1

WHAT IS SECURITY?

1.1 INTRODUCTION

The central role of computer security for the working of the economy, the defense of the country, and the protection of our individual privacy is universally acknowledged today. This is a relatively recent development; it has resulted from the rapid deployment of Internet technologies in all fields of human endeavor and throughout the world that started at the beginning of the 1990s. Mainframe computers have handled secret military information and personal computers have stored private data from the very beginning of their existence in the mid-1940s and 1980s, respectively. However, security was not a crucial issue in either case: the information could mostly be protected in the old-fashioned way, by physically locking up the computer and checking the trustworthiness of the people who worked on it through background checks and screening procedures. What has radically changed and made the physical and administrative approaches to computer security insufficient is the interconnectedness of computers and information systems. Highly sensitive economic, financial, military, and personal information is stored and processed in a global network that spans countries, governments, businesses, organizations, and individuals. Securing this cyberspace is synonymous with securing the normal functioning of our daily lives.

Engineering Information Security: The Application of Systems Engineering Concepts to Achieve Information Assurance, Second Edition. Stuart Jacobs.
© 2016 by The Institute of Electrical and Electronics Engineers, Inc. Published 2016 by John Wiley & Sons, Inc.
Companion Website: www.wiley.com/go/informationsecurity2jacobs

Secure information systems must work reliably despite random errors, disturbances, and malicious attacks. Mechanisms incorporating security measures are not just hard to design and implement but can also backfire by decreasing efficiency, sometimes to the point of making the system unusable. This is why some programmers used to look at security mechanisms as an unfortunate nuisance; they require more work, do not add new functionality, and slow down the application and thus decrease usability. The situation is similar when adding security at the hardware, network, or organizational level: increased security makes the system clumsier and less fun to use; just think of the current airport security checks and contrast them to the happy (and now so distant) pre–September 11, 2001 memories of buying your ticket right before boarding the plane. Nonetheless, systems must work, and they must be secure; thus, there is a fine balance to maintain between the level of security on one side and the efficiency and usability of the system on the other. One can argue that there are three key attributes of information systems:

1. Processing capacity—speed
2. Convenience—user friendliness
3. Secure—reliable operation

The process of securing these systems is finding an acceptable balance of these attributes.

1.2 THE SUBJECT OF SECURITY

Security is a word used to refer to many things, so its use has become somewhat ambiguous. Here we will try to clarify just what security focuses on. Over the years, the subject of information security has been considered from a number of perspectives, as a concept, a function, and a subject area. We will discuss each of these perspectives and examine their value.

1.2.1 Branches of Security

A concept approach treats security as a set of related activity areas, or branches. Figure 1.1 shows the security-related areas typically considered. Note that all the areas are mutually dependent on each other. Within Figure 1.1, the rings do not define a hierarchy among the different areas of security. The rings are meant to express a layered approach to achieving cost-effective information security.

Each security area focuses on a specific need to erect a barrier against inappropriate use of, or access to, the assets (information, capabilities, property, equipment, personnel, processes, etc.) considered valuable to an organization. Since there are now multiple avenues (approaches) by which assets can be targeted, multiple security area activities are necessary. Physical security capabilities are necessary to control physical access to:

- buildings, rooms, and offices;
- equipment used for processing, storing, transferring, or accessing information; and

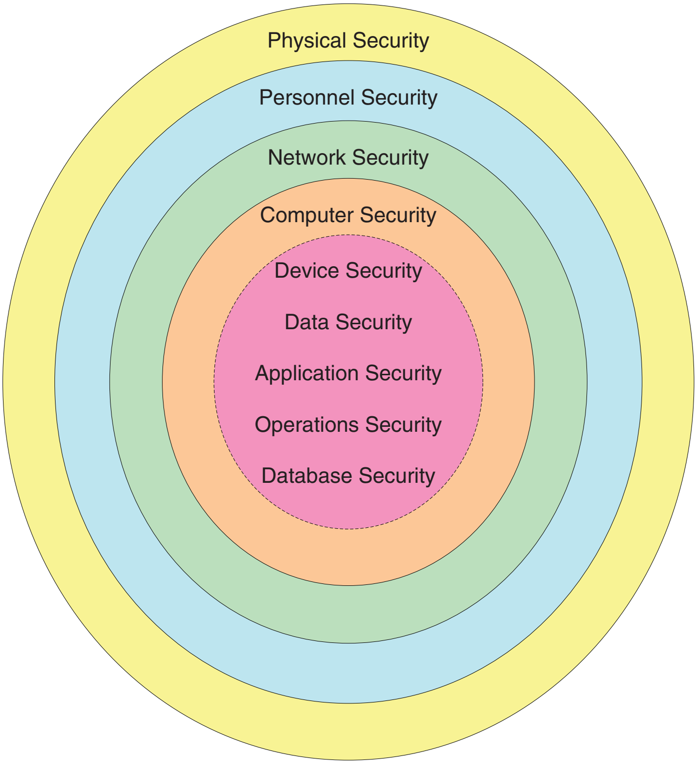


Figure 1.1. Areas of security

- the cables used for communicating information between facilities, buildings, and even between individual systems within a building, floor, or rooms.

Personnel security processes and procedures are necessary to:

- ensure that an organization's employees have been accurate in representing who they are and that academic or professional credentials and past experience are valid;
- verify the identities and validate the reasons for nonemployee (guests, visitors, service/supply personnel) access to the organization's facilities or other assets;
- ensure that the organization's security-related policies and procedures conform to legal constrains for employment, document disciplinary activities, and conditions for termination of employment; and
- inform both new and continuing employees as to what the organization considers necessary, acceptable, and unacceptable behavior.

Network security technology, processes, and procedures are necessary to ensure that:

- data transferred between networked devices is adequately protected from tampering, misuse, or destruction;
- networked devices are appropriately managed, monitored, and utilized; and
- networking resources are used only for acceptable activities.

Computer security spans all aspects of computing equipment hardware, software, usage, and administration (e.g., device, data, applications/operating systems, operations, and database subareas), and is necessary to ensure that they are:

- adequately protected from tampering, misuse, or destruction;
- appropriately managed and monitored;
- utilized for organization sanctioned activities and purposes; and
- available to support organization activities, processes, and functions.

Frequently, security discussions focus primarily on networks, their links and interconnecting equipment, and on securing operating systems and applications. However, providing network security is just not enough. Attackers can leverage other weaknesses to bypass the network security mechanisms in place. Network and computer security both need to be considered along with the other branches of security. The reader needs to remember that the term "information security" is generally used to refer to concepts, mechanisms, activities, and objectives that span all of the security areas mentioned above.

Regardless of what security area/branch is under discussion, the following three views of security measures can be applied to any situation: *defense*, *deterrence*, and *detection*. These are known as the three *D*s of security.

- *Defense*—protect assets first. Network areas should be analyzed before adopting any protective efforts. Defense measures reduce the likelihood of an attack and lessen the risk of damage. Lack of defensive measures will leave sensitive information exposed and lead to losses. For example, installing a firewall is a good defensive measure. But, this may not be enough. The other two modes of security—deterrence and detection—should not be ignored.
- *Deterrence*—reduce the frequency of security compromises. With deterrence mechanisms and policies in place, attackers have to expend more effort, and thus risk discovery. Deterrence policies within an organization are enforced by using threats of discipline and termination of the employee if any company policies are violated (email, web browsing, etc.) Entering a computer network without company authorization is illegal, and laws are in place to prosecute and punish intruders. Intruders who know that their activities are being monitored will likely think twice before attacking a system.

- *Detection*—sound the alarm. Unfortunately, in practice, security control is the least implemented policy and often neglected. When security is violated, without security enforcers in place, the security breach could go unnoticed for a long time.

