

1

Introduction to Information Security

Do not figure on opponents not attacking;
worry about your own lack of preparation.

BOOK OF THE FIVE RINGS

PRINCIPLES of
INFORMATION
SECURITY

Second Edition

Learning Objectives

Upon completion of this material, you should be able to:

- Understand the definition of information security
- Comprehend the history of computer security and how it evolved into information security
- Understand the key terms and critical concepts of information security as presented in the chapter
- Outline the phases of the security systems development life cycle
- Understand the roles of professionals involved in information security within an organization

Introduction

- Information security: a “well-informed sense of assurance that the information risks and controls are in balance.” —Jim Anderson, Inovant (2002)
- Necessary to review the origins of this field and its impact on our understanding of information security today

The History of Information Security

- Began immediately after the first mainframes were developed
- Created to aid code-breaking computations during World War II
- Physical controls to limit access to sensitive military locations to authorized personnel: badges, keys, and facial recognition
- Rudimentary in defending against physical theft, espionage, and sabotage



Earlier versions of the German code machine Enigma were first broken by the Poles in the 1930s. The British and Americans managed to break later, more complex versions during World War II. The increasingly complex versions of the Enigma, especially the submarine or *Unterseeboot* version of the Enigma, caused considerable anguish to allied forces before finally being cracked. The information gained from decrypted transmissions was used to anticipate the actions of German armed forces. "Some ask why, if we were reading the Enigma, we did not win the war earlier. One might ask, instead, when, if ever, we would have won the war if we hadn't read it."

Courtesy of National Security Agency

FIGURE 1-1 The Enigma²

The History of Information Security

- One of 1st documented problems
 - Early 1960s
 - Not physical
 - Accidental file switch
 - Entire password file
 - printed on every output file

The 1960s

- Additional mainframes online
- Advanced Research Procurement Agency (ARPA) began to examine feasibility of redundant networked communications
- Larry Roberts developed ARPANET from its inception
- ARPANET is the first Internet

ARPANET Program Plan

June 3, 1968

In ARPA, the Program Plan is the master document describing a major program. This plan, which I wrote in 1968, had the following concepts:

1. Objectives – Develop Networking and Resource Sharing
2. Technical Need – Linking Computers
3. Military Need – Resource Sharing - Not Nuclear War
4. Prior Work – MIT-SDC experiment
5. Effect on ARPA – Link 17 Computer Research Centers, Network Research Plan - Develop IMP's and start 12/69
6. Cost – \$3.4 M for 68-71

ADVANCED RESEARCH PROJECTS AGENCY
Washington, D.C. 20301

Program Plan No. 723

Date: 3 June 1968

RESOURCE SHARING COMPUTER NETWORKS

A. Objective of the Program.

The objective of this program is twofold: (1) To develop techniques and obtain experience on interconnecting computers in such a way that a very broad class of interactions are possible, and (2) To improve and increase computer research productivity through resource sharing. By establishing a network tying IPT's research centers together, both goals are achieved. In fact, the most efficient way to develop the techniques needed for an effective network is by involving the research talent at these centers in prototype activity.

Just as time-shared computer systems have permitted groups of hundreds of individual users to share hardware and software resources with one another, networks connecting dozens of such systems will permit resource sharing between thousands of users. Each system, by virtue of being time-shared, can offer any of its services to another computer system on demand. The most important criterion for the type of network interconnection desired is that any user or program on any of the networked computers can utilize any program or subsystem available on any other computer without having to modify the remote program.

Courtesy of Dr. Lawrence Roberts

FIGURE 1-2 ARPANET Program Plan⁴

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 ARPANET
 - Non-existent user identification and authorization to system

R-609

- Information security began with Rand Report R-609 (paper that started the study of computer security)
- Scope of computer security grew from physical security to include:
 - Safety of data
 - Limiting unauthorized access to data
 - Involvement of personnel from multiple levels of an organization
 - First identified role of management and policy

The History of Information Security

- Multics
 - Operating System
 - Security primary goal
 - Didn't go very far
 - Several developers created Unix
- Late 1970s: microprocessor expanded computing capabilities and security threats
 - From mainframe to PC
 - Decentralized computing
 - Need for sharing resources increased
 - Major changed computing

The 1990s

- Networks of computers became more common; so too did the need to interconnect networks
- Internet became first manifestation of a global network of networks
- In early Internet deployments, security was treated as a low priority
 - Many of the problems that plague e-mail on the Internet are the result to this early lack of security

The Present

- The Internet brings millions of computer networks into communication with each other—many of them unsecured
- Ability to secure a computer's data influenced by the security of every computer to which it is connected

What is Security?

