

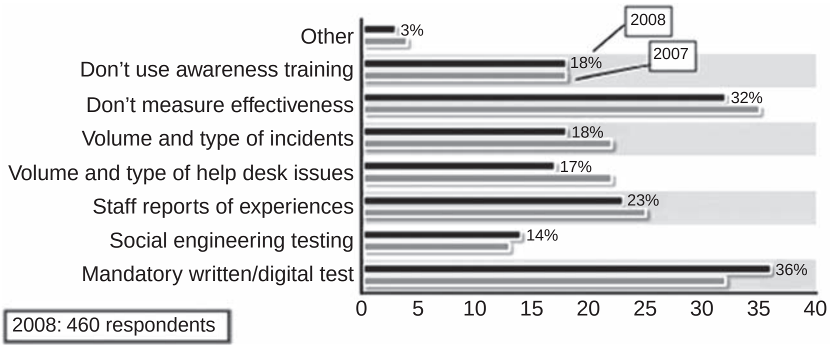


Figure 1.20: Awareness training metrics.

4. Security Monitoring and Effectiveness

Security monitoring and effectiveness are the next evolutions to a constant presence of security-aware personnel who actively monitor and research events in real time. A substantial number of suspicious events occur within most enterprise networks and computer systems every day and go completely undetected. Only with an effective security monitoring strategy, an incident response plan, and security validation and metrics in place will an optimal level of security be attained. The idea is to automate and correlate as much as possible between both events and vulnerabilities and to build intelligence into security tools so that they alert you if a known bad set of events has occurred or a known vulnerability is actually being attacked.

To come full circle: You need to define a security monitoring and log management strategy; an integrated incident response plan; validation and penetration exercises against security controls; and security metrics to help measure whether there has been improvement in your organization's handling of these issues.

Security Monitoring Mechanisms

Security monitoring involves real-time or near-real-time monitoring of events and activities happening on all your organization's important systems at all times. To properly monitor an organization for technical events that can lead to an incident or an investigation, usually an organization uses a security information and event management (SIEM) and/or log management tool. These tools are used by security analysts and managers to filter through tons of event data and to identify and focus on only the most interesting events.

Understanding the regulatory and forensic impact of event and alert data in any given enterprise takes planning and a thorough understanding of the quantity of data the system will be required to handle. The better logs can be stored, understood, and correlated, the better the possibility of detecting an incident in time for mitigation. In this case, what you don't know *will* hurt you. The need to respond to incidents, identify anomalous or unauthorized behavior, and secure intellectual property has never been more important. Without a solid log management strategy, it becomes nearly impossible to have the necessary data to perform a forensic investigation, and without monitoring tools, identifying threats and responding to attacks against confidentiality, integrity, or availability become much more difficult. For a network to be compliant and an incident response or forensics investigation to be successful, it is critical that a mechanism be in place to do the following:

- Securely acquire and store raw log data for as long as possible from as many disparate devices as possible while providing search and restore capabilities of these logs for analysis.
- Monitor interesting events coming from all important devices, systems, and applications in as near real time as possible.

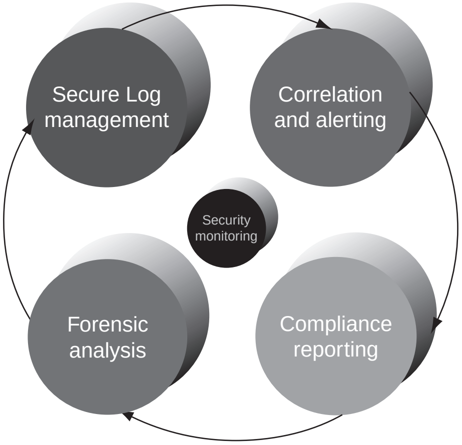


Figure 1.21: Security monitoring.

- Run regular vulnerability scans on your hosts and devices and correlate these vulnerabilities to intrusion detection alerts or other interesting events, identifying high-priority attacks as they happen and minimizing false positives.

SIEM and log management solutions in general can assist in security information monitoring (see Figure 1.21) as well as regulatory compliance and incident response by doing the following:

- Aggregating and normalizing event data from unrelated network devices, security devices, and application servers into usable information.
- Analyzing and correlating information from various sources such as vulnerability scanners, IDS/IPS, firewalls, servers, and so on, to identify attacks as soon as possible and help respond to intrusions more quickly.
- Conducting network forensic analysis on historical or real-time events through visualization and replay of events.
- Creating customized reports for better visualization of your organizational security posture.
- Increasing the value and performance of existing security devices by providing a consolidated event management and analysis platform.
- Improving the effectiveness and helping focus IT risk management personnel on the events that are important.
- Meeting regulatory compliance and forensics requirements by securely storing all event data on a network for long-term retention and enabling instant accessibility to archived data.

