# INFORMATION SECURITY

# UNIT-1

## Chapter – 1:

### What is information security?

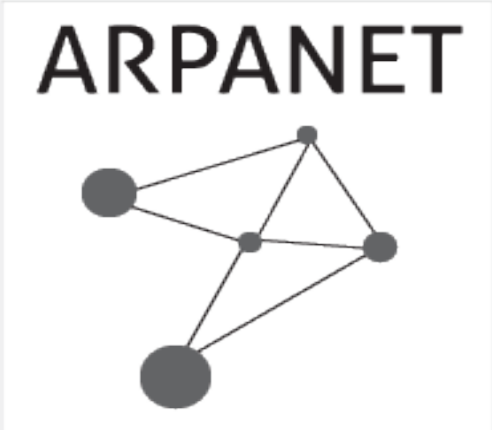
Information security in today's enterprise is a "well-informed sense of assurance that the information risks and controls are in balance." –Jim Anderson, Inovant (2002)

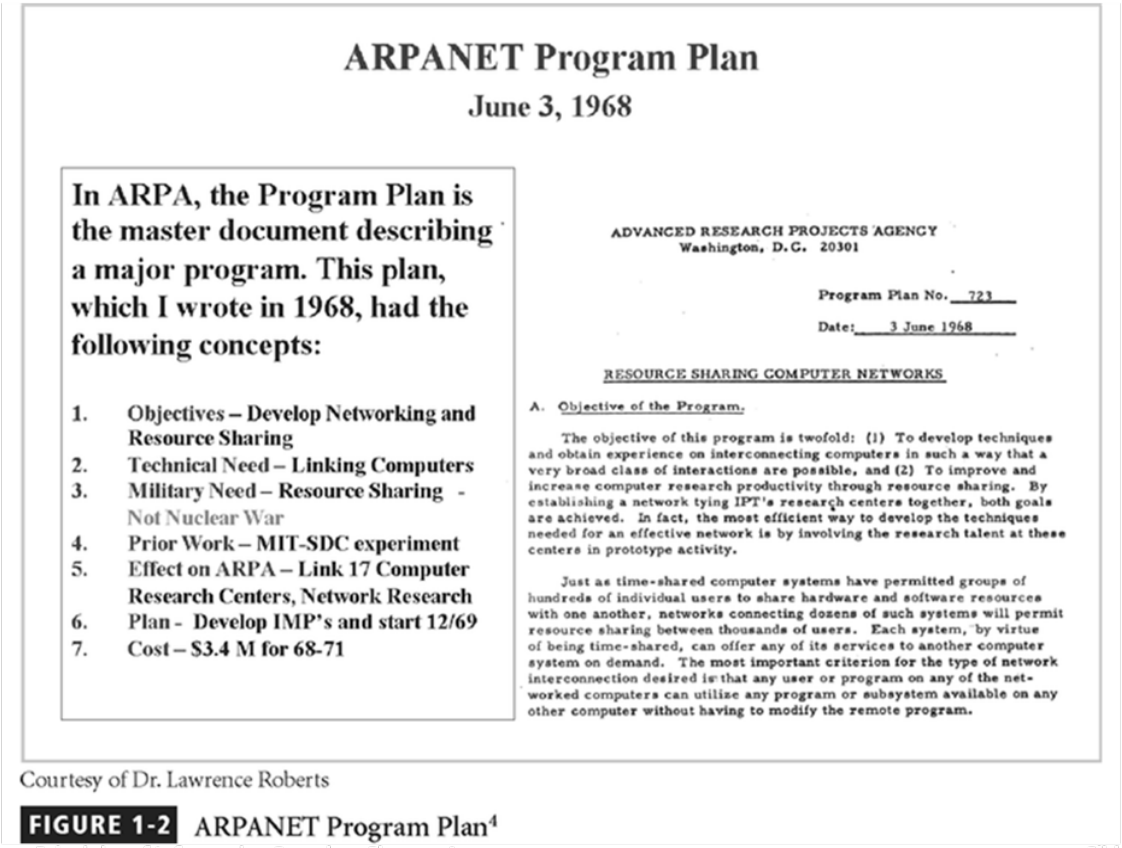
### History of information security

- Computer security began immediately after the first mainframes were developed
- Groups developing code-breaking computations during World War II created the first modern computers
- Physical controls were needed to limit access to authorized personnel to sensitive military locations
- Only rudimentary controls were available to defend against physical theft, espionage, and sabotage

**The 1960s**

- Department of Defense's Advanced Research Project Agency (ARPA) began examining the feasibility of a redundant networked communications
- Larry Roberts developed the project from its inception






Courtesy of Dr. Lawrence Roberts

**FIGURE 1-2** ARPANET Program Plan[4]



**The 1970s and 80s**

- ARPANET grew in popularity as did its potential for misuse
- Fundamental problems with ARPANET security were identified
  - No safety procedures for dial-up connections to the ARPANET
  - User identification and authorization to the system were non-existent
- In the late 1970s the microprocessor expanded computing capabilities and security threats

**R-609 – The Start of the Study of Computer Security**

- Information Security began with Rand Report R-609
- The scope of computer security grew from physical security to include:

- Safety of the data
- Limiting unauthorized access to that data
- Involvement of personnel from multiple levels of the organization

- **The Paper that Started the Study of Computer Security**
- It began with Rand Report R-609, sponsored by the Department of Defense, which attempted to define multiple controls and mechanisms necessary for the protection of a multi-level computer system.
- The scope of computer security grew from physical security to include:
- Safety of the data itself
- Limiting of random and unauthorized access to that data
- Involvement of personnel from multiple levels of the organization
- At this stage, the concept of computer security evolved into the more sophisticated system we call information security.

**The 1990s**

- Networks of computers became more common, so too did the need to interconnect the networks
- Resulted in the Internet, the first manifestation of a global network of networks
- In early Internet deployments, security was treated as a low priority

**The Present**

- The Internet has brought millions of computer networks into communication with each other – many of them unsecured
- Ability to secure each now influenced by the security on every computer to which it is connected

## What Is Security?

- **"**The quality or state of being secure--to be free from danger"
- To be protected from adversaries
- A successful organization should have multiple layers of security in place:
  - Physical security
  - Personal security
  - Operations security
  - Communications security
  - Network security

## PHYSICAL SECURITY

Physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism.

Physical security is often overlooked (and its importance underestimated) in favor of more technical and dramatic issues such as hacking, viruses, Trojans, and spyware. However, breaches of physical security can be carried out with little or no technical knowledge on the part of an attacker. Moreover, accidents and natural disasters are a part of everyday life, and in the long term, are inevitable.

There are three main components to physical security. First, obstacles can be placed in the way of potential attackers and sites can be hardened against accidents and environmental disasters. Such measures can include multiple locks, fencing, walls, fireproof safes, and water sprinklers. Second, surveillance and notification systems can be put in place, such as lighting, heat sensors, smoke detectors, intrusion detectors, alarms, and cameras. Third, methods can be implemented to apprehend attackers (preferably before any damage has been done) and to recover quickly from accidents, fires, or natural disasters.

## PERSONAL SECURITY

It means to protect the individual or group of individuals who are authorized used to access the organization and its operations.

## OPERATIONS SECURITY

It deals with protecting the details of a particular operation or a set of activities

It is the process of protecting little pieces of data that could be grouped together to give the bigger picture.

## COMMUNICATION SECURITY

Communications security is the discipline of preventing unauthorized interceptors from accessing telecommunications in an intelligible form, while still delivering content to the intended recipients. In the United States Department of Defense culture, it is often referred to by the abbreviation COMSEC. The field includes crypto security, transmission security, emission security, traffic-flow security. and physical security of COMSEC equipment.

COMSEC is used to protect both classified and unclassified traffic on military communications networks, including voice, video, and data. It is used for both analog and digital applications, and both wired and wireless links. **Crypto security:** The component of communications security that results from the provision of technically sound cryptosystems and their proper use. This includes ensuring message confidentiality and authenticity.