- “The quality or state of being secure—to be free from danger”
- A successful organization should have multiple layers of security in place:
 - Physical security
 - Personal security
 - Operations security
 - Communications security
 - Network security
 - Information security

What is Information Security?

- The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information
- Necessary tools: policy, awareness, training, education, technology
- C.I.A. triangle was standard based on confidentiality, integrity, and availability
- C.I.A. triangle now expanded into list of critical characteristics of information

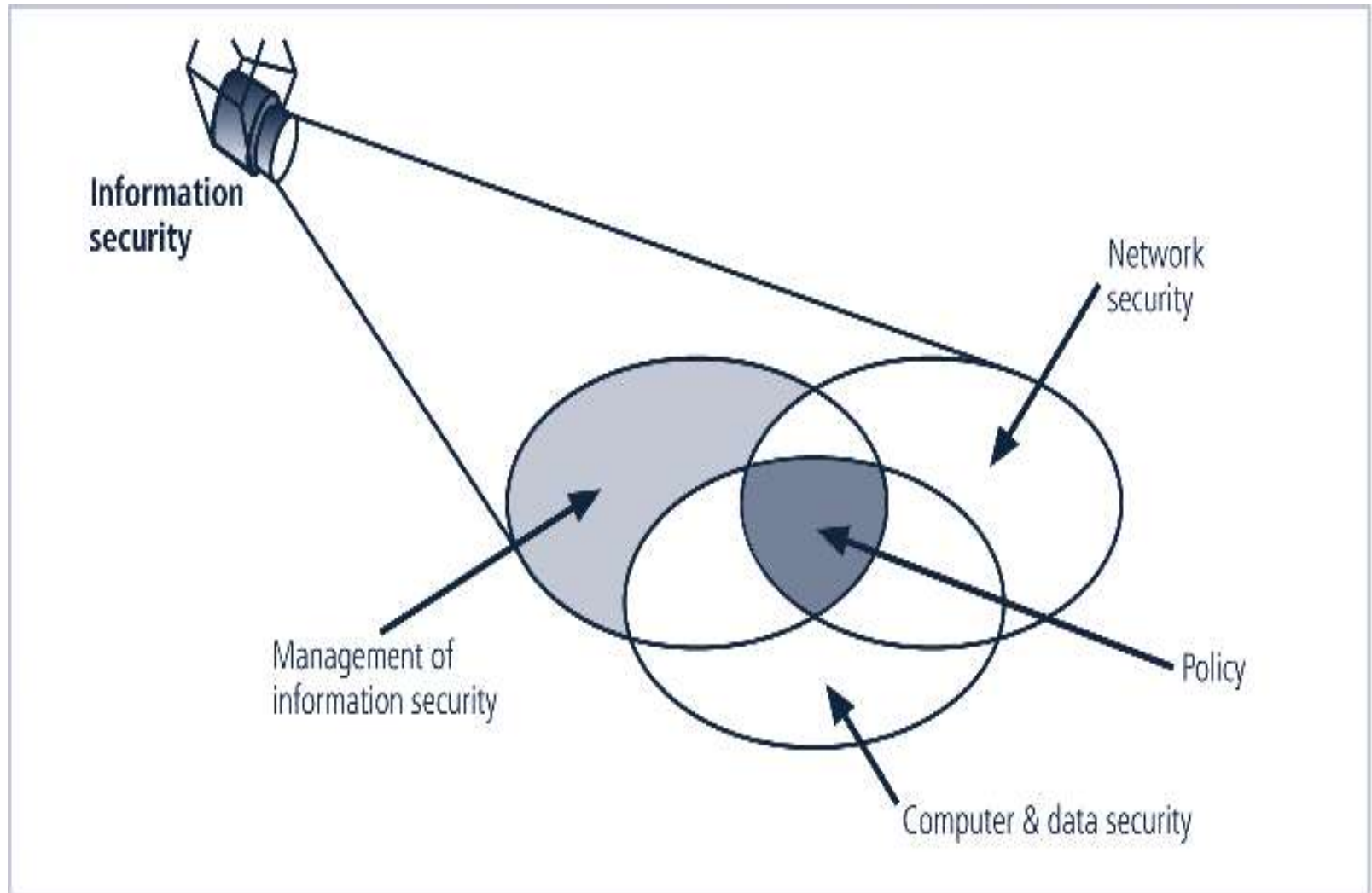


FIGURE 1-3 Components of Information Security

Critical Characteristics of Information

- The value of information comes from the characteristics it possesses:
 - Timeliness
 - No value if it is too late
 - Availability
 - No interference or obstruction
 - Required format
 - Accuracy
 - Free from mistakes
 - Authenticity
 - Quality or state of being genuine, i.e., sender of an email
 - Confidentiality
 - Disclosure or exposure to unauthorized individuals or system is prevented

Critical Characteristics of Information

- Integrity
 - Whole, completed, uncorrupted
 - Cornerstone
 - Size of the file, hash values, error-correcting codes, retransmission
- Utility
 - Having value for some purpose
- Possession
 - Ownership
 - Breach of confidentiality results in the breach of possession, not the reverse