Incidence Response and Forensic Investigations

Network forensic investigation is the investigation and analysis of all the packets and events generated on any given network in the hope of identifying the proverbial needle in a haystack. Tightly related is incident response, which entails acting in a timely manner to an identified anomaly or attack across the system. To be successful, both network investigations and incident response rely heavily on proper event and log management techniques. Before an incident can be responded to, there is the challenge of determining whether an event is a routine system event or an actual incident. This requires that there be some framework for incident classification (the process of examining a possible incident and determining whether or not it requires a reaction). Initial reports from end users, intrusion detection systems, host- and network-based malware detection software, and system administrators are all ways to track and detect incident candidates [40].

As mentioned in earlier sections, the phases of an incident usually unfold in the following order: preparation, identification (detection), containment, eradication, recovery, and lessons learned. The preparation phase requires detailed understanding of information systems and the threats they face; so to perform proper planning, an organization must develop predefined responses that guide users through the steps needed to properly respond to an incident. Predefining incident responses enables rapid reaction without confusion or wasted time and effort, which can be crucial for the success of an incident response. Identification occurs once an actual incident has been confirmed and properly classified as an incident that requires action. At that point the IR team moves from identification to containment. In the containment phase, a number of action steps are taken by the IR team and others. These steps to respond to an incident must occur quickly and may occur concurrently, including notification of key personnel, the assignment of tasks, and documentation of the incident. Containment strategies focus on two tasks: first, stopping the incident from getting any worse, and second, recovering control of the system if it has been hijacked.

Once the incident has been contained and system control regained, eradication can begin, and the IR team must assess the full extent of damage to determine what must be done to restore the system. Immediate determination of the scope of the breach of confidentiality, integrity, and availability of information and information assets is called *incident damage assessment*. Those who document the damage must be trained to collect and preserve evidence in case the incident is part of a crime investigation or results in legal action.

At the moment that the extent of the damage has been determined, the recovery process begins to identify and resolve vulnerabilities that allowed the incident to occur in the first place. The IR team must address the issues found and determine whether they need to install and/or replace or upgrade the safeguards that failed to stop or limit the incident or were missing from the system in the first place. Finally, a discussion of lessons learned should always be conducted to prevent future similar incidents from occurring and review what could have been done differently [41].

Validating Security Effectiveness

The process of validating security effectiveness comprises making sure that the security controls that you have put in place are working as expected and that they are truly mitigating the risks they claim to be mitigating. There is no way to be sure that your network is not vulnerable to something if you haven't validated it yourself. The only way to have a concrete means of validation is to ensure that the information security policy addresses your organizational needs and assess compliance with your security policy across all systems, assets, applications, and people.

Here are some areas where actual validation should be performed; in other words, these are areas where assigned IT personnel should go with policy in hand, log in, and verify the settings and reports before the auditors do:

- Verifying operating system settings
- Reviewing security device configuration and management
- Establishing ongoing security tasks
- Maintaining physical security
- Auditing security logs
- Creating an approved product list
- Reviewing encryption strength
- Providing documentation and change control

Vulnerability Assessments and Penetration Tests

Validating security (see Figure 1.22) with internal as well as external vulnerability assessments and penetration tests is a good way to measure an increase or decrease in overall security, especially if similar assessments are conducted on a regular basis. There are several ways to test security of applications, hosts, and network devices. With a vulnerability assessment, usually limited scanning tools or just one scanning tool is used to determine vulnerabilities that exist in the target system. Then a report is created and the manager reviews a holistic picture of security. With authorized penetration tests, the process is a little different. In that case, the data owner is allowing someone to use just about any means within reason (in other words, many different tools and techniques) to gain access to the system or information. A successful penetration test does not provide the remediation avenues that a vulnerability assessment does; rather, it is a good test of how difficult it would be for someone to truly gain access if he were trying.