It is mainly concerned with the protection of communications media, technology and content.

## NETWORK SECURITY

Network security[1] consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

**What Is Information Security?**

Information security, therefore, is the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information.

But to protect the information and its related systems from danger, tools, such as policy, awareness, training, education, and technology are necessary.

The C.I.A. triangle has been considered the industry standard for computer security since the development of the mainframe. It was solely based on three characteristics that described the utility of information: confidentiality, integrity, and availability.

The C.I.A. triangle has expanded into a list of critical characteristics of information.

**Critical Characteristics Of Information**

The value of information comes from the characteristics it possesses.

**Availability** - enables users who need to access information to do so without interference or obstruction and in the required format. The information is said to be available to an authorized user when and where needed and in the correct format.

**Accuracy** - free from mistake or error and having the value that the end-user expects. If information contains a value different from the user's expectations due to the intentional or unintentional modification of its content, it is no longer accurate.

**Authenticity** - the quality or state of being genuine or original, rather than a reproduction or fabrication. Information is authentic when it is the information that was originally created, placed, stored, or transferred.

**Confidentiality** - the quality or state of preventing disclosure or exposure to unauthorized individuals or systems.

**Integrity** - the quality or state of being whole, complete, and uncorrupted. The integrity of information is threatened when the information is exposed to corruption, damage, destruction, or other disruption of its authentic state.

**Utility** - the quality or state of having value for some purpose or end. Information has value when it serves a particular purpose. This means that if information is available, but not in a format meaningful to the end-user, it is not useful.

**Possession** - the quality or state of having ownership or control of some object or item. Information is said to be in possession if one obtains it, independent of format or other characteristic. While a breach of confidentiality always results in a breach of possession, a breach of possession does not always result in a breach of confidentiality.

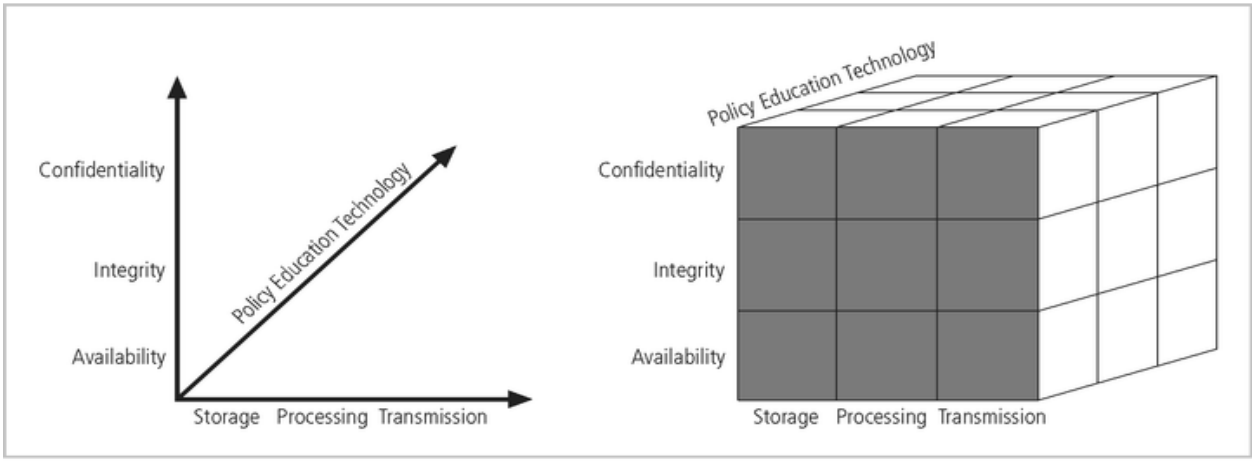



**FIGURE 1-3** NSTISSC Security Model

This graphic informs the fundamental approach of the chapter and can be used to illustrate the intersection of information states (x-axis), key objectives of C.I.A. (y-axis) and the three primary means to implement (policy, education and technology).

## Components of an Information System

To fully understand the importance of information security, it is necessary to briefly review the elements of an information system.

An Information System (IS) is much more than computer hardware; it is the entire set of software, hardware, data, people, and procedures necessary to use information as a resource in the organization.

**Securing the Components**

When considering the security of information systems components, it is important to understand the concept of the computer as the subject of an attack as opposed to the computer as the object of an attack.

When a computer is the subject of an attack, it is used as an active tool to conduct the attack. When a computer is the object of an attack, it is the entity being attacked.

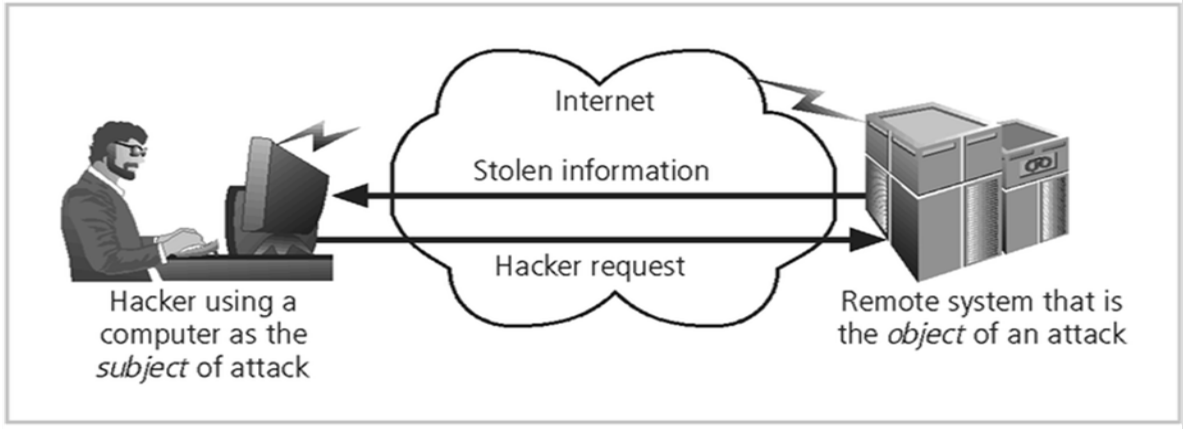



**FIGURE 1-5** Computer as the Subject and Object of an Attack



**Balancing Security and Access**

- It is impossible to obtain perfect security - it is not an absolute; it is a process
- Security should be considered a balance between protection and availability
- To achieve balance, the level of security must allow reasonable access, yet protect against threats

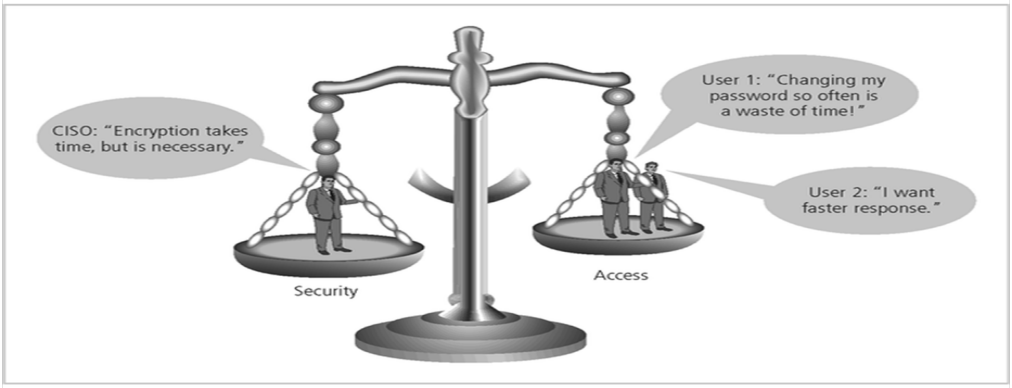



**FIGURE 1-6** Balancing Security and Access

The above figure intends to show that tradeoffs between security and access.