Each of the three *D*s is important and complements the others. A security program that spans all three *D* categories provides strong protection. The following are examples of how each strategy can be implemented:

- *Defensive controls*—firewalls, access lists in routers, spam filters, virus filters, etc.
- *Deterrent controls*—email messages to employees, posting of Internet sites visited, display of IP addresses to external visitors, etc.
- *Detective controls*—audit trails, log files, intrusion detection systems, summary reports, etc.

1.2.2 Defining Security by Function

Alternatively, security can be categorized under the following functional areas:

- Risk avoidance
- Deterrence
- Prevention
- Detection
- Recovery

1.2.2.1 Risk Avoidance. An enterprise should do a risk assessment that identifies what value and risk each component has to the system in whole and include strategies that reduce the likelihood of behavior/activity that can be damaging. Risk avoidance covers consideration of which components are required and which are optional. Components include hardware, services, processes, and applications. The components should be documented, reviewed, and the assessments of their value and risk accepted by all parties in the organization.

1.2.2.2 Deterrence. Deterrence is a common method of control used by governments, businesses, and individuals to cause people to think twice before performing an action. For example, a person's actions could be manipulated by the negative motivational influence with displaying a message, such as

> Your IP address 132.208.213.4 has been recorded and all activity is subject to monitoring and logging. Unauthorized access is subject to civil and criminal prosecution.

when any unauthorized person logs into a server or accesses a system. The individual may then reconsider proceeding further. There are, of course, individuals who will not comply, and this mechanism will not deter a worm, virus, or an automated attacker. Nevertheless, such notice at least informs an intruder that further activity is comparable to trespassing. Posting such a notice is a component, but not the sole component, of an organization's effort at ensuring "due diligence." Due diligence is a concept that applies in both civil and criminal contexts. In the civil litigation arena, due diligence refers to the effort made by a prudent or reasonable party to avoid harm to another party, and failure to make this effort could be considered negligence. In the criminal arena, due diligence is an available defense to a crime; however, defendants must prove beyond a reasonable doubt that they took every reasonable precaution.[1]

1.2.2.3 Prevention. From a business perspective, there is no product, or set of products, that will completely eliminate the chance of a security-related incident. There are two obvious explanations for this:

- The expense of such a set of products, and their likely negative impact(s) on operational usefulness and life-cycle costs, will undoubtedly outweigh the economic damages suffered from the loss(es) caused by an incident. Unless a cost–benefit analysis is performed, more money may be expended to protect an asset than is justified by the asset's value. For example, it does not make economic sense to spend $10,000,000 to protect an asset with a replacement cost of $1,000,000.
- Business systems routinely interact with humans who may have motives contrary to an organization's interests. Humans are the least dependable component in any system dedicated to ensuring the security of an organization's assets. History is full of examples where "highly trusted" people engaged in unauthorized, even criminal, activities.

There are certain situations where a security-related incident can result in the loss of life or equivalent harm. Law enforcement organizations, branches of the military, and other governmental and nongovernmental groups work under such circumstances. The security breaches the military, security, and law enforcement type of organizations face are frequently measured in people dying. This type of loss cannot be considered acceptable at any cost, and consequently what the community considers affordable becomes a social/political issue as to priorities, philosophy, and ethics.

However, most mishaps can be prevented by employing both procedural and technical security mechanisms that enforce authentication, authorization, confidentiality, and integrity based on well-thought out planning. Procedural mechanisms encompass understanding what needs protection, who needs access, who is responsible for different

[1] This observation is not intended to provide the reader with legal advice. The reader should consult legal counsel regarding civil or criminal issues.

things, and what management and administrative responsibilities need to be considered. Procedural mechanisms can include separation of duties, mandated auditing, and separation of operational from development environments. Technical mechanisms include deploying packet filtering, strong authentication, encryption, virus prevention, malicious code filtering, and so forth. Each product provides a degree of protection and, when deployed in combination, can provide cost-effective layers of protection.

1.2.2.4 Detection. Despite the best prevention measures, a system is prone to be attacked[2] at some time. Measures should be in place to detect and record the presence and activities of not just the suspected attacker, but any administrative personnel, service users, subscribers, or customers as the conditions change. Most organizations are allowed by law to monitor activity within their networks for maintenance purposes. Commercial organizations may control any activity within their internal networks. Telecommunications service providers (TSPs) who offer telephone (telecommunications) services and web/data (information) services to the general public are also required to support law enforcement organizations/agencies (LEOs) in “wire-taps” and “intercepts” of criminal suspects. Organizations, both large and small, should make use of intrusion detection (IDS) mechanisms, auditing and log analysis, virus/spy/malware scanners, and file-monitoring programs.

1.2.2.5 Recovery. Recovery considers how an organization is able to perform its primary functions and operations even in the face of natural or human-created situations. This area has been typically referred to as “disaster recovery” although the term “business continuity” is becoming more common today. Unfortunately, business continuity planning too frequently focuses primarily on natural disasters. Human-created situations, including security-oriented attacks, necessitate consideration in any business continuity plan. A physical recovery plan is important. Such a plan should include a solid backup and recovery system, procedures for secure off-site storage, contact lists, and so forth. Some plans should have a section dealing with business continuity using such mechanisms as geographic facility and system redundancy, redundant links and servers, and distributed load-sharing implementations. A logical recovery plan should include discussion of how to restore organizational capabilities even when some form of security-related attack is occurring. Planning for these situations needs to consider how:

- assets under attack can be isolated from “healthy” enterprise resources, thereby limiting the scope of an attack and minimizing the extent of damage or loss;
- services or functions remain available to legitimate users while an attack is occurring; and
- damaged or destroyed assets will be restored upon cessation of an attack.

[2] The term “attack” here is used to refer to some action by a human, or initiated by a human, that is *intended* to cause some form of damage or loss to assets of an organization. A key component of what constitutes an attack is motivation. The author does not consider an unintentional act to constitute an attack, even though such act or action may increase the likelihood of an attack occurring.

1.2.3 The Common Body of Knowledge (CBK) Security Domains

Over 20 years ago, many organizations recognized that geographically distributed interconnected systems were much more vulnerable than mainframe systems with minimal connectivity. At that time, few educational institutions offered any form of information security curricula, let alone academic degrees. This deficiency led to the establishment of the International Information Systems Security Certification Consortium (ISC)^2, a nonprofit organization with the purpose of educating and certifying information security professionals. (ISC)^2 certifications are based on a compendium of information security topics called the "common body of knowledge" (CBK). The CBK is the critical body of knowledge that serves as a common framework of security concepts, definitions, and principles that foster understanding of best practices among those engaged in activities related to information assurance/security.

The CBK categorizes security issues in terms of its elements in the following domains (areas):

- Access control systems and methodology
- Applications and systems development security
- Business continuity planning and disaster recovery planning
- Cryptography
- Information security and risk management
- Legal, regulations, compliance, and investigations
- Operations security
- Physical security
- Security architecture and models
- Telecommunications and network security

Confidentiality, integrity, and availability (CIA) are the core tenets of information security and are widespread over all the domains of the Common Body of Knowledge. *Confidentiality* is the measure of the secrecy of information. An organization determines how data are to be used and assigns a confidentiality level to that data. If transmitted from one place to the other, it ensures that the data were not observed by those who are not entitled to know about those contents. *Integrity* ensures that the information is accurate and reliable. If transmitted from one place to the other, it ensures that the data were not tampered with. *Availability* deals with the ability of users to access the information. It is commonly achieved through access control systems, redundant links and servers, and also with policies that take natural disasters into consideration.

1.2.3.1 Access Control Systems and Methodology. By the CBK definition, access control refers to a collection of mechanisms that allow the user/administrator of a system to have a directing or restraining influence over the behavior, use, and content of the system. Consequently, access controls are enforcement mechanisms that determine whether an action is authorized to occur. Access control methods determine what a user can access in the system. User's actions can be monitored for accountability. There are two main types of access control methods:

- *Discretionary access control (DAC)*—the access control decision is made by the individual user. For example, the user creates a file and defines an access control list specifying who can access the file and how much access (read, write, etc.) each user can have.
- *Mandatory access control (MAC*)—access control is imposed by categorizing resources and users based on a predetermined set of established criteria. For example, in military and government organizations dealing with sensitive data, the users and resources may be organized into the following categories: unclassified, confidential, secret, and top secret.