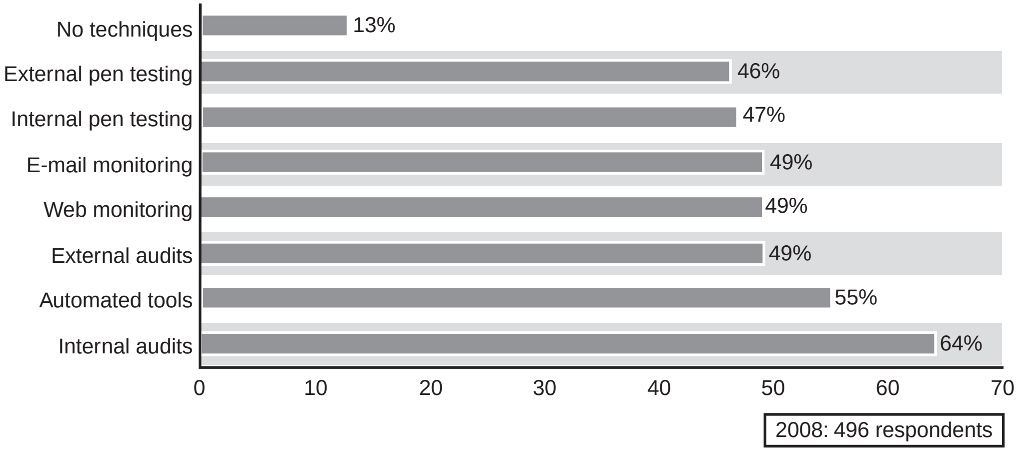


Figure 1.22: Security validation techniques, CSI/FBI survey, 2008.

Further Reading

[1] Richardson R, CSI Director. CSI Computer Crime & Security Survey, CSI Web site, http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf; 2008.

[2] 45 C.F.R. § 164.310 Physical safeguards, Justia Web site, http://law.justia.com/us/cfr/title45/45-1.0.1.3.70.3.33.5.html.

[3] Saleh AlAboodi A. A New Approach for Assessing the Maturity of Information Security, CISSP; www.isaca.org/Template.cfm?Section5Home&CONTENTID534805&TEMPLATE5/ContentManagement/ContentDisplay.cfm.

[4] Jaquith A. Security Metrics: Replacing Fear, Uncertainty and Doubt. Addison-Wesley; 2007.

[5] AppSec2005DC-Anthony Canike-Enterprise AppSec Program PowerPoint Presentation. OWASP; www.owasp.org/index.php/Image:AppSec2005DC-Anthony_Canike-Enterprise_AppSec_Program.ppt.

[6] CISSP 10 Domains ISC2 Web site, https://www.isc2.org/cissp/default.aspx.

[7] Cloud Computing: The Enterprise Cloud, Terremark Worldwide Inc. Web site, www.theenterprisecloud.com/.

[8] Defense in Depth: A Practical Strategy for Achieving Information Assurance in Today’s Highly Networked Environments. National Security Agency, Information Assurance Solutions Group – STE 6737.

[9] Definition of Defense in Depth. OWASP Web site, www.owasp.org/index.php/Defense_in_depth.

[10] Definition of Information Security, Wikipedia, http://en.wikipedia.org/wiki/Information_security.

[11] GSEC. GIAC Security Essentials Outline. SANS Institute; https://www.sans.org/training/description.php?tid.

[12] ISO 17799 Security Standards. ISO Web site, https://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm.

[13] Whitman ME, Mattord HJ. Management of Information Security, Course Technology; 2007 March 27, 2nd ed.

[14] Krause M, Tipton H.F. Information Security Management Handbook. 6th ed. Auerbach Publications, CRC Press LLC.

[15] Scarfone K, Mell P. NIST Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS), Recommendations of the National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf.

[16] Frankel Bernard S, Owens EL, Scarfone K. NIST Special Publication 800-97: Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, Recommendations of the National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf.
[17] Bowen P, Hash J, Wilson M. NIST Special Publication 800-100: Information Security Handbook: A Guide for Managers, Recommendations of the National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf.
[18] Caralli RA, Wilson WR. the Survivable Enterprise Management Team. The Challenges of Security Management, Networked Systems Survivability Program. Software Engineering Institute, www.cert.org/archive/pdf/ESMchallenges.pdf.
[19] Harris S. All in One CISSP Certification Exam Guide. 4th ed. McGraw Hill.
[20] Symantec Global Internet Security Threat Report, Trends for July–December 2007, vol. XII. Symantec Web site: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf; April 2008.
[21] Galway L. Quantitative Risk Analysis for Project Management, A Critical Review, WR-112-RC, Rand.org Web site, www.rand.org/pubs/working_papers/2004/RAND_WR112.pdf; February 2004.