**Bottom up Approach To Security Implementation**

Security can begin as a grass-roots effort when systems administrators attempt to improve the security of their systems. This is referred to as the bottom-up approach.

The key advantage of the bottom-up approach is the technical expertise of the individual administrators.

Unfortunately, this approach seldom works, as it lacks a number of critical features, such as participant support and organizational staying power.

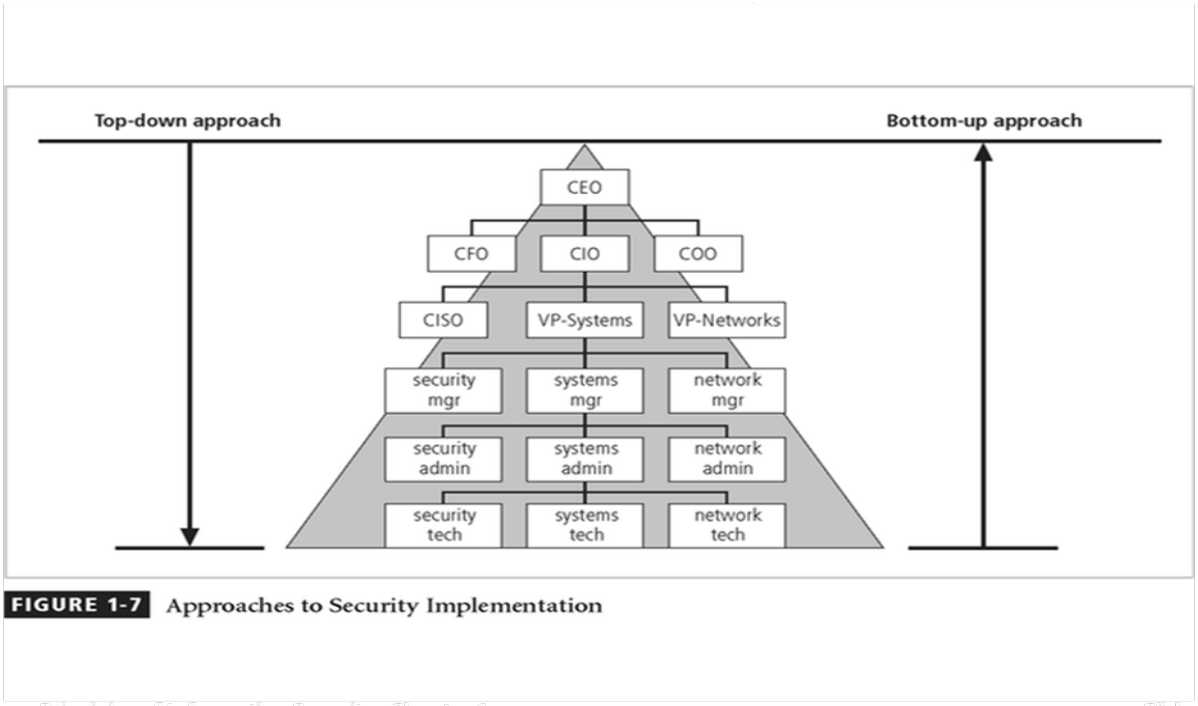



**FIGURE 1-7** Approaches to Security Implementation



Key concept here is the direction of the left and right side arrows to show where planning is sourced and from which direction the pressure for success if driven.

**Top-down Approach to Security Implementation**

An alternative approach, which has a higher probability of success, is called the top-down approach. The project is initiated by upper management who issue policy, procedures and processes, dictate the goals and expected outcomes of the project, and determine who is accountable for each of the required actions.

The top-down approach has strong upper management support, a dedicated champion, dedicated funding, clear planning and the opportunity to influence organizational culture.

The most successful top-down approach also involves a formal development strategy referred to as a systems development life cycle.

**The Systems Development Life Cycle**

Information security must be managed in a manner similar to any other major system implemented in the organization.

The best approach for implementing an information security system in an organization with little or no formal security in place, is to use a variation of the Systems Development Life Cycle (SDLC): the Security Systems Development Life Cycle (SecSDLC).

Methodology

The SDLC is a methodology for the design and implementation of an information system in an organization.

A methodology is a formal approach to solving a problem based on a structured sequence of procedures.

Using a methodology ensures a rigorous process, and avoids missing those steps that can lead to compromising the end goal.

The goal is creating a comprehensive security posture.

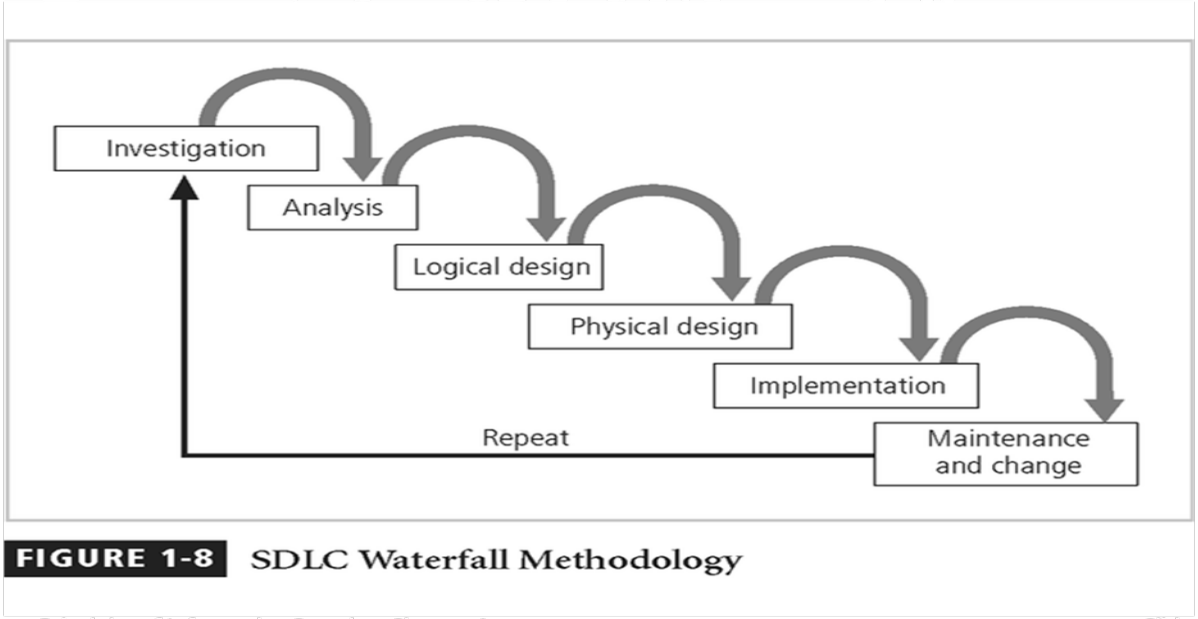



**FIGURE 1-8** SDLC Waterfall Methodology

## SDLC and the SecSDLC

The entire process may be initiated in response to specific conditions or combinations of conditions.

The impetus to begin the SecSDLC may be event-driven - started in response to some occurrence or plan-driven - as a result of a carefully developed implementation strategy.

At the end of each phase comes a structured review or "reality check" during which the team determines if the project should be continued, discontinued, outsourced, or postponed until additional expertise or organizational knowledge is acquired.

## Investigation

The first phase, investigation, is the most important.

What is the problem the system is being developed to solve?

This phase begins with an examination of the event or plan that initiates the process.

The objectives, constraints and scope of the project are specified. A preliminary cost/benefit analysis is developed to evaluate the perceived benefits and the appropriate levels of cost an organization is willing to expend to obtain those benefits.

A feasibility analysis is performed to assesses the economic, technical, and behavioral feasibilities of the process and to ensure that implementation is worth the organization's time and effort.

## Analysis

The analysis phase begins with the information learned during the investigation phase.

This phase consists primarily of assessments of the organization, the status of current systems, and the capability to support the proposed systems.

Analysts begin to determine what the new system is expected to do, and how it will interact with existing systems.