Based on these two broad types of access control, several methods have been developed to make them more comprehensive. Some of these are:

- *Lattice based*—defines the relationships within a MAC system. Usually, groups exist within each category and the access control method determines how control flows from one group to the other.
- *Rule based*—again a MAC-based system that uses a strict set of rules but requires a lot of management and administration.
- *Role based*—a MAC-based system where various roles are defined and users assigned to these roles. Permissions are now based on the job roles rather than by specific user. Examples of roles include system administrators, backup operators, and printer managers.
- *Access control list (ACL)*—often used to define rules in firewalls and routers based on IP addresses. Also used by some operating systems to define the access allowed by users to resources.

The CBK access control domain not only focuses on access control mechanisms, but also includes:

- identification and authentication mechanisms and techniques,
- administration of access control mechanisms, and
- mechanisms/methods for attacking information systems.

1.2.3.2 Application and Systems Development Security. By the CBK definition, this domain refers to the controls that are included within systems and applications software in centralized and distributed environments and the steps used in their development. Applications are vulnerable through buffer overflow attacks, cross-site attacks, SQL injection attacks, and so forth. Software security should be considered at the beginning of the design and implementation phases. Developers should understand how to produce secure, stable, and efficient software that is not vulnerable to known common types of attacks. Development projects, being under time pressure, often overlook these security aspects. This domain educates programmers and users about these inherent threats that their developed applications could face at a later time.

The CBK Application and Systems Development Security domain not only focuses on system internal security mechanisms, but also includes:

- data warehousing and data mining,
- risks associated with various software development practices,
- vulnerabilities within software components, and
- malicious software used for attacking information systems.

1.2.3.3 Business Continuity Planning and Disaster Recovery Planning. This domain addresses the continuation of the business in the event of a major disruption to normal business operations. In the event of a natural disaster or a major calamity, the entire company's resources could be lost. Whether the company survives or not depends on how the company prepares for these types of events. Having a *disaster recovery plan* determines what is required to keep the business functioning. These items should be prepared ahead of time and the procedures required to get the necessary data back online should be thought of. This plan is a short-term plan. Its objectives include:

- protecting the organization from major systems failure,
- minimizing the risk to the organization from delays in providing services,
- guaranteeing the reliability of standby systems through testing and simulation, and
- minimizing the decision-making required by personnel during a disaster.

The *business continuity plan* is a long-term plan that looks at recovery from beginning to end. It incorporates the disaster recovery plan and put into action when a threat occurs. It is essential to keep the recovery plans up to date, monitor critical assets, and so forth. This helps reduce damage in the long run. The major components of this process are:

- Scope and plan initiation—to create the scope and define the parameters of the plan.
- Business impact assessment—to understand the impact of a disruptive event.
- Business continuity plan development—include plan implementation, testing, and maintenance.

Plan approval and implementation is another component that involves getting the plan approved and making people aware of the plan. Also important is implementing a maintenance procedure for updating the plan as needed.

1.2.3.4 Cryptography. By the CBK definition, this domain addresses the principles, means, and methods of disguising information to ensure its integrity, confidentiality, and authenticity. Data are encrypted and validated to ensure that the data remain secure and intact. Only authorized people can access the encrypted data through the process of decryption. Cryptography can also provide nonrepudiation (irrefutable proof that a message was created by a given person). Two types of encryption exist:

- *Symmetric encryption*—uses a shared key to both encrypt and decrypt the data.
- *Asymmetric encryption*—uses two keys, a public key and a corresponding private key. Before data are transmitted, the data are encrypted with the recipient's public key. The encrypted data can only be decrypted with the recipient's private key.

The CBK Cryptography domain not only focuses on system internal security mechanisms, but also includes:

- infrastructures for the management of public keys allowing individuals to obtain valid keys and know when keys are no longer valid,
- risks associated with various encryption algorithms and how they may be deployed, and
- techniques for attacking the use of cryptography.

1.2.3.5 Information Security and Risk Management. This domain is concerned with the identification of an organization's information assets and the development, documentation, and implementation of policies, standards, procedures, and guidelines that ensure confidentiality, integrity, and availability. Management tools such as data classification, risk assessment, and risk analysis are used to identify the threats, classify them, and consider asset vulnerabilities so that effective security controls can be implemented. This domain also includes personnel security, training, and security awareness. The organization needs to determine the items to be protected, see how they are accessed, and then select controls, and audit the users who operate the devices.

What are the threats to our infrastructure, and what is at risk? Consider the confidentiality, integrity, and availability tenets of security. Any physical damage or interruptions in providing system services affect availability. Unauthorized disclosure of information breaches confidentiality. Any loss of control over the system compromises integrity. If there is a theft, it affects all the three aspects mentioned above.

1.2.3.6 Legal, Regulations, Compliance, and Investigations. By the CBK definition, this domain addresses computer crime laws and regulations, investigative measures and techniques that can be used if a crime is committed, methods to gather evidence, and the ethical issues and code of conduct for security professionals. Intruders can access private data, destroy information, steal intellectual property, and so forth. The owner of the system should report the crime, making sure that no evidence is destroyed or lost. Federal, state, or civil laws may be applicable depending on the crime committed. Even if the attacker is identified, it is important not to attack the attacker. Attacking an attacker is considered illegal by many nations and should not be engaged in.

Computer forensics is the field of computer crime investigation and deals with the collection of information from computer systems that will be admissible in courts of law. Gathering, control, storage, and preservation of evidence are crucial. The evidence must be relevant, legally permissible, reliable, properly identified, and preserved to be admissible. Legal evidence can be classified into the following types:

- *Best evidence*—original or primary evidence rather than a copy.
- *Secondary evidence*—copy of the evidence.
- *Direct evidence*—information gathered through a witness.
- *Conclusive evidence*—incontrovertible evidence.
- *Expert opinion.*
- *Circumstantial evidence*—inference of information from other facts.
- *Hearsay evidence*—computer-generated records.

Incident planning addresses the handling of malicious attacks through technical means and should address the following questions:

- What is the incident?
- How should it be reported?
- To whom it should be reported?
- When should management be informed of the incident?
- What action to take if an incident is detected?
- Who handles the response to an incident?
- How much damage was caused by the incident?
- What information was damaged or compromised by the incident?
- How are follow-up and review after the incident handled?
- What additional safeguards can be instituted as a result?

This CBK domain also includes consideration of software licensing and software piracy along with import–export laws and issues.

1.2.3.7 Operations Security. This domain identifies the controls over hardware, software, and information, and operations personnel with access privileges to any of these resources. Auditing and monitoring mechanisms are used to identify security events and report the information appropriately. To build a defensive system, put yourself in your opponent's place and see where the vulnerabilities are. Determine the resources that need to be protected and the privileges that need to be restricted. The following key principles have to be considered: identifying critical information, analyzing threats, assessing vulnerabilities and risks, and applying countermeasures. Operations Security uses indicators collected via log files, auditing, monitoring, and the like. Other sources of information gathering come from intrusion detection programs where administrators can look for anomalies. Penetration testing can also be utilized that play the role of an attacker to find a way into the system.

The operations security controls are categorized as follows:

- *Preventative controls*—to lower the impact of unintentional errors on the system and prevent unauthorized access to the system.
- *Detective controls*—to detect errors once they occur.
- *Corrective controls*—to mitigate any loss through data recovery procedures.
- *Recovery controls*—to allow restoration of operational capabilities during, or after, the occurrence of a security breach.