References

[1] Cloud computing, the enterprise cloud. Terremark Worldwide Inc., Web site, http://www.theenterprisecloud.com/
[2] Definition of information security. Wikipedia, http://en.wikipedia.org/wiki/Information_security
[3] Caralli RA, Wilson WR. The challenges of security management, Survivable Enterprise Management Team, Networked Systems Survivability Program, Software Engineering Institute, http://www.cert.org/archive/pdf/ESMchallenges.pdf
[4] CISSP Ten domains. ISC2 Web site, https://www.isc2.org/cissp/default.aspx
[5] Krause M, Tipton HF. Information Security Management Handbook. 6th ed. CRC Press LLC
[6] ISO 17799 security standards. ISO Web site, http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm
[7] Saleh Al Aboodi S. A New Approach for Assessing the Maturity of Information Security. CISSP.
[8] ISO 17799 security standards. ISO Web site, http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm
[9] Reference not available.
[10] Symantec Global Internet, Security Threat Report, Trends for July–December 07, vol. XII. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf; Published April 2008.
[11] Richardson R. 2008 CSI Computer Crime & Security Survey (The latest results from the longest-running project of its kind), http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf
[12] Richardson R. 2008 CSI Computer Crime & Security Survey (The latest results from the longest-running project of its kind), http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf
[13] Richardson R. 2008 CSI Computer Crime & Security Survey (The latest results from the longest-running project of its kind), http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf
[14] Richardson R. 2008 CSI Computer Crime & Security Survey (The latest results from the longest-running project of its kind), http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf
[15] Richardson R. 2008 CSI Computer Crime & Security Survey (The latest results from the longest-running project of its kind), http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf
[16] Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments. National Security Agency, Information Assurance Solutions Group – STE 6737.
[17] Harris S. All in One CISSP Certification Exam Guide. 4th ed. McGraw Hill Companies.

[18] Galway L. Quantitative Risk Analysis for Project Management, A Critical Review, WR-112-RC, http://www.rand.org/pubs/working_papers/2004/RAND_WR112.pdf; February 2004.

[19] OWASP Definition of Defense in Depth, http://www.owasp.org/index.php/Defense_in_depth.

[20] Whitman ME, Mattord HJ. Management of Information Security. 2nd ed. Course Technology; 2007 March 27.

[21] Whitman ME, Mattord HJ. Management of Information Security. 2nd ed. Course Technology; 2007 March 27.

[22] Whitman ME, Mattord HJ. Management of Information Security. 2nd ed. Course Technology; 2007 March 27.

[23] Whitman ME, Mattord HJ. Management of Information Security. 2nd ed. Course Technology; 2007 March 27.

[24] 45 C.F.R. § 164.310 Physical safeguards, http://law.justia.com/us/cfr/title45/45-1.0.1.3.70.3.33.5.html

[25] 45 C.F.R. § 164.310 Physical safeguards, http://law.justia.com/us/cfr/title45/45-1.0.1.3.70.3.33.5.html

[26] 45 C.F.R. § 164.310 Physical safeguards, http://law.justia.com/us/cfr/title45/45-1.0.1.3.70.3.33.5.html

[27] GSEC. GIAC Security Essentials Outline. SANS Institute, www.sans.org/training/description.php?tid=672

[28] Scarfone K, Mell P. NIST Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS). Recommendations of the National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

[29] Frankel S, Eydt B, Owens L, Scarfone K. NIST Special Publication 800-97: Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. Recommendations of the National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf

[30] Frankel S, Eydt B, Owens L, Scarfone K. NIST Special Publication 800-97: Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. Recommendations of the National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf

[31] Frankel S, Eydt B, Owens L, Scarfone K. NIST Special Publication 800-97: Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. Recommendations of the National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf

[32] Frankel S, Eydt B, Owens L, Scarfone K. NIST Special Publication 800-97: Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. Recommendations of the National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf

[33] Frankel S, Eydt B, Owens L, Scarfone K. NIST Special Publication 800-97: Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. Recommendations of the National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf

[34] Frankel S, Eydt B, Owens L, Scarfone K. NIST Special Publication 800-97: Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. Recommendations of the National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf

[35] Frankel S, Eydt B, Owens L, Scarfone K. NIST Special Publication 800-97: Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. Recommendations of the National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf

[36] Frankel S, Eydt B, Owens L, Scarfone K. NIST Special Publication 800-97: Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. Recommendations of the National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf

[37] AppSec2005DC-Anthony Canike-Enterprise AppSec Program PowerPoint Presentation. OWASP. http://www.owasp.org/index.php/Image:AppSec2005DC-Anthony_Canike-Enterprise_AppSec_Program.ppt

[38] Bowen P, Hash J, Wilson M. NIST Special Publication 800-100: Information Security Handbook: A Guide for Managers. Recommendations of the National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

[39] Bowen P, Hash J, Wilson M. NIST Special Publication 800-100: Information Security Handbook: A Guide for Managers. Recommendations of the National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

[40] Whitman ME, Mattord HJ. Management of Information Security. 2nd ed. Course Technology; 2007 March 27.

[41] Whitman ME, Mattord HJ. Management of Information Security. 2nd ed. Course Technology; 2007 March 27.