This phase ends with the documentation of the findings and a feasibility analysis update.

## Logical Design

In the logical design phase, the information gained from the analysis phase is used to begin creating a solution system for a business problem.

Then, based on the business need, select applications capable of providing needed services.

Based on the applications needed, select data support and structures capable of providing the needed inputs.

Finally, based on all of the above, select specific technologies to implement the physical solution.

In the end, another feasibility analysis is performed.

**Physical Design**

During the physical design phase, specific technologies are selected to support the alternatives identified and evaluated in the logical design.

The selected components are evaluated based on a make-or-buy decision (develop in-house or purchase from a vendor).

Final designs integrate various components and technologies.

After yet another feasibility analysis, the entire solution is presented to the end-user representatives for approval.

**Implementation**

In the implementation phase, any needed software is created or purchased

Components are ordered, received and tested.

Afterwards, users are trained and supporting documentation created.

Again a feasibility analysis is prepared, and the users are then presented with the system for a performance review and acceptance test.

**Maintenance and Change**

The maintenance and change phase is the longest and most expensive phase of the process.

This phase consists of the tasks necessary to support and modify the system for the remainder of its useful life cycle.

Even though formal development may conclude during this phase, the life cycle of the project continues until it is determined that the process should begin again from the investigation phase. When the current system can no longer support the changed mission of the organization, the project is terminated and a new project is implemented.

**The Security Systems Development Life Cycle**

The same phases used in the traditional SDLC can be adapted to support the specialized implementation of a security project.

The fundamental process is the identification of specific threats and the creation of specific controls to counter those threats.

The SecSDLC unifies the process and makes it a coherent program rather than a series of random, seemingly unconnected actions.

**Investigation**

The investigation of the SecSDLC begins with a directive from upper management, dictating the process, outcomes and goals of the project, as well as the constraints placed on the activity.

Frequently, this phase begins with a statement of program security policy that outlines the implementation of security.

Teams of responsible managers, employees and contractors are organized, problems analyzed, and scope defined, including goals objectives, and constraints not covered in the program policy.

Finally, an organizational feasibility analysis is performed to determine whether the organization has the resources and commitment necessary to conduct a successful security analysis and design.

**Analysis**

In the analysis phase, the documents from the investigation phase are studied.

The development team conducts a preliminary analysis of existing security policies or programs, along with documented current threats and associated controls.

This phase also includes an analysis of relevant legal issues that could impact the design of the security solution.

The risk management task - identifying, assessing and evaluating the levels of risk facing the organization, also begins in this stage.

**Logical Design**

The logical design phase creates and develops the blueprints for security, and examines and implements key policies that influence later decisions.

Also at this stage, critical planning is developed for incident response actions to be taken in the event of partial or catastrophic loss.

Next, a feasibility analysis determines whether or not the project should continue or should be outsourced.

**Physical Design**

In the physical design phase, the security technology needed to support the blueprint outlined in the logical design is evaluated, alternative solutions generated, and a final design agreed upon.

The security blueprint may be revisited to keep it synchronized with the changes needed when the physical design is completed.

Criteria needed to determine the definition of successful solutions is also prepared during this phase.

Included at this time are the designs for physical security measures to support the proposed technological solutions.

At the end of this phase, a feasibility study should determine the readiness of the organization for the proposed project, and then the champion and users are presented with the design.

At this time, all parties involved have a chance to approve the project before implementation begins.

**Implementation**

The implementation phase is similar to the traditional SDLC.

The security solutions are acquired (made or bought), tested, and implemented, and tested again.

Personnel issues are evaluated and specific training and education programs conducted.

Finally, the entire tested package is presented to upper management for final approval.

**Maintenance and Change**

The maintenance and change phase, though last, is perhaps most important, given the high level of ingenuity in today's threats.

The reparation and restoration of information is a constant duel with an often-unseen adversary.

As new threats emerge and old threats evolve, the information security profile of an organization requires constant adaptation to prevent threats from successfully penetrating sensitive data

**Security Professionals And The Organization**

It takes a wide range of professionals to support a diverse information security program.

To develop and execute specific security policies and procedures, additional administrative support and technical expertise is required

**Senior Management**

Chief Information Officer - the senior technology officer, although other titles such as Vice President of Information, VP of Information Technology, and VP of Systems may be used. The CIO is primarily responsible for advising the Chief Executive Officer, President or company owner on the strategic planning that affects the management of information in the organization.

Chief Information Security Officer - the individual primarily responsible for the assessment, management, and implementation of securing the information in the organization. The CISO may also be referred to as the Manager for Security, the Security Administrator, or a similar title.

**Security Project Team**

A number of individuals who are experienced in one or multiple requirements of both the technical and non-technical areas.

**The champion**: a senior executive who promotes the project and ensures its support, both financially and administratively, at the highest levels of the organization.

**The team leader**: a project manager, who may be a departmental line manager or staff unit manager, who understands project management, personnel management, and information security technical requirements.

**Security policy developers**: individuals who understand the organizational culture, policies, and requirements for developing and implementing successful policies.

**Risk assessment specialists**: individuals who understand financial risk assessment techniques, the value of organizational assets, and the security methods to be used.

**Security professionals**: dedicated, trained, and well-educated specialists in all aspects of information security from both technical and non-technical standpoints.

**Systems administrators**: individuals with the primary responsibility for administering the systems that house the information used by the organization.

**End users**: those the new system will most directly impact. Ideally, a selection of users from various departments, levels, and degrees of technical knowledge assist the team in focusing on the application of realistic controls applied in ways that do not disrupt the essential business activities they seek to safeguard.

**Data Ownership**

Now that you understand the responsibilities of both senior management and the security project team, we can define the roles of those who own and safeguard the data.

**Data Owner** - responsible for the security and use of a particular set of information. Data owners usually determine the level of data classification associated with the data, as well as changes to that classification required by organization change.

**Data Custodian** - responsible for the storage, maintenance, and protection of the information. The duties of a data custodian often include overseeing data storage and backups, implementing the specific procedures and policies laid out in the security policies and plans, and reporting to the data owner.

**Data Users** - the end systems users who work with the information to perform their daily jobs supporting the mission of the organization. Everyone in the organization is responsible for the security of data, so data users are included here as individuals with an information security role.

**Communities Of Interest**

Each organization develops and maintains its own unique culture and values. Within that corporate culture, there are communities of interest.

These include:

- Information Security Management and Professionals
- Information Technology Management and Professionals
- Organizational Management and Professionals

**Information Security: Is It An Art Or A Science?**

With the level of complexity in today's information systems, the implementation of information security has often been described as a combination of art and science.

The concept of the security artesian is based on the way individuals perceived systems technologists since computers became commonplace.

**Security as Art**

There are no hard and fast rules regulating the installation of various security mechanisms.

Nor are there many universally accepted complete solutions.

While there are many manuals to support individual systems, once these systems are interconnected, there is no magic user's manual for the security of the entire system.

This is especially true with the complex levels of interaction between users, policy, and technology controls.

**Security as Science**

We are dealing with technology developed by computer scientists and engineers—technology designed to perform at rigorous levels of performance.

Even with the complexity of the technology, most scientists would agree that specific scientific conditions cause virtually all actions that occur in computer systems.

Almost every fault, security hole, and systems malfunction is a result of the interaction of specific hardware and software.

If the developers had sufficient time, they could resolve and eliminate these faults.

**Security as a Social Science**

There is a third view: security as a social science.

Social science examines the behavior of individuals as they interact with systems, whether societal systems or in our case information systems.

Security begins and ends with the people inside the organization and the people that interact with the system planned or otherwise.

End users that need the very information the security personnel are trying to protect may be the weakest link in the security chain.

By understanding some of the behavioral aspects of organizational science and change management, security administrators can greatly reduce the levels of risk caused by end users, and create more acceptable and supportable security profiles.