Monitoring and auditing are an integral part of operations security. Monitoring includes scrutinizing for illegal software installation, for hardware faults, and for anomalies. Monitoring tools are used for intrusion detection, penetration testing, and violation analysis. Auditing allows the review of patterns of access, discovery of any attempts to bypass the protection mechanisms, and security controls.

Another critical part of this domain is the maintenance of antivirus, and other anti-malware capabilities, personnel training, and resource protection activities. Security and fault tolerance technologies are included, along with security standards, operational compliance to regulations, and the concept of due diligence (also referred to as due care).

1.2.3.8 Physical Security. This domain addresses countermeasures that can be utilized to physically protect organization's resources and sensitive information from physical threats. Protecting from remote intruders is just not enough. Steps must be taken to protect assets that can be accessed physically. Examples of threats to physical security include emergencies (fire, building damage, utility loss, water damage, etc.), natural disasters (earthquakes, floods, etc.), and human intervention (sabotage, vandalism, etc.).

Controls for physical security include administrative controls and physical and technical controls. Administrative controls involve facility requirements planning, facility security management, and administrative personnel controls. Facility requirements planning deals with the planning for physical security controls in the early stages of the site construction, for example, choosing and designing a secure site. Audit trails and emergency procedures fall under facility security management. Administrative personnel controls include pre-employment screening, ongoing employee checks, and post-employment procedures. Environmental and life safety controls are required to sustain the personnel's or computer's operating environment, and these include power, fire detection, heating, ventilation, air conditioning, and the like.

Physical and technical controls relate to the areas of facility control requirements, access control devices, intrusion detection and alarms, inventory control, and media storage requirements. Storage media should be properly destroyed when no longer needed. Formatting a disk once doesn't destroy all the data and the disk should be overwritten or formatted at least seven times to conform to object reuse standards.

1.2.3.9 Security Architecture and Models. By the CBK definition, this domain spans the concepts, principles, structures, and standards used to design, implement, monitor, and secure operating systems, equipment, networks, and applications, including the controls used to enforce various levels of confidentiality, integrity, and availability. Some of the architectural models that define information security are:

- *Bell–LaPadula model*—defines security through confidentiality and is designed using a *no write down, no read up* approach. This model maintains security through classification levels. Subjects are allowed access to a classified object only if their clearance is at that level or higher.
- *Biba model*—focuses on the integrity of data and is designed using a *no write up, no read down* approach. This model is based on the trust relations that exist between subjects and objects and ensures that no subject can depend on a less trustworthy object.
- *Clark–Wilson model*—enforces data integrity for commercial applications. The model ensures that the data modifications made are consistent and done with well-formed transactions. This model also addresses the case where a computer crash occurs as data are being modified. In such a case, the system should roll back to the original state.
- *Access Control List (ACL) model*—the most commonly used model to define access rights between data and the users.

Also considered within this domain are:

- the functions and capabilities within operating systems for state management, memory management, kernel and monitoring activities;
- architecture evaluation methodologies such as the Trusted Computer Security Evaluation Criteria (TCSEC), Information Technology Security Evaluation Criteria (ITSEC), and Common Criteria (CC);
- application and system software problems, logic flaws, and design/implementation errors that create opportunities for system compromises/attacks; and
- the concepts of certification and accreditation.

1.2.3.10 Telecommunications and Network Security. By the CBK definition, this domain encompasses the structures, transmission methods, transport formats, and security measures used to provide integrity, availability, authentication, and confidentiality for transmissions over private and public communication networks and media/cabling. This is the largest and most technical domain in the CBK. It includes the OSI model with the seven layers of functionality: physical, data-link, network, transport, session, presentation, and application layers. Included herein are the subjects of:

- local area networks (LANs), enterprise, metropolitan, and wide area networks;
- common network devices, such as routers, bridges, switches, and firewalls;

- network security protocols; and
- common forms of attacks against network infrastructures.

It deals with the actual hardware used to connect information systems to each other. Security is dealt with in terms of hubs, routers, switches, and firewalls, for example. To keep the data safe, secure, and error-free, the domain deals with the safeguards and protocols that administrators have to enforce.

1.2.3.11 CBK Summary. The Common Body of Knowledge provides an organized delineation of the major subjects that impact information security. The CBK in fact addresses all the aspects of security discussed at the beginning of this section. However, the CBK does not provide guidance on achieving sufficient protection for an organization's assets. The domains of the CBK are not organized to facilitate establishing an enterprise set of processes that ensure information security is achieved. The following fictionalized event provides an illustration of how security in modern organizations has become extremely complex.

1.3 A TWENTY-FIRST CENTURY TALE

To understand some of the problems associated with modern computer system security, let us consider the following scenario. This is not based on any specific actual event, rather it is an abstraction of events that have occurred over the last few years.

1.3.1 The Actors

Alice: Alice is a salesperson at a mall jewelry store (MJS Company).

Bob: Bob is a product buyer for a very successful Internet retail corporation (IRC Corp.).

Carol: Carol is a network administrator for a large cable Internet service provider (CISP Corp.).

Debbie: Debbie is a former employee of CISP Corp.

Other parties are not identified.

1.3.1.1 Bob's Story. Bob was surfing the web one evening (March 2) from home looking for interesting products his company (IRC Corp.) should consider adding to their inventory. After some three hours of searching, he had downloaded a number of web pages onto a "thumb" drive to show his director what Bob thought would be great new products. The next morning Bob transferred the pages onto his office PC from the thumb drive, printed them out, and emailed them as attachments to his boss, the VP of purchasing. During the day, Bob kept experiencing long delays when using the IRC-integrated purchasing application and even called the help desk to complain of slow response times. That afternoon, Bob received a call wherein his boss told him that three of IRC's major suppliers had called and suspended all shipments in transit, necessitating that the warehouse be ordered to put orders not yet shipped on hold.

What Bob was *not* told was that the IRC CEO had received an anonymous email claiming the sender to be the cause of IRC's supply problems. The sender also claimed able to disrupt IRC's business bank accounts, lines of credit with the financial community, and share IRC confidential information with its competitors. The sender would do all these things if IRC refused to deposit US$200,000,000 into a Caymans Islands located bank account by 10 AM EST March 15. The CEO, her VPs, and legal counsel were meeting that evening to decide how to proceed. The email warned IRC against contacting law enforcement agencies or the press.

1.3.1.2 Carol's Story. On April 15, Carol was having lunch at the CISP Corp. cafeteria when her pager started beeping. Carol saw that she was needed in the Network Operations Center (NOC) immediately. When she entered the NOC control room, she learned that all the company DSL access networks on the east coast were overloaded with traffic and the customer help desk was receiving hundreds of calls from irate service subscribers. One NOC administrator had remotely accessed one of the newer access edge routers, which included a new network traffic-monitoring and analysis subfunction that came built into the base product.

The router reported that it was experiencing an "ARP storm" on all of the 100,000 DLS access links terminated by this router. The router also reported that it was seeing network packets destined for TCP port 80 at any machine that responded to the ARP requests flooding the sub-net. The 10 other newer routers, just recently deployed, reported similar conditions when queried. These 11 routers represented only 1% of the 1100 access routers deployed, so if the older access routers were also trying to cope with "ARP storms," then most of CISP's 35,000,000 east coast subscribers' Internet service was being affected.

CISP Corp. senior management had decided, when initially planning to purchase access routers, that the CISP network design staff could not sufficiently justify spending twice the budget to buy routers that included advanced security capabilities beyond the basic packet filtering (firewall functionality). The well-recommended network consultant CISP hired to review the plans reported that additional security capabilities were unnecessary and would interfere with network performance, thereby reinforcing management's position. As a result of this decision, the NOC staff had no way to stop these "ARP storms" except to direct each router to filter out, or block, all network traffic directed at TCP port 80. This action eliminated the storms after about five hours; however, CISP commercial subscribers kept calling and complaining that their ecommerce web systems could not be reached by online retail customers and that CISP Corp. was not meeting the Service Level Agreements (SLAs) in the contacts signed with CISP's commercial subscribers.