NSTISSC Security Model

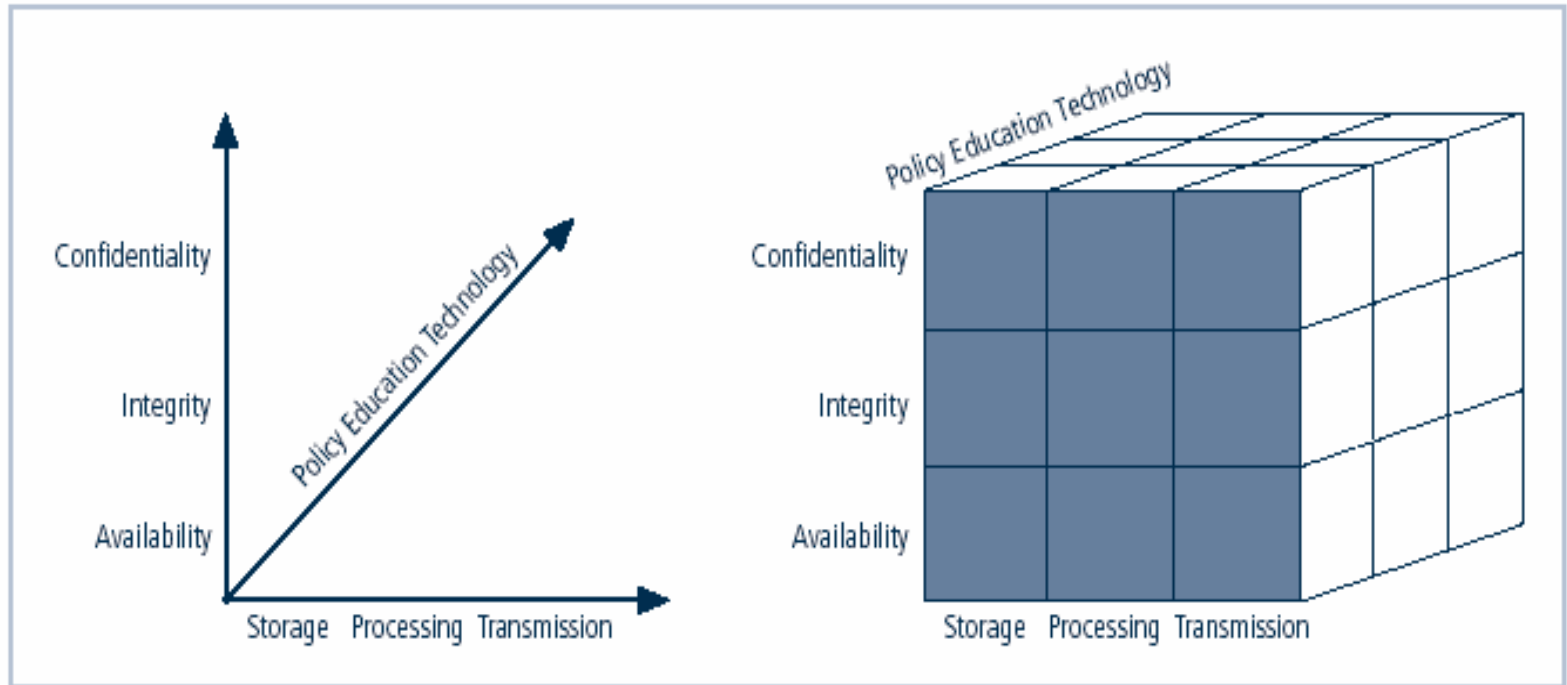


FIGURE 1-4 NSTISSC Security Model

Components of an Information System

- Information System (IS) is entire set of software, hardware, data, people, procedures, and networks necessary to use information as a resource in the organization
- Software
 - Perhaps most difficult to secure
 - Easy target
 - Exploitation substantial portion of attacks on information
- Hardware
 - Physical security policies
 - Securing physical location important
 - Laptops
 - Flash memory

Components of an Information System

- Data
 - Often most valuable asset
 - Main target of intentional attacks
- People
 - Weakest link
 - Social engineering
 - Must be well trained and informed
- Procedures
 - Threat to integrity of data
- Networks
 - Locks and keys won't work

Securing Components

- Computer can be subject of an attack and/or the object of an attack
 - When the subject of an attack, computer is used as an active tool to conduct attack
 - When the object of an attack, computer is the entity being attacked
- 2 types of attack
 - Direct
 - Hacker uses their computer to break into a system
 - Indirect
 - System is compromised and used to attack other systems