# The Need for Security

## INTRODUCTION

Information security is unlike any other aspect of information technology. It is an arena where the primary mission is to ensure things stay the way they are.

If there were no threats to information and systems, we could focus on improving systems that support the information, resulting in vast improvements in ease of use and usefulness.

The first phase, Investigation, provides an overview of the environment in which security must operate, and the problems that security must address.

## BUSINESS NEEDS FIRST, TECHNOLOGY NEEDS LAST

Information security performs four important functions for an organization:

1. Protects the organization's ability to function
2. Enables the safe operation of applications implemented on the organization's IT systems
3. Protects the data the organization collects and uses
4. Safeguards the technology assets in use at the organization

### Protecting the Ability of the Organization to Function

Both general management and IR management are responsible for implementing information security to protect the ability of the organization to function.

"information security is a management issue in addition to a technical issue, it is a people issue in addition to the technical issue."

To assist management in addressing the needs for information security, communities of interest must communicate in terms of business impact and the cost of business interruption and avoid arguments expressed only in technical terms.

**Enabling the Safe Operation of Applications**

Today's organizations are under immense pressure to create and operate integrated, efficient, and capable applications.

The modern organization needs to create an environment that safeguards applications using the organization's IT systems, particularly the environment of the organization's infrastructure.

Once the infrastructure is in place, management must understand it has not abdicated to the IT department its responsibility to make choices and enforce decisions, but must continue to oversee the infrastructure.

**Protecting Data Organizations Collect and Use**

Many organizations realize that one of their most valuable assets is their data, because without data, an organization loses its record of transactions and/or its ability to deliver value to its customers.

Protecting data in motion and data at rest are both critical aspects of information security.

An effective information security program is essential to the protection of the integrity and value of the organization's data.

**Safeguarding the Technology Assets in Organizations**

To perform effectively, organizations must add secure infrastructure services based on the size and scope of the enterprise.

When an organization grows and more capabilities are needed, additional security services may have to be provided locally.

Likewise, as the organization's network grows to accommodate changing needs, more robust technology solutions may be needed to replace security programs the organization has outgrown.

## THREATS TO INFORMATION SECURITY

To make sound decisions about information security, create policies, and enforce them, management must be informed of the various kinds of threats facing the organization, its applications, data and information systems.

A threat is an object, person, or other entity that represents a constant danger to an asset.

To better understand the numerous threats facing the organization, a categorization scheme has been developed allowing us to group threats by their respective activities.

By examining each threat category in turn, management can most effectively protect its information through policy, education and training, and technology controls.

The 2002 Computer Security Institute/Federal Bureau of Investigation (CSI/FBI) survey on Computer Crime and Security Survey found:

90% of organizations responding, primarily large corporations and government agencies, detected computer security breaches within the last year.

80% of these organizations lost money to computer breaches, totaling over $455,848,000 up from $377,828,700 reported in 2001.

The number of attacks that came across the Internet rose from 70% in 2001 to 74% in 2002.

Only 34% of organizations reported their attacks to law enforcement.

**TABLE 2-1** Threats to Information Security[4]

| Categories of threat | Examples |
|---|---|
| 1. Acts of human error or failure | Accidents, employee mistakes |
| 2. Compromises to intellectual property | Piracy, copyright infringement |
| 3. Deliberate acts of espionage or trespass | Unauthorized access and/or data collection |
| 4. Deliberate acts of information extortion | Blackmail of information disclosure |
| 5. Deliberate acts of sabotage or vandalism | Destruction of systems or information |
| 6. Deliberate acts of theft | Illegal confiscation of equipment or information |
| 7. Deliberate software attacks | Viruses, worms, macros, denial-of-service |
| 8. Forces of nature | Fire, flood, earthquake, lightning |
| 9. Deviations in quality of service from service providers | Power and WAN service issues |
| 10. Technical hardware failures or errors | Equipment failure |
| 11. Technical software failures or errors | Bugs, code problems, unknown loopholes |
| 12. Technological obsolescence | Antiquated or outdated technologies |

**Potential Acts of Human Error or Failure**

This category includes the possibility of acts performed without intent or malicious purpose by an individual who is an employee of an organization.

Inexperience, improper training, the making of incorrect assumptions, and other circumstances can cause problems.

Employees constitute one of the greatest threats to information security, as the individuals closest to the organizational data.

Employee mistakes can easily lead to the following: revelation of classified data, entry of erroneous data, accidental deletion or modification of data, storage of data in unprotected areas, and failure to protect information.

Many threats can be prevented with controls, ranging from simple procedures, such as requiring the user to type a critical command twice, to more complex procedures, such as the verification of commands by a second party.


**FIGURE 2-1** Acts of Human Error or Failure

## Potential Deviations in Quality of Service by Service Providers

This category represents situations in which a product or services are not delivered to the organization as expected.

The organization's information system depends on the successful operation of many inter-dependent support systems including, power grids, telecom networks, parts suppliers, service vendors, and even the janitorial staff and garbage haulers.

Internet service, communications, and power irregularities are three sets of service issues that dramatically affect the availability of information and systems.

## Internet Service Issues

For organizations that rely heavily on the Internet and the Web to support continued operations, the threat of the potential loss of Internet service can lead to considerable loss in the availability of information.

Many organizations have sales staff and telecommuters working at remote locations.

When an organization places its web servers in the care of a Web Hosting provider, that outsourcer assumes responsibility for all Internet Services as well as for the hardware and operating system software used to operate the web site.

## Communications and other Service Provider Issues

Other utility services can impact organizations as well.

Among these are telephone, water, wastewater, trash pickup, cable television, natural, or propane gas, and custodial services.

The threat of loss of these services can lead to the inability of an organization to function properly.

## Power Irregularities

The threat of irregularities from power utilities are common and can lead to fluctuations such as power excesses, power shortages, and power losses.

In the U.S., buildings are "fed" 120-volt, 60-cycle power usually through 15 and 20 amp circuits.

Voltage levels can:

**spike** – momentary increase or surge – prolonged increase;

**sag** – momentary low voltage, or brownout – prolonged drop;

**fault** – momentary loss of power, or blackout – prolonged loss;

Since sensitive electronic equipment, especially networking equipment, computers, and computer-based systems are susceptible to fluctuations, controls can be applied to manage power quality.

## Deliberate Acts of Espionage or Trespass

This threat represents a well-known and broad category of electronic and human activities that breach the confidentiality of information.

When an unauthorized individual gains access to the information an organization is trying to protect, that act is categorized as a deliberate act of espionage or trespass.

When information gatherers employ techniques that cross the threshold of what is legal and/or ethical, they enter the world of industrial espionage.

Instances of shoulder surfing occur at computer terminals, desks, ATM machines, public phones, or other places where a person is accessing confidential information.

### Deliberate Acts of Espionage or Trespass

The threat of Trespass can lead to unauthorized, real or virtual actions that enable information gatherers to enter premises or systems they have not been authorized to enter.

Controls are sometimes implemented to mark the boundaries of an organization's virtual territory.

These boundaries give notice to trespassers that they are encroaching on the organization's cyberspace.

The classic perpetrator of deliberate acts of espionage or trespass is the hacker.

In the gritty world of reality, a hacker uses skill, guile, or fraud to attempt to bypass the controls placed around information that is the property of someone else. The hacker frequently spends long hours examining the types and structures of the targeted systems.