While the CISP Network Operations Center (NOC) staff were working on cleaning up after the "ARP storms," they started getting calls from well over 200 emergency 911 centers complaining of thousands of 911 calls that appeared to be false, preventing the timely handling of "real" 911 calls. Upon investigation, the staff found that virtually every CISP VoIP subscriber user agent (UA) application was the source of these calls.

Their only option was to shut down the CISP VoIP servers, thereby terminating the ability of the misbehaving UAs to continue placing 911 calls. They then proceeded to further investigate what was the cause of these problems so that the VoIP service could be restored.

1.3.1.3 Alice's Story. When Alice got home the afternoon of Friday March 15, she found two letters from credit card companies she did not recognize and two post office notices informing her that she had registered letters waiting to be signed for and picked up. It was only 3:30 PM, so she decided to call the local post office and check if she could come there now and get the registered letters, but when she picked up the phone, there was no dial tone. She had been having some small problems with her Voice over IP (VoIP) Internet phone service the last couple of months, nuisance problems with her address book, and some calls being dropped mid-conversation, but nothing like this. So she decided to take a chance and just drive to the post office.

Getting there she signed for the letters that were from two banks. The bank letters were demanding overdue payments on a homeowners credit line and an auto loan, neither of which she had applied for. Alice had no idea what these letters were about, yet knew she had a mess on her hands.

Upon returning home, Alice opened the two credit card company letters and found statements for credit card accounts she had never applied for. One of the accounts had an outstanding balance due of over $15,000 and the other a balance due of over $11,000. At this point, she realized she was a victim of "identity theft," yet had no idea how this could have happened.

1.3.2 What Actually Occurred

Back in October, Debbie was identified as the CISP employee who was logging into the CISP Internet phone service management system and setting up accounts for her friends to use at no cost to them. What the CISP investigators did not know was that Debbie was part of a street gang that had links to an international crime syndicate headquartered in Vladivostok, Russia. Also unbeknown to the investigators, Debbie had been copying CISP customer personal and account information, and her gang was selling this stolen identity information to a crime syndicate that was reselling the information to anyone willing to pay their price. Debbie's stolen information included the IP addresses, host names, and other details of CISP's servers and network organization. Identity information of one customer (Alice) was used by gang members to:

- open charge accounts and run up over $62,000 of fraudulent charges and cash advances;
- take out an auto loan and buy a $110,000 Porsche sports car that they then sold to a chop shop for $55,000; and
- apply for, and receive, a $150,000 home equity credit line from which they immediately borrowed $145,000 in cash.

A set of other CISP customer identities, and network information, were sold by the syndicate to a splinter group of an organization accusing the United States of economic despotism in central Africa. This splinter group decided to launch an attack on the US economy in retaliation. They had access to a retired KGB intelligence specialist who loved payment in untraceable "blood diamonds." The specialist recommended attacking the US communications infrastructure, causing confusion and fostering panic. The group commissioned the specialist to craft an attack that could leverage the identity information recently purchased from the syndicate. The syndicate provided information disclosed that CISP's VoIP service infrastructure relied on the User Agent (UA) software available to VoIP service subscribers and remotely retrieved, via tFTP, from CISP UA servers whenever the subscriber's PC or phone powered up.

What the specialist came up with was a malicious form of the User Agent software used by VoIP service subscribers. Given the syndicate provided information about CISP's VoIP infrastructure, it took the specialist just a few hours to remotely log into the 30 CISP UA servers and substitute the malicious UA software for the authentic UA software in each server. By the end of two weeks, every CISP VoIP service subscriber's device was running the bogus UA software. This software behaved identically to the authentic UA software except that it had a few built-in additional capabilities.

Each malicious UA, once running, would connect to an Instant Messaging (IM) server and listen for a command. This attack approach basically provided the splinter group with an army of remote machines (a "zombie army") ready to do the group's bidding. The group waited until March 15, the day the tyrant Caesar was struck down, and then issued their attack command via the IM server to the listening UAs. The command directed every UA to start making calls to 911, disconnect immediately upon the call being answered, and then repeat the cycle. Within 30 minutes, CISP was forced to shut down all its VoIP servers.

One of the identities sold to the crime syndicate was for a commercial account for IRQ Corp. The crime syndicate decided to try and raid IRQ for valuable information and extort money from IRQ as well. One of the IRQ employees identified as a target was Bob and the stolen information included Bob's home email address. With this information, the syndicate sent Bob an email designed to look as though it had come from the IRQ Human Resources (HR) department requesting that Bob log into his employee benefits account and verify personal information via a web link in the email. Unknown to Bob, when he clicked on the link, his web browser was directed to a fake IRQ HR web server run by the syndicate. The fake web server redirected Bob's browser back to the real HR web server, but not until it had installed a "root-kit" on Bob's home PC.

Bob did not notice anything unusual, so he reviewed his personal employee information, found everything in order, and logged out of the HR site, and then did some work-related web surfing. The "root-kit" software on Bob's PC not only provided a "backdoor" into Bob's PC for the syndicate's use but also included the ability to infect any removable media (floppy disks, thumb drives, etc.) with a virus that would install the "root-kit" on any machine the removable media was mounted on. Another component of the "root-kit" was a variant of the Code Red worm designed to locate IIS web servers, infect them, locate additional IIS targets, and on each infected IIS server install the “root-kit,” find all infected server information about customers and business activities, and then FTP the information back to the syndicate.

When Bob transferred his web files from the thumb drive to his IRC PC the next day, the virus was able to infect the PC, thereby installing the “root-kit” software and launching the Code Red worm within IRC’s company network. The worm immediately discovered the IP sub-net address range used within IRC’s internal network and started issuing ARP request messages to locate and identify all other machines in the network and what OS was running on each. The worm accomplished the discovery by sending an ARP request to every sub-net IP address within the address range used within IRC’s company network. Whenever an ARP reply indicated that a machine is running the MS Windows Internet Information Server (IIS), the worm would then send the discovered machine a carefully crafted http message over TCP to port 80.

This message was crafted to cause a “buffer overflow” within any version of IIS and cause the IIS process to then receive a second http message containing a copy of the worm to the discovered machine, infecting it with the “root-kit” and worm. The process then repeated itself until all machines running IIS were infected (compromised). As part of infecting each discovered machine, the “root-kit” malicious software would proceed to search the local disks for any data that included information on contracts, customers, business relationships, and anything else that dealt with people, money, or financial relationships. All information found was then FTP’ed to a syndicate server.

The syndicate was blackmailing a database-mining expert at a large manufacturer of business applications. This expert, who had a criminal past he wanted kept hidden, was being coerced to develop business analysis software for the syndicate that would produce reports about targeted companies based on data retrieved from information attacks/thefts by the syndicate against large corporate targets. This analysis allowed the syndicate to identify avenues of attack against IRC for extortion purposes. The syndicate decided to immediately interfere with some of IRC’s supply sources since IRC had an “extra-net” link between its business servers and the servers of IRC’s three largest product suppliers. The approach taken was to construct fraudulent messages canceling all current contracts and send these messages to the “extra-net” reachable supplier order processing servers. Upon receipt of these messages, the three suppliers then halted all shipments to IRC pending review.

1.3.3 How Could All This Have Been Prevented?

There was really nothing Alice could have done to prevent her identity and personal information from being stolen. However, Alice could have taken more time to review statements and other personal financial information for signs of unauthorized transactions. She could also have considered closer self-monitoring of her credit status or hired a service to do the monitoring for her.