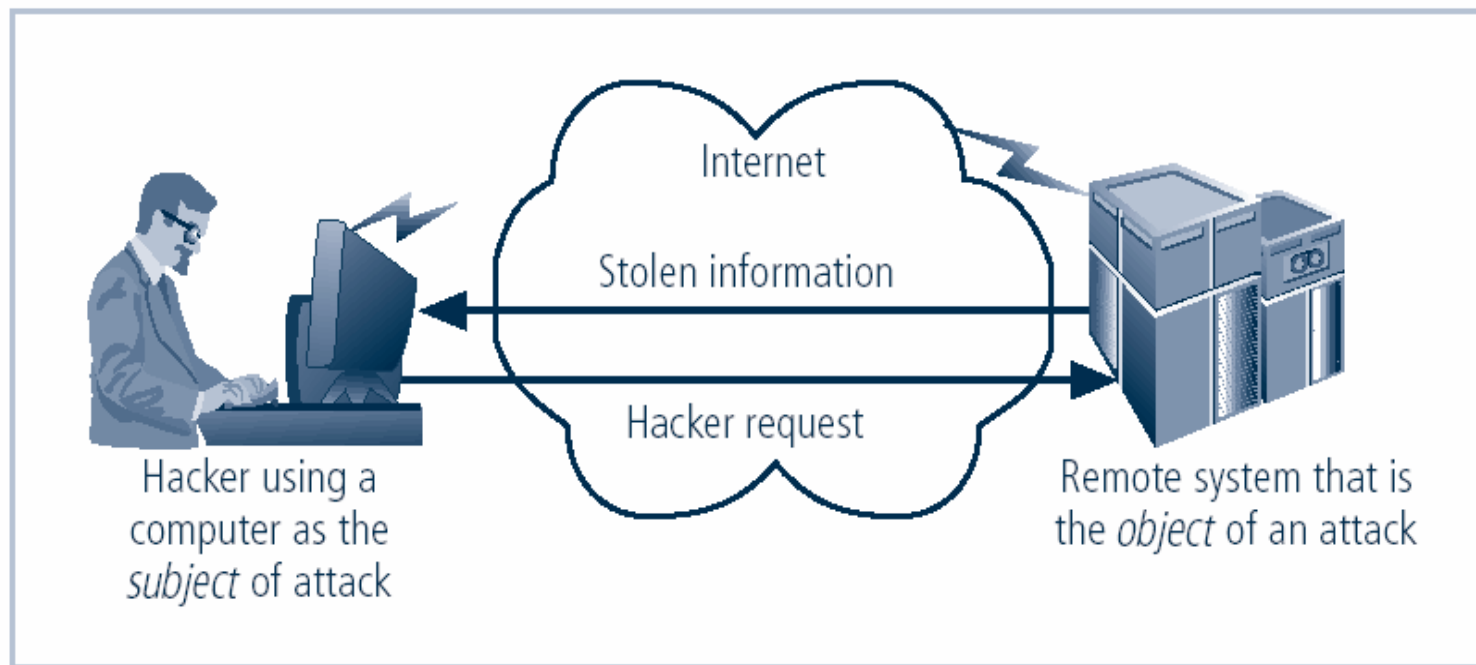


FIGURE 1-6 Computer as the Subject and Object of an Attack

Balancing Information Security and Access

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

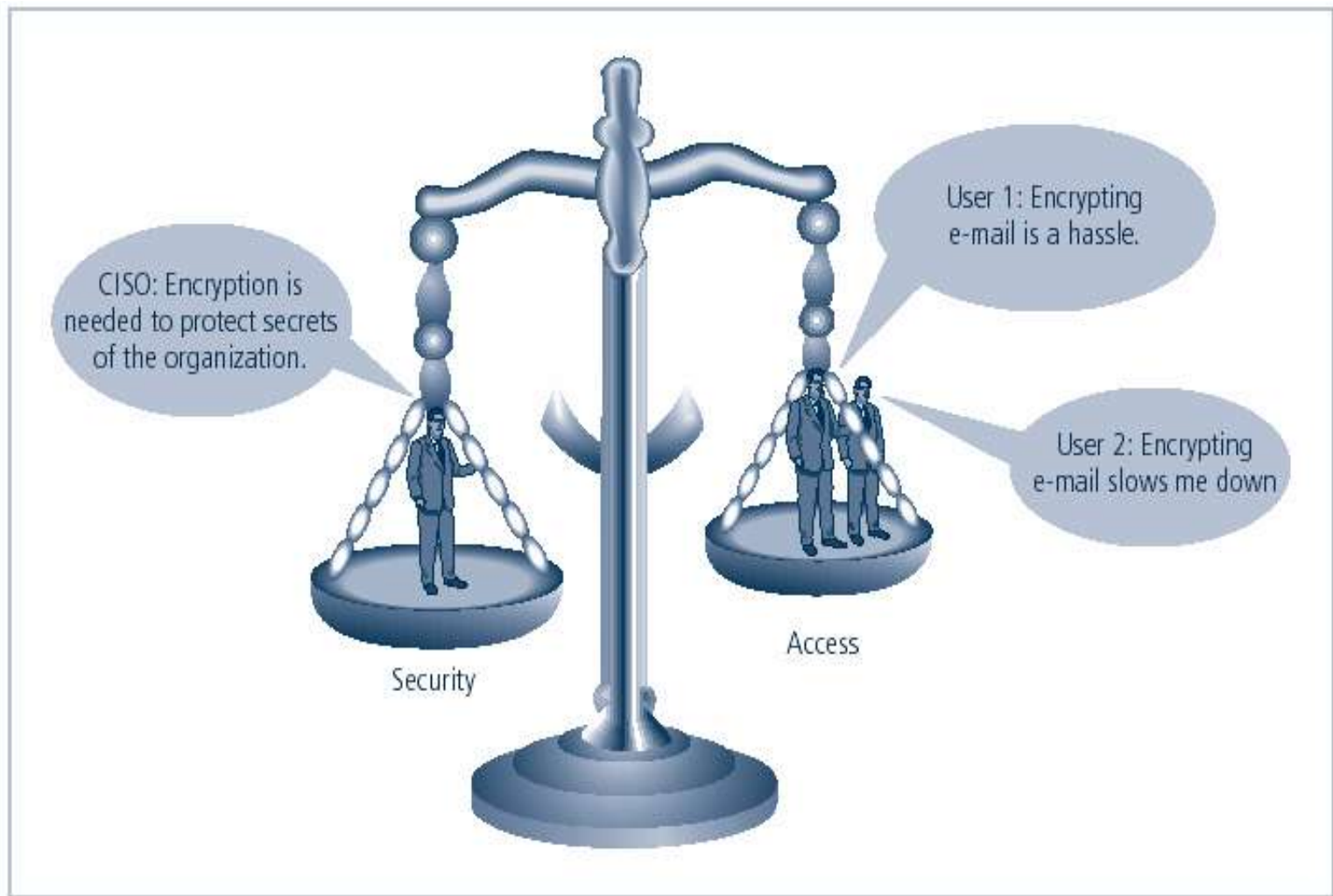


FIGURE 1-7 Balancing Information Security and Access

Approaches to Information Security

Implementation: Bottom-Up Approach

- Grassroots effort: systems administrators attempt to improve security of their systems
- Key advantage: technical expertise of individual administrators
- Seldom works, as it lacks a number of critical features:
 - Participant support
 - Organizational staying power