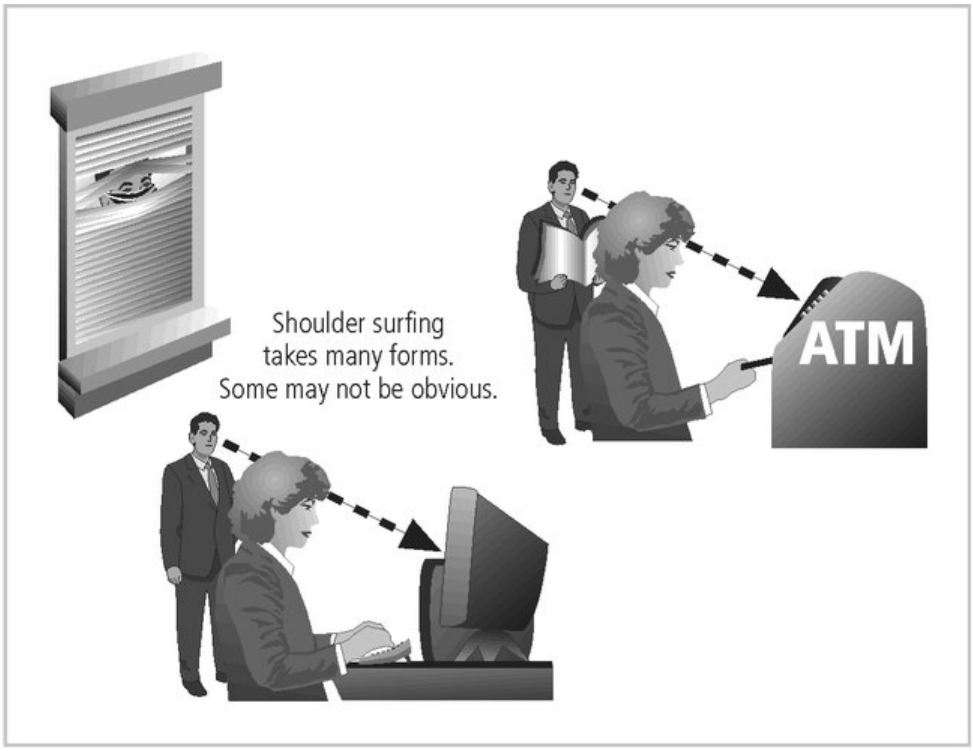



**FIGURE 2-2** Shoulder Surfing

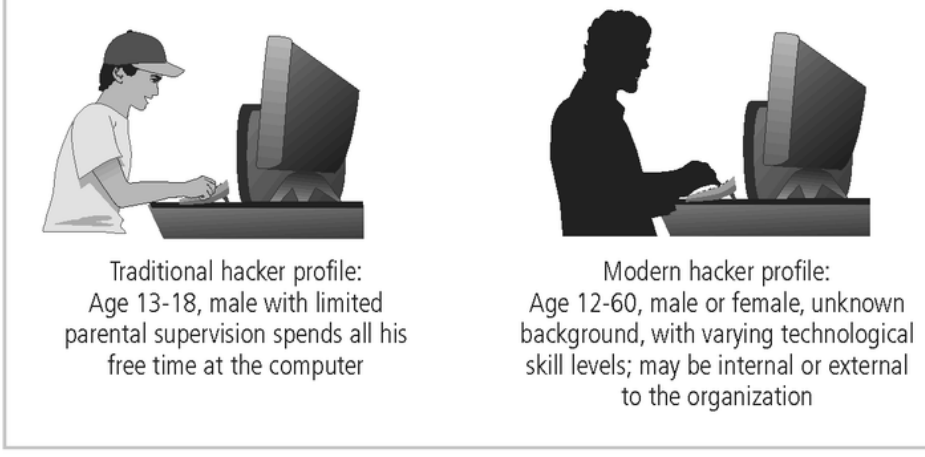



**FIGURE 2-3** Hacker Profiles

There are generally two skill levels among hackers.

The first is the expert hacker, who develops software scripts and codes exploits used by the second category, the novice, or unskilled hacker.

The expert hacker is usually a master of several programming languages, networking protocols, and operating systems and also exhibits a mastery of the technical environment of the chosen targeted system.

However, expert hackers have now become bored with directly attacking systems, and have turned to writing software.

The software they are writing is automated exploits that allow novice hackers to become script kiddies, hackers of limited skill who use expert-written software to exploit a system, but do not fully understand or appreciate the systems they hack.

As a result of preparation and continued vigilance, attacks conducted by scripts are usually predictable, and can be adequately defended against.

There are other terms for system rule breakers :

The term cracker is now commonly associated with an individual who “cracks” or removes the software protection from an application designed to prevent unauthorized duplication.

A phreaker hacks the public telephone network to make free calls, disrupt services, and generally wreak havoc.

**Deliberate Acts of Information Extortion**

The threat of information extortion is the possibility of an attacker or formerly trusted insider stealing information from a computer system and demanding compensation for its return or for an agreement to not disclose the information.

Extortion is common in credit card number theft.

**Deliberate Acts of Sabotage or Vandalism**

Equally popular today is the assault on the electronic face of an organization, its Web site.

This category of threat addresses the individual or group of individuals who want to deliberately sabotage the operations of a computer system or business, or perform acts of vandalism to either destroy an asset or damage the image of the organization.

These threats can range from petty vandalism by employees to organized sabotage against an organization.

Organizations frequently rely on image to support the generation of revenue, so if an organization's Web site is defaced, a drop in consumer confidence is probable, reducing the organization's sales and net worth.

Compared to Website defacement, vandalism within a network is more malicious in intent and less public.

Today, security experts are noticing a rise in another form of online vandalism in what are described as hacktivist or cyber-activist operations. A more extreme version is referred to as cyber-terrorism.

**Deliberate Acts of Theft**

Theft is the illegal taking of another's property. Within an organization, that property can be physical, electronic, or intellectual.

The value of information suffers when it is copied and taken away without the owner's knowledge.

Physical theft can be controlled quite easily. A wide variety of measures can be used from simple locked doors, to trained security personnel, and the installation of alarm systems.

Electronic theft, however, is a more complex problem to manage and control. Organizations may not even know it has occurred.

**Deliberate Software Attacks**

Deliberate software attacks occur when an individual or group designs software to attack an unsuspecting system. Most of this software is referred to as malicious code or malicious software, or sometimes malware.

These software components or programs are designed to damage, destroy, or deny service to the target systems.

Some of the more common instances of malicious code are viruses and worms, Trojan horses, logic-bombs, back doors, and denial-of-services attacks.

Computer viruses are segments of code that perform malicious actions.

This code behaves very much like a virus pathogen attacking animals and plants, using the cell's own replication machinery to propagate and attack.

The code attaches itself to the existing program and takes control of that program's access to the targeted computer.

The virus-controlled target program then carries out the virus's plan, by replicating itself into additional targeted systems.

The macro virus is embedded in the automatically executing macro code, common in office productivity software like word processors, spread sheets, and database applications.

The boot virus, infects the key operating systems files located in a computer's boot sector.

Worms - malicious programs that replicate themselves constantly without requiring another program to provide a safe environment for replication. Worms can continue replicating themselves until they completely fill available resources, such as memory, hard drive space, and network bandwidth.

Trojan horses - software programs that hide their true nature, and reveal their designed behavior only when activated. Trojan horses are frequently disguised as helpful, interesting or necessary pieces of software, such as readme.exe files often included with shareware or freeware packages.

Back door or Trap door - A virus or worm can have a payload that installs a back door or trap door component in a system. This allows the attacker to access the system at will with special privileges.

Polymorphism - A threat that changes its apparent shape over time, representing a new threat not detectable by techniques that are looking for a pre-configured signature. These threats actually evolve variations in size and appearance to elude detection by anti-virus software programs, making detection more of a challenge.

Virus and Worm Hoaxes - As frustrating as viruses and worms are, perhaps more time and money is spent on resolving virus hoaxes. Well-meaning people spread the viruses and worms when they send e-mails warning of fictitious or virus laden threats.