In the story, Debbie’s unauthorized activities were the starting point. CISP’s personnel policies and administrative procedures could have included criminal and financial “background” investigation of employee applicants to ensure a lower probability of employees abusing the access granted to them to CISP information and infrastructure components. If CISP required that all account administration activities be logged and changes only be allowed by authenticated administrative personnel with two employees necessary to complete any major change, then CISP subscriber information would not have been so easy to steal. Lack of stolen account information would not have allowed the syndicate to exhort IRC for money nor the splinter group to launch attacks against CISP's VoIP service and the 911 Emergency Response Centers. If CISP had partitioned its access networks, via routers, into smaller address ranges, then attempts by the worm to flood these access networks and locate additional targets would have been constrained to just the network segments to which an already infected PC was attached.

If CISP had deployed some type of application message-filtering capability (intrusion prevention) within each access router, then the Code Red http messages could have been blocked, further reducing the likelihood of other CISP subscriber machines being compromised. An Intrusion Prevention capability would have allowed for the selective blocking of only Code Red worm initiated http messages such that other commercial http-based activity could have continued to occur. CISP's deployment of VoIP UA software downloading via non-authenticated tFTP made substituting the malicious UA software possible.

Had Bob installed up-to-date antivirus/spyware software, then his PC would most likely not have gotten infected by the "root-kit" and Code Red worm. If IRC required all company PCs to have antivirus/spyware software installed and kept up to date, then Bob's office PC, and other IRC machines, would not likely have been infected either. If IRC had partitioned its internal network, via routers, into different address ranges, then attempts by the worm to flood the network and locate additional targets would have been constrained to just the network segment to which Bob's PC was attached. If IRC had deployed some type of application message-filtering capability (Intrusion Prevention) beyond basic firewall filtering, then the Code Red http messages could have been blocked, further reducing the likelihood of other IRC machines being compromised.

1.3.4 They Did Not Live Happily Ever After

The specific events, people, and organizations related above are fictional but based on real events. The FBI and the Computer Security Institute (CSI) have been conducting surveys to determine the magnitude and extent of security-related events within industry. These surveys routinely highlight that over 55% of all acknowledged business security events were caused by insiders (employees or other individuals granted access to business systems and resources). Over the last few years, the press/media have provided numerous reports of:

- major corporations losing control over customer information and records after being attacked from the outside (in 1994 a Russian national allegedly masterminded the break-in of Citicorp's electronic funds transfer system and a gang of hackers under his leadership breached Citicorp's security 40 times that year. They were alleged to have transferred $12 million from customer accounts and withdraw an estimated $400,000);

- government agencies from which databases of citizen information have been lost or stolen that were in the custody of agency personnel;
- financial institutions that have lost backup media containing thousands of customer records while in transit;
- business laptops vanishing that contained many forms of corporate-sensitive information;
- increase in network-based activity by organized crime to steal the identities of individuals using techniques such as “phishing,” faked ecommerce websites, spyware, and worms to snare unsuspecting people.

These events can happen. Some have already occurred. This is our twenty first-century reality, it is not fiction!

1.4 WHY ARE YOU IMPORTANT TO COMPUTER SECURITY?

A computer system’s security is only as good as its weakest link. The process involves everyone, not only the people overlooking security exclusively. If just one person does not pay attention to the system’s security, the whole system’s security can be compromised. Nowadays, almost every computer is connected to the Internet. Home users should also take care about information security. The chance of your computer being attacked is as likely as that of any other computer connected to the Internet. It does not matter if your system has little or no relevance to the attacker.

What exactly can happen if your system is attacked? Here are some of the consequences. All data on the system could be lost. Your password may have been cracked, and the attacker breaks into the system and steals information. Your computer could be hijacked and could be used as a gateway to attack other computers. As a result, you could be liable for inflicted damages.

Why would someone want to attack your computer? What are some of the reasons?

- Excitement and thrill for inexperienced attackers
- Bragging rights for experienced hackers who target high-profile companies
- Fame in the media
- Revenge by disgruntled former employees (in some cases, insiders too!)
- Access to sensitive information (company’s proprietary information, credit cards, social security numbers, etc.)
- Denial-of-service attacks against particular websites
- Need of storage space to store illegal or pirated software on unsuspecting computers
- Using other computers to launch attacks so as to cover their tracks
- To intercept passwords through packet sniffers and keystroke recorders

What are the attackers looking for in a target?

- Systems with a high-speed continuous Internet connection
- Systems on which their activity will go unnoticed
- Systems with poor, or not used, security capabilities.

It comes as no surprise that the top targets are home computers with a broadband connection to the Internet, whose owners are likely to be less knowledgeable about computers, have little or no security, and most of them use Windows operating systems. Also the systems in colleges and universities are potential targets where many are accessed by multiple users and no one is likely to notice any unusual activity.

1.4.1 What Are the Threats to Your Computer?

The main forms of attacks against any computer system can be grouped under the following areas:

- *Viruses and worms*—Worms are programs designed to replicate and spread on their own without the user's knowledge. Some of them are an annoyance but some could be malicious and destructive. They are often hidden inside innocuous programs. Viruses in email messages often masquerade as games or pictures to encourage users to open and run them. Viruses try to replicate themselves by infecting other programs on your system. Worms can replicate themselves by sending out email messages themselves.
- *Trojan horses*—programs that appear normal to the users but have a secret purpose that the user is unaware of. Usually used as backdoor entries into systems at a later time. For example, a user downloads a game to their computer, but other components could as well have been installed without their knowledge. Viruses or worms are often smuggled inside a trojan horse.
- *Spyware*—small, hidden programs that run on your system and are typically used to track the user's activities. Spyware allows intruders to monitor and access the system. Spyware gets installed when programs are downloaded from unknown sources.
- *Denial-of-service attacks*—to prevent legitimate users from accessing a system. A common technique is to bombard a target with a large volume of data that it cannot reasonably handle. Usually web servers and file servers are the target. The servers become so busy attempting to respond to the attack that the system ignores legitimate requests for connections.
- *Social engineering*—when hackers psychologically trick legitimate users to give them the information needed to access the systems.
- *Program flaws*—applications running on computers that are not foolproof and typically have flaws. Some of these flaws could cause the application to behave abnormally under certain conditions. When someone finds out about these

problems, they post these as application vulnerabilities. Attackers can now use these vulnerabilities and take control of the systems.

- *Poor passwords*—password cracker programs are now widely available that try every word to match the user's password. Users should be encouraged to use random passwords meeting certain criteria and to change them periodically.
- *Poor security practices*—leaving a computer unprotected, installing software without the system administrator's knowledge, and so forth pose additional risks to computer systems.

1.4.2 As a User, What to Do?

The following are some remedies to counter the threats discussed in the previous section:

- *Viruses and worms*—Users must make sure that antivirus software and virus signature definitions are up to date. Users must also be careful when opening email attachments and preferably use text-only email.
- *Trojan horses*—Users should be careful when downloading programs into their computers and should only do so from trustworthy sources.
- *Spyware*—Use anti-spyware tools to recognize the unwanted programs running on the system.
- *Denial-of-service attacks*—In this case the user can do very little on their own. They can protect their computer so that their machine is less likely to be used in a denial-of-service attack against some other computer.
- *Social engineering*—Users need to be suspicious when someone asks for sensitive computer information and should be aware of the IT procedures in place.
- *Program flaws*—The best way to minimize the risks against application flaws is to keep them updated by installing the latest patches, manually or automatically.
- *Poor passwords*—Users should use hard-to-guess passwords and should not write them down. Passwords should never be given out or shared.
- *Poor security practices*—The best practice is to disconnect or shut down the system when not in use. Also unnecessary programs and services should be removed or disabled. Sharing capabilities with files and printers should never be allowed, and it is a good practice to install a firewall on the system.

These remedies should not be applied randomly, however; rather they should be part of a well-thought out set of plans based on sufficient analysis to achieve the required degree of protection.