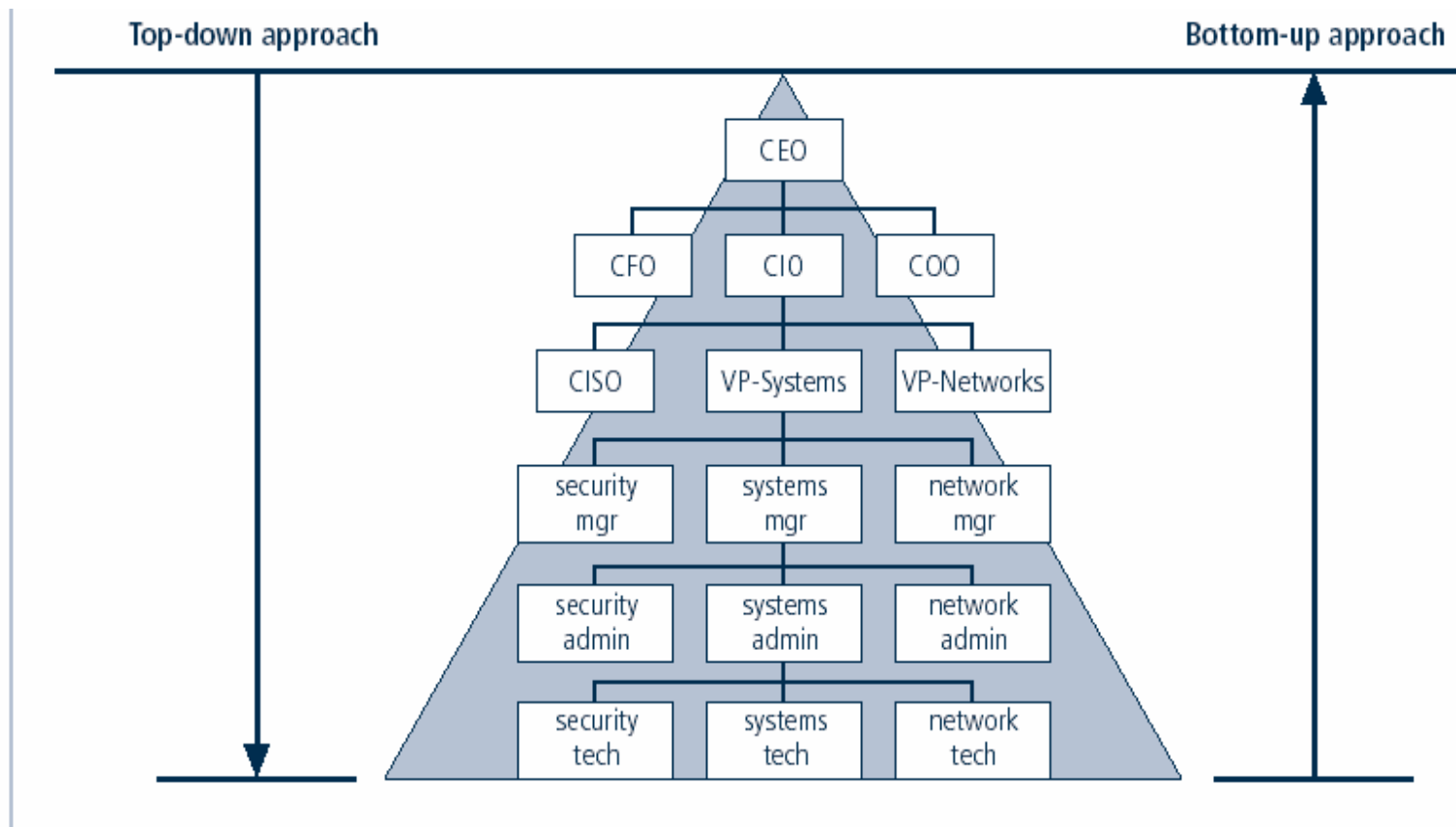


FIGURE 1-8 Approaches to Information Security Implementation

Approaches to Information Security Implementation: Top-Down Approach

- Initiated by upper management
 - Issue policy, procedures and processes
 - Dictate goals and expected outcomes of project
 - Determine accountability for each required action
- The most successful also involve formal development strategy referred to as systems development life cycle