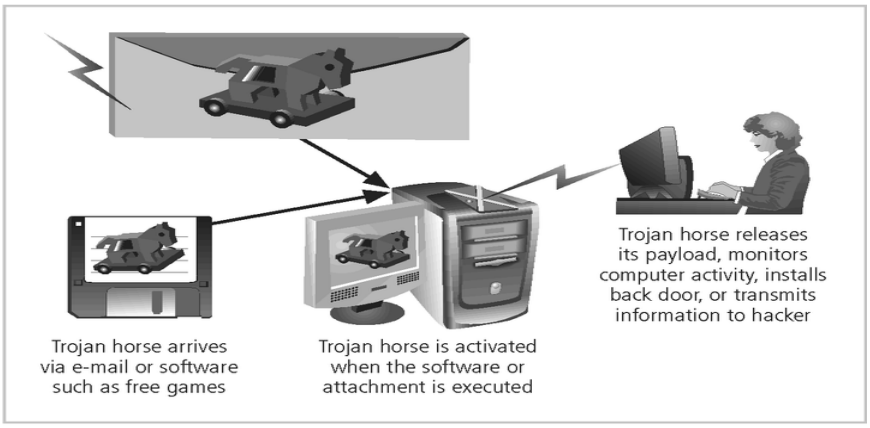



**FIGURE 2-8** Trojan Horse Attack

## Compromises to Intellectual Property

Many organizations create or support the development of intellectual property as part of their business operations.

Intellectual property is defined as “the ownership of ideas and control over the tangible or virtual representation of those ideas.”

Intellectual property for an organization includes trade secrets, copyrights, trademarks, and patents.

Once intellectual property (IP) has been defined, and properly identified, breaches to IP constitute a threat to the security of this information.

Most common in IP breaches involve the unlawful use or duplication of software-based intellectual property, known as software piracy.

In addition to the laws surrounding software piracy, two watchdog organizations investigate allegations of software abuse: Software & Information Industry Association (SIIA) formerly the Software Publishers Association, and the Business Software Alliance (BSA).

Enforcement of copyright violations, piracy, and the like has been attempted through a number of technical security mechanisms, including digital watermarks, embedded codes.

Many organizations create or support the development of intellectual property as part of their business operations.

Intellectual property is defined as “the ownership of ideas and control over the tangible or virtual representation of those ideas.”

Intellectual property for an organization includes trade secrets, copyrights, trademarks, and patents.

Once intellectual property (IP) has been defined, and properly identified, breaches to IP constitute a threat to the security of this information.

Most common in IP breaches involve the unlawful use or duplication of software-based intellectual property, known as software piracy.

In addition to the laws surrounding software piracy, two watchdog organizations investigate allegations of software abuse: Software & Information Industry Association (SIIA) formerly the Software Publishers Association, and the Business Software Alliance (BSA).

Enforcement of copyright violations, piracy, and the like has been attempted through a number of technical security mechanisms, including digital watermarks, embedded codes.

## Forces of Nature

Forces of nature, force majeure, or acts of God pose the most dangerous threats, because they are unexpected and can occur with very little warning.

These threats can disrupt not only the lives of individuals, but also the storage, transmission, and use of information.

These include fire, flood, earthquake, and lightning as well as volcanic eruption and insect infestation.

Since it is not possible to avoid many of these threats, management must implement controls to limit damage and also prepare contingency plans for continued operations.

## Technical Hardware Failures or Errors

Technical hardware failures or errors occur when a manufacturer distributes to users equipment containing a known or unknown flaw.

These defects can cause the system to perform outside of expected parameters, resulting in unreliable service or lack of availability.

Some errors are terminal, in that they result in the unrecoverable loss of the equipment. Some errors are intermittent, in that they only periodically manifest themselves, resulting in faults that are not easily repeated.

## Technical Software Failures or Errors

This category of threats comes from purchasing software with unknown, hidden faults.

Large quantities of computer code are written, debugged, published, and sold only to determine that not all bugs were resolved.

Sometimes, unique combinations of certain software and hardware reveal new bugs.

Sometimes, these items aren't errors, but are purposeful shortcuts left by programmers for honest or dishonest reasons.

## Technological Obsolescence

When the infrastructure becomes antiquated or outdated, it leads to unreliable and untrustworthy systems.

Management must recognize that when technology becomes outdated, there is a risk of loss of data integrity to threats and attacks.

Ideally, proper planning by management should prevent the risks from technology obsolesce, but when obsolescence is identified, management must take immediate action.

## ATTACKS

An attack is the deliberate act that exploits vulnerability.

It is accomplished by a threat-agent to damage or steal an organization's information or physical asset.

An exploit is a technique to compromise a system. Vulnerability is an identified weakness of a controlled system whose controls are not present or are no longer effective. An attack is then the use of an exploit to achieve the compromise of a controlled system.

### Malicious Code

This kind of attack includes the execution of viruses, worms, Trojan horses, and active web scripts with the intent to destroy or steal information.

The state of the art in attacking systems in 2002 is the multi-vector worm.

These attack programs use up to six known attack vectors to exploit a variety of vulnerabilities in commonly found information system devices.

| Sr. No. | Key | Threat | Attack |
|---|---|---|---|
| 1 | Intentional | Threats can be intentional like human negligence/failure or unintentional like natural disaster. | The attack is a deliberate action. An attacker have a motive and plan the attack accordingly. |
| 2 | Malicious | The threat may or may not malicious. | The attack is always malicious. |
| 3 | Definition | The threat by definition is a condition/circumstance which can cause damage to the system/asset. | Attack by definition, is an intended action to cause damage to system/asset. |
| 4 | Chance for Damage | Chance to damage or information alteration varies from low to very high. | The chance to damage or information alternation is very high. |
| 5 | Detection | A threat is difficult to detect. | An attack is comparatively easy to detect. |
| 6 | Prevention | A threat can be prevented by controlling the vulnerabilities. | An attack cannot be prevented by merely controlling the vulnerabilities. Other measures like backup, detect and act etc are required to handle a cyber-attack. |

**TABLE 2-2** Attack Replication Vectors

| Vector | Description |
|---|---|
| IP scan and attack | Infected system scans random or local range of IP addresses and targets any of several vulnerabilities known to hackers or left over from previous exploits such as Code Red, Back Orifice, or PoizonBox |
| Web browsing | If the infected system has write access to any Web pages, it makes all Web content files (.html, .asp, .cgi, and others) infectious, so that users who browse to those pages become infected |
| Virus | Each infected machine infects certain common executable or script files on all computers to which it can write with virus code that can cause infection |
| Shares | Using vulnerabilities in file systems and the way many organizations configure them, it copies the viral component to all locations it can reach |
| Mass mail | By sending e-mail infections to addresses found in the infected system's address book, copies of the infection are sent to many users whose mail-reading programs automatically run the program and infect other systems |
| Simple Network Management Protocol (SNMP) | In early 2002, the SNMP vulnerabilities known to many in the IT industry were brought to the attention of the multi-vector attack community. SNMP buffer overflow and weak community string attacks are expected by the end of 2002 |

**Attack Descriptions**

IP Scan and Attack - Infected system scans random or local range of IP addresses and targets any of several vulnerabilities known to hackers or left over from previous exploits.

Web Browsing - If the Infected system has write access to any Web pages, it makes all Web content files infectious, so that users who browse to those pages become infected.

Virus - Each infected machine infects certain common executable or script files on all computers to which it can write with virus code that can cause infection.

Shares - Using vulnerabilities in file systems and the way many organizations configure them, it copies the viral component to all locations it can reach.

Mass Mail - By sending e-mail infections to addresses found in the infected systems address book, copies of the infection are sent to many users whose mail-reading programs automatically run the program and infect other systems.

Simple Network Management Protocol - In early 2002, the SNMP vulnerabilities known to many in the IT industry were brought to the attention of the multi-vector attack community.

Hoaxes - A more devious approach to attacking computer systems is the transmission of a virus hoax, with a real virus attached.

Back Doors - Using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource.

Password Crack - Attempting to reverse calculate a password.

Brute Force - The application of computing and network resources to try every possible combination of options of a password.

Dictionary - The dictionary password attack narrows the field by selecting specific accounts to attack and uses a list of commonly used passwords (the dictionary) to guess with.