1.4.3 The Reality of Cybercrime and Cyberwarfare

Today's enterprises, and society in general, have become highly dependent on the use of computer systems and the networks that interconnect these systems. Even the smallest businesses rely on computer-based applications, let alone the major critical infrastructure components (power generation/distribution, transportation, communications, finance, etc.) of a modern country. In fact, criminal organizations have evolved to not only adopt use of networked systems but have gone so far as to target these systems, as in cybercrime, cyber-blackmail, and even cyberwarfare.

Following are some examples of cybercrime and cyberwarfare that reinforce the aforementioned points:

- Computer security has become recognized globally as a key feature of modern life. For example, as Clarke and Knake[3] point out cyberwarfare is already a significant component of international conflict.
- The NRC[4] reported that:

  "Cyber-security has been building for some time. For example, as part of a 1997 exercise ('Eligible Receiver'), an NSA (National Security Agency) hacker team demonstrated how to break into DOD (Department of Defense) computers and the U.S. electric power grid system. They simulated a series of rolling power outages and 911 emergency telephone overloads in Washington, D.C., and other cities. They also succeeded in showing how to break into unclassified systems at four regional military commands and the National Military Command Center in Washington, D.C. And they showed how to gain supervisory-level access to 36 networks, enabling email and telephone service disruptions."
- Rachael King[5] reported that:

  "The security breach at EMC Corp.'s RSA unit may cost the banking industry as much as $100 million to replace identification tokens that left their computers vulnerable to spying.

  RSA clients include Wells Fargo & Co. and Northwest Bancshares Inc. as well as defense contractor Lockheed Martin Corp., which said a May 21 cyber attack on its computers is linked to the March breach of RSA's SecurID database.

  Avivah Litan, a security analyst at Stamford, Connecticut-based Gartner, said in an interview: Bethesda, Maryland-based Lockheed, the world's largest military contractor, said June 4 it had already mailed new tokens to 45,000 employees. Raytheon Co., the biggest maker of missiles, and Northrop Grumman Corp., maker of B-2 stealth bombers and Global Hawk drones, are also SecurID users, according to RSA.

  Litan estimates that there are 3,500 FDIC-insured institutions, with about 500 to 1,000 people each using security tokens. If all the banks agree to RSA's offer, the cost of distribution would be $50 million to $100 million.

  The attack began with e-mails sent to small groups of RSA users, presumably employees, that were titled '2011 Recruitment Plan' and wound up in their junk

[3] *Cyber War: The Next Threat to National Security and What to Do About It*, R. A. Clarke and R. Knake, Ecco, 2010, ISBN-13 978-0061962233.

[4] *Trust in Cyberspace*, Committee on Information Systems Trustworthiness, National Research Council, 1999, citing "Infowar Game Shut Down U.S. Power Grid, Disabled Pacific Command," B. Gertz, *Washington Times*, April 17, 1998, p. A1.

[5] "EMC's RSA Security Breach May Cost Bank Customers $100 Million," R. King, *Bloomberg*, 2011, http://www.businessweek.com/news/2011-06-08/emc-s-rsa-security-breach-may-cost-bank-customers-100-million.html.

files, RSA told analysts including Litan in an April 1 conference call. Attached to those e-mails was a spreadsheet that contained malicious software that gathered security credentials until it found the targeted system. Secret data was stolen and sent to an outside hosting provider, according to an April 1 blog post by Litan."

- As reported by the Boston Globe,[6] "A hacker broke into a wireless carrier's network over at least seven months and read emails and personal computer files of hundreds of customers, including the Secret Service agent investigating the hacker, the government said yesterday."
- Hiawatha Bray reported in the Boston Globe[7] that:

  "On Nov. 30, only days before Internet activists shut down the websites of credit card companies Visa and MasterCard, five major online retailers faced a similar attack, timed to coincide with the start of the holiday shopping season. The attacks against Visa and MasterCard paralyzed their company websites for hours. But even though the assault on the retail sites used similar methods, they didn't have the same effect. The floods of illicit data were intercepted by a global network run by Akamai Technologies Inc. . . ."

These are but a few of the growing number of reported security events that are now regularly reported by the media.

1.5 END OF THE BEGINNING

Eugene Spafford[8] makes the point that "Asking the wrong questions when building and deploying systems results in systems that cannot be sufficiently protected against the threats they face."[9] He adds that "Asking how to make system 'XYZ' secure against all threats is, at its core, a nonsensical question." A number of other recommendations that Spafford makes are:

- "one has to understand what (assets) needs to be protected, where these assets are located and their value to the organization;
- who/what has to be protected against, namely who has to be defended against;
- what level(s) of protection make(s) economic sense or are required by legislation or regulation;

[6] "Hacker Cracks T-Mobile Network," *Boston Globe*, 2005, http://www.boston.com/business/technology/articles/2005/01/13/hacker_cracks_t_mobile_network/.

[7] H. Bray, 2010, http://www.boston.com/yourtown/cambridge/articles/2010/12/20/akamai_arbor_defending_against_internet_service_attacks/.

[8] Eugene Spafford, a noted security expert, teaches Computer Science at Purdue University and serves as the Executive Director of the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue.

[9] Spafford, E. "Privacy and Security—Answering the Wrong Questions Is No Answer," *Communications of the ACM*, June 2009.

- within the deployment environment, what security issues exist; and
- what constitutes acceptable risks (e.g., how much damage or loss can be considered an acceptable cost of doing business."[9]

One way to address these matters is by posing the following questions during the initial planning and analysis phase of a project:

- Assets—what do I need to protect?
  So the first priority is to identify what needs to be protected. Without identifying properly what needs to be protected, the solution will be inadequate to meet security needs. For example, assets may include customer data, email addresses, credit card and social security numbers, encryption of network data, databases, firewalls, and redundant servers. There are assets that are intangible as well, such as an organization's reputation for stability and reliability. The investment community is greatly influenced by public perception, and a company can potentially suffer sufficient economic and social damage as to force it into bankruptcy. All assets, be they tangible or intangible, have value to an organization; thus, the cost to replace an asset needs to be identified before one can determine how much should be expended to protect the asset.
- Risks—what are the threats, vulnerabilities, and risks?
  To protect the identified assets, one needs to find out the vulnerabilities that might be exploited by potential threat agents and attack methods. Vulnerabilities may be present within an asset, exist due to how an asset is used or accessed, or be a result of the environment within which an asset exists or is deployed. The next task is to itemize the threats to these assets and their sources—who may attack the assets (threat agents), what forms of attacks could/would be used, the probability that attacks may occur, and the likelihood and magnitude of potential damage/loss. An analysis of assets, vulnerabilities, and threats is critical in determining what security capabilities should be deployed, where security capabilities should be located, what constitutes a reasonable expenditure for an identified security capability, and what constitutes an economically reasonable expenditure for protecting a specific asset.
- Protections—how to protect the assets?
  The logical next step is to consider the security capabilities/services that could be used to provide the required type of protection for assets against the threats identified in the preceding step. Protections may take the form of procedures for users and administrators, types of mandatory authentication, forms of authorization and access controls, approaches for ensuring availability, types of monitoring and auditing, and so forth. This step identifies the general techniques that will be used to achieve the identified levels of protection.
- Tools/mechanisms—what to do to protect the assets?
  Now evaluate the available security technologies, tools, products, mechanisms, and procedures that can provide the types of protections identified in the step

above. Consider, for each evaluated tool/mechanism, the specific type and extent of protection provided, the expected acquisition cost (to purchase and deploy), and the anticipated operational cost (for training, administration, management/maintenance, and replacement). In considering these costs, one should be able to list relative cost and benefit of each tool/mechanism compared to the value of the assets being protected.

- Priorities—what order to implement the security steps?
  Most often it is not practical to implement simultaneously all the security steps identified above. So priorities need to be assigned to the tools and techniques so as to implement them in a reasonable order. Attending to all the questions above in sequential order should help install a successful security system for an organization. These questions help identify security requirements and implement actionable measures for an effective information security plan.