The Systems Development Life Cycle

- Systems development life cycle (SDLC) is methodology and design for implementation of information security within an organization
- Methodology is formal approach to problem-solving based on structured sequence of procedures
- Using a methodology
 - ensures a rigorous process
 - avoids missing steps
- Goal is creating a comprehensive security posture/program
- Traditional SDLC consists of six general phases

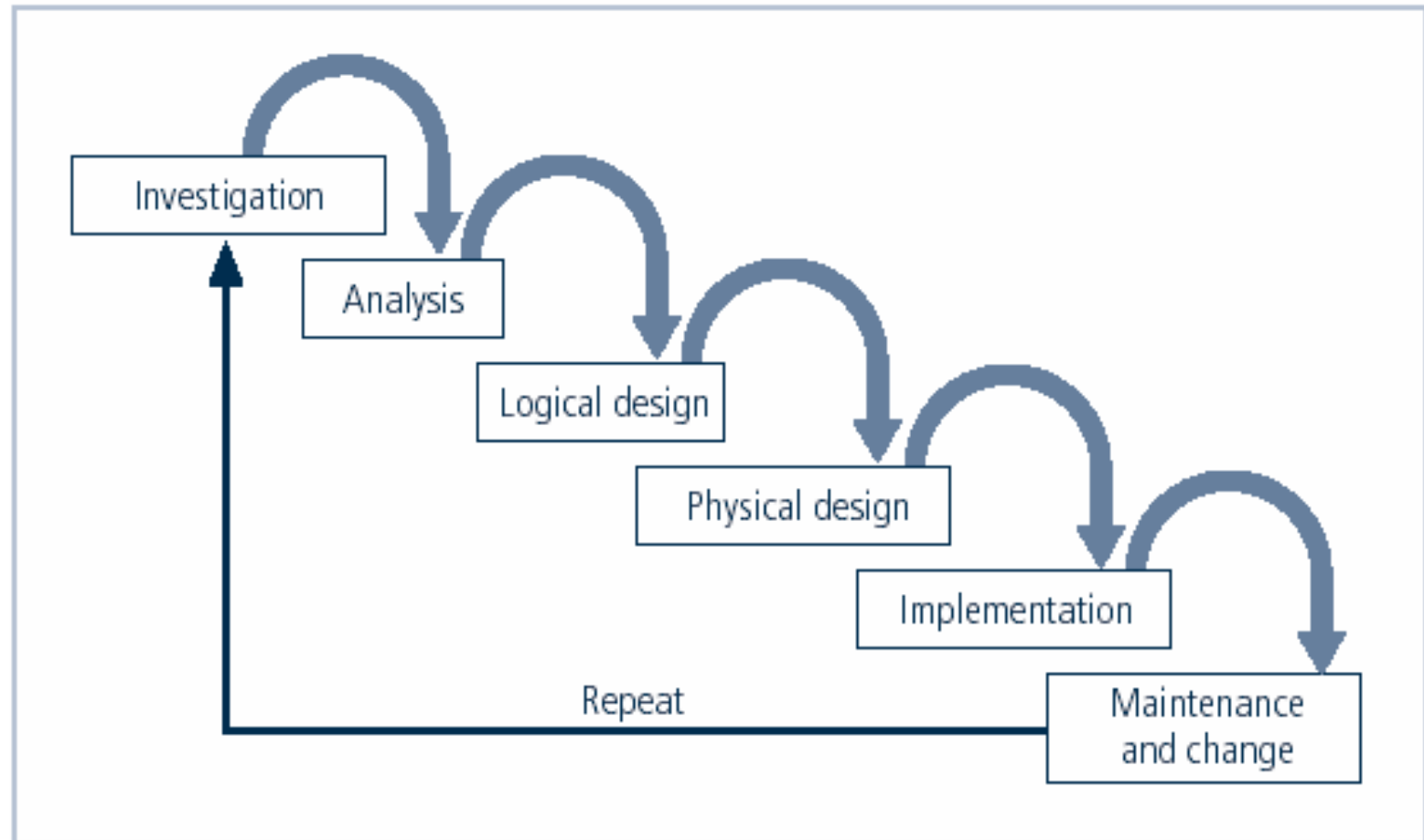


FIGURE 1-9 SDLC Waterfall Methodology

The Security Systems Development Life Cycle

- The same phases used in traditional SDLC may be adapted to support specialized implementation of an IS project
- Identification of specific threats and creating controls to counter them
- SecSDLC is a coherent program rather than a series of random, seemingly unconnected actions

The Security Systems Development Life Cycle

- Investigation
 - Identifies process, outcomes, goals, and constraints of the project
 - Begins with enterprise information security policy
- Analysis
 - Existing security policies, legal issues,
 - Perform risk analysis

The Security Systems Development Life Cycle

- Logical Design
 - Creates and develops blueprints for information security
 - Incident response actions: Continuity planning, Incident response, Disaster recovery
 - Feasibility analysis to determine whether project should continue or be outsourced
- Physical Design
 - Needed security technology is evaluated, alternatives generated, and final design selected

The Security Systems Development Life Cycle

- Implementation
 - Security solutions are acquired, tested, implemented, and tested again
 - Personnel issues evaluated; specific training and education programs conducted
 - Entire tested package is presented to management for final approval
- Maintenance and Change
 - Most important
 - Constant changing threats
 - Constant monitoring, testing updating and implementing change

Security Professionals and the Organization

- Wide range of professionals required to support a diverse information security program
- Senior management is key component; also, additional administrative support and technical expertise required to implement details of IS program

Senior Management

- Chief Information Officer (CIO)
 - Senior technology officer
 - Primarily responsible for advising senior executives on strategic planning
- Chief Information Security Officer (CISO)
 - Primarily responsible for assessment, management, and implementation of IS in the organization
 - Usually reports directly to the CIO