Denial-of-service (DoS) - the attacker sends a large number of connection or information requests to a target. So many requests are made that the target system cannot handle them successfully along with other, legitimate requests for service. This may result in a system crash, or merely an inability to perform ordinary functions.

Distributed Denial-of-service (DDoS) - an attack in which a coordinated stream of requests is launched against a target from many locations at the same time.

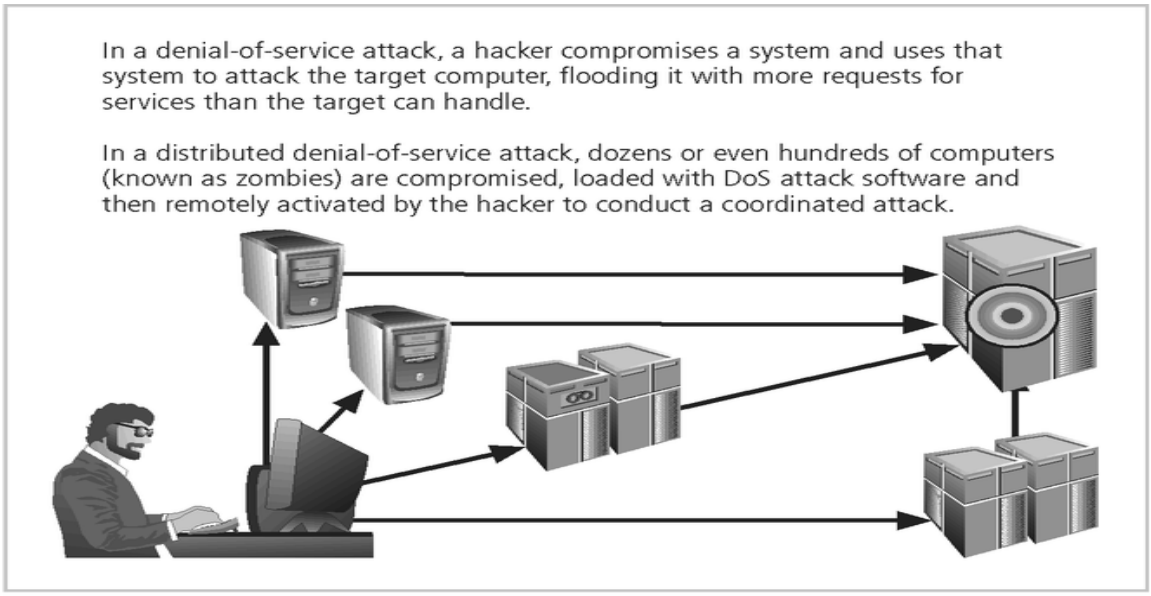



**FIGURE 2-9** Denial-of-Service Attacks

Spoofing - a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.

Man-in-the-Middle - In the man-in-the-middle or TCP hijacking attack, an attacker sniffs packets from the network, modifies them, and inserts them back into the network.

Spam - unsolicited commercial e-mail. While many consider Spam a nuisance rather than an attack, it is emerging as a vector for some attacks.

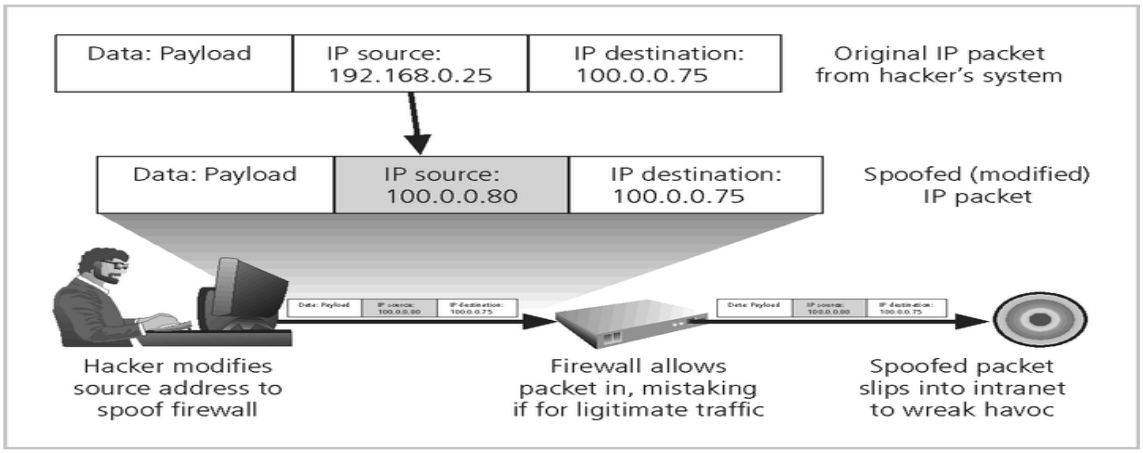



**FIGURE 2-10** IP Spoofing

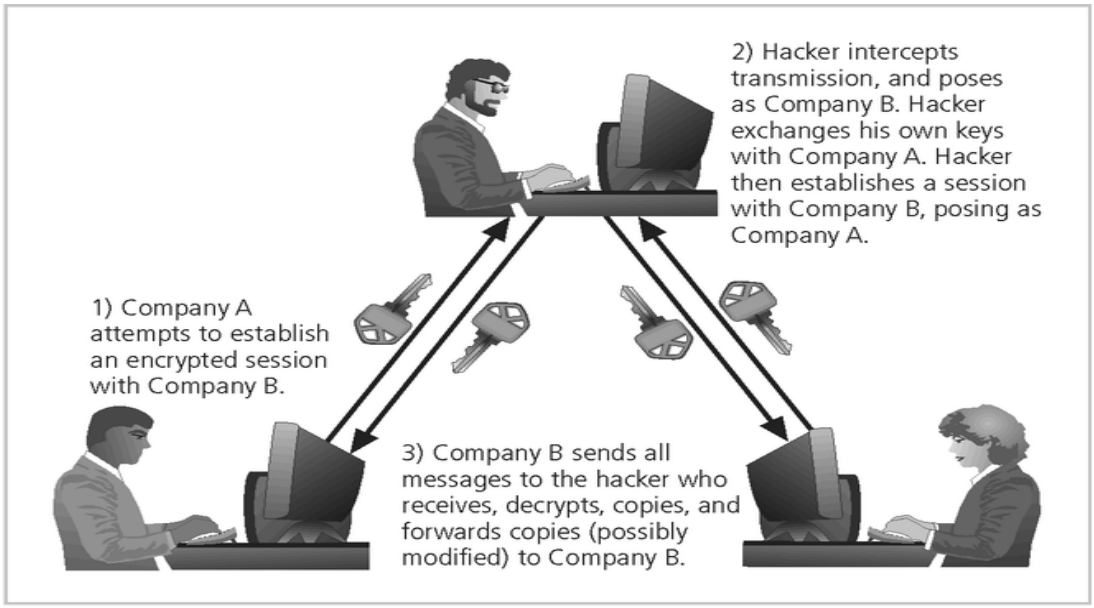



**FIGURE 2-11** Man-in-the-Middle Attack

Mail-bombing - Another form of e-mail attack that is also a DoS, in which an attacker routes large quantities of e-mail to the target.

Sniffers - a program and/or device that can monitor data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information from a network.

Social Engineering - Within the context of information security, the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker.

“People are the weakest link. You can have the best technology; firewalls, intrusion-detection systems, biometric devices ... and somebody can call an unsuspecting employee. That's all she wrote, baby. They got everything.”

“brick attack” – the best configured firewall in the world can’t stand up to a well placed brick.

Buffer Overflow - an application error that occurs when more data is sent to a buffer than it can handle. When the buffer overflows, the attacker can make the target system execute instructions, or the attacker can take advantage of some other unintended consequence of the failure.

Timing Attack - relatively new, works by exploring the contents of a web browser’s cache. This could allow the designer to collect information on access to password-protected sites. Another attack by the same name involves attempting to intercept cryptographic elements to determine keys and encryption algorithms.