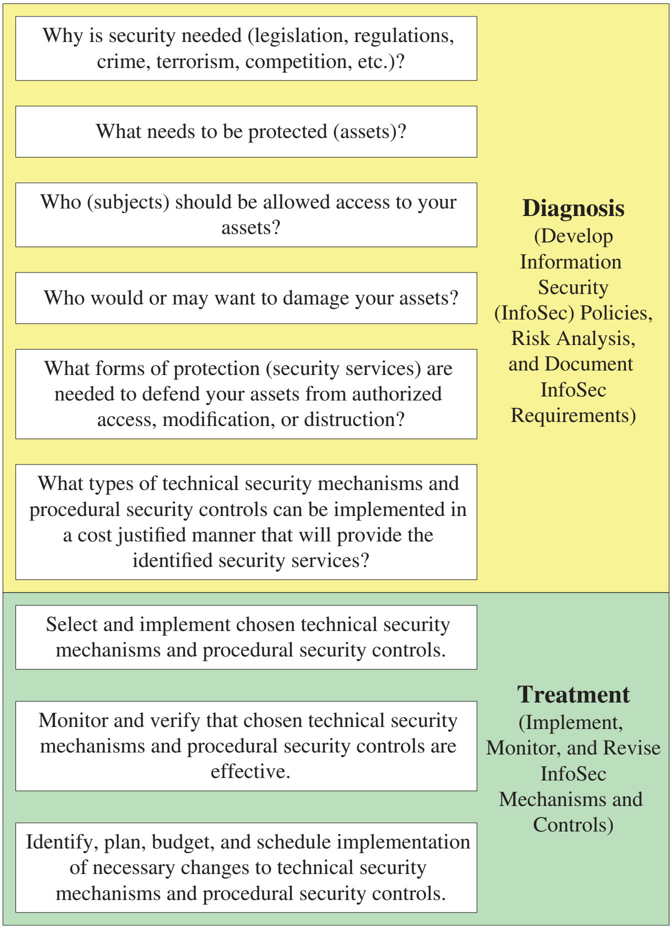
This book does not directly follow the CBK or the "by-function" approach to information security, as these two approaches do not provide sufficient guidance in developing an overarching enterprise information security program. To these approaches we would add three more attributes:

3. Integration with other enterprise operational and management activities.
4. "Risk mitigation" within the reality of business priorities.
5. A methodology that facilitates oversight, is auditable, and provides consistent and traceable results from organizational security objectives to specific security practices and procedures.

This book generally follows a systems engineering methodology that considers the technical, procedural, and managerial aspects of systems from initial conceptualization through requirements analysis, design, implementation, operations to replacement (decommissioning). An approach is borrowed from the medical world, which requires one to diagnose what the problem is prior to prescribing a treatment rather than just treating symptoms. Figure 1.2 highlights this approach.

This approach maps to chapters as follows:

- Chapter 1 is part of **Diagnosis** and considers why information security is needed, how security problems can have widespread impacts, and reviews the more common ways security is discussed and the deficiencies/limitations of these views.
- Chapter 2 is part of **Diagnosis** and discusses the many legal, technical, competitive, criminal, and consumer forces and influences that are rapidly changing our information-dependent society along with exploring the concepts of systems engineering and the value these concepts provide to the development of new products and services along with the maintenance and evolution to existing products and services.



Why is security needed (legislation, regulations, crime, terrorism, competition, etc.)?

What needs to be protected (assets)?

Who (subjects) should be allowed access to your assets?

Who would or may want to damage your assets?

What forms of protection (security services) are needed to defend your assets from authorized access, modification, or distruction?

What types of technical security mechanisms and procedural security controls can be implemented in a cost justified manner that will provide the identified security services?

Diagnosis (Develop Information Security (InfoSec) Policies, Risk Analysis, and Document InfoSec Requirements)

Select and implement chosen technical security mechanisms and procedural security controls.

Monitor and verify that chosen technical security mechanisms and procedural security controls are effective.

Identify, plan, budget, and schedule implementation of necessary changes to technical security mechanisms and procedural security controls.

Treatment (Implement, Monitor, and Revise InfoSec Mechanisms and Controls)

Figure 1.2. InfoSec diagnosis and treatment

- Chapters 3 and 4 review fundamental security concepts of subjects, objects, security services, and the role of cryptography in information security (Chapter 3) and consider different approaches for achieving authentication of individuals and systems (Chapter 4).
- Chapter 5 is part of **Diagnosis** and delves into how to establish and manage an information security program, evaluate vulnerabilities, threats, and risks, and develop security requirements, and considers the value and impact of security standards and the major organizations involved with developing these standards.
- Chapter 6 is part of **Diagnosis** and describes the different forms and types of networks currently in use along with the protocols relied upon that are the cause of

many security problems. All protocol layers are considered and any security capabilities are analyzed for effectiveness and usability.

- Chapter 7 is part of **Diagnosis** and focuses on the near future "Next-Generation Network" concepts and services defined within the developing Internet Multimedia Subsystem framework.
- Chapter 8 is part of **Diagnosis** and provides an in-depth discussion of computer hardware that impacts information security and the role of operating systems in supporting information security and what security mechanisms an operating system should include.
- Chapter 9 is part of **Treatment** and provides an examination of security capabilities in the major commercially available operating system (Unix variants, Windows variants, and real-time) and then considers security issues within applications software. This chapter concludes with a review of the different forms of malicious software (malware) encountered today and a number of anti-malware applications currently available.
- Chapters 10 and 11 are part of **Treatment** and provide descriptions and analysis of the available networking security mechanisms within each protocol layer of networks. Both stand-alone applications (including their associated protocols) and the major application frameworks, such as Java, .NET, CORBA, and DCE, are discussed from a security capabilities perspective,
- Chapter 12 is part of both **Diagnosis** and **Treatment** and explores the security issues within management of networks, especially management of security, and considers the organizational needs for effective security management, operational security mechanisms, security operations, and other life-cycle security issues. This chapter concludes with consideration of security within development, integration, and component purchasing activity areas.

1.6 CHAPTER SUMMARY

There are many types of behavior related to information/communications systems, and their operation, that put our technological society in danger. We provided and discussed a modern-day tale that showed some of the many threats to computer networks, information systems, and organizations. This tale also showed that everyone is either part of the problem or part of the solution by starting to consider what to do. We examined a number of general ways of discussing security: the CBK, by-function, and then systems engineering approaches. We considered the many general security concepts and complexities associated with issues of safety, and information availability, and enterprise infrastructures. The two basic perspectives on information security (defining security by functions instead of by Common Body of Knowledge) were discussed. Four key security questions were presented to suggest an alternative way for protecting organizations. This alternative approach is the primary focus of this book.

1.7 FURTHER READING AND RESOURCES

Some recommended resources are:

- *Computer-Related Risks*, P. G. Neumann, Addison-Wesley, 1995, ISBN 0-201-55805-X.
- *Spyworld: Inside the Canadian and American Intelligence Establishments*, M. Frost and M. Gratton, Doubleday Canada, 1994, ISBN 0-385-25494-6.
- *Privacy for Sale: How Computerization Has Made Everyone*'s *Private Life an Open Secret*, J. Rothfeder, Simon and Schuster, 1992, ISBN 0-671-73492-X.

Although these books are more than 15 years old, they are still worth reading for information and insights as to the complexities of protecting information from misuse. Neumann's book still provides one of the best general treatments on information system risks. Frost and Gratton's book offers a unique view on how intelligence agencies have operated in the past and are likely to continue operating in a similar manner into the future. Rothfeder's book considers what has become just the beginning of our now highly networked and computerized society. The amount of information being collected on individuals is mind boggling in this "Internet age." Every time a person connects to almost any website, not just the primary site, but many other sites linked into the primary site, "cookies" and other tracking mechanisms are frequently used to record who the person is along with expressed interests. Some websites even load tracking software directly onto a person's computer to gather even more information.