Information Security Project Team

- A number of individuals who are experienced in one or more facets of technical and non-technical areas:
 - Champion: Senior executive who promotes the project
 - Team leader: project manager, departmental level manager
 - Security policy developers
 - Risk assessment specialists
 - Security professionals
 - Systems administrators
 - End users

Data Ownership

- Data Owner: responsible for the security and use of a particular set of information
- Data Custodian: responsible for storage, maintenance, and protection of information
- Data Users: end users who work with information to perform their daily jobs supporting the mission of the organization

Communities Of Interest

- Group of individuals united by similar interest/values in an organization
 - Information Security Management and Professionals
 - Information Technology Management and Professionals
 - Organizational Management and Professionals

Key Terms

- Access
- Asset
- Attack
- Control, Safeguard or Countermeasure
- Exploit
- Exposure
- Hacking
- Object
- Risk
- Security Blueprint
- Security Model
- Security Posture or Security Profile
- Subject
- Threats
- Threat Agent
- Vulnerability

Critical infrastructure

- From Wikipedia.
- Critical infrastructure is a term used by [governments](#) to describe systems or material [assets](#) that are essential for the functioning of a society and economy. Most commonly associated with the term are facilities for:
 - [electricity generation](#) and distribution;
 - [telecommunication](#);
 - [water supply](#);
 - [agriculture](#), food production and distribution;
 - [heating](#) ([natural gas](#), [fuel oil](#));
 - [public health](#);
 - [transportation](#) systems (fuel supply, railway network, airports);
 - [financial services](#);
 - [security services](#) (police, military).
- Critical-infrastructure protection is the study, design and implementation of precautionary measures aimed to reduce the risk that critical infrastructure fails as the result of [war](#), [disaster](#), [civil unrest](#), [vandalism](#), or [sabotage](#).

Summary

- Information security is a “well-informed sense of assurance that the information risks and controls are in balance.”
- Computer security began immediately after first mainframes were developed
- Successful organizations have multiple layers of security in place: physical, personal, operations, communications, network, and information.

Summary

- Security should be considered a balance between protection and availability
- Information security must be managed similar to any major system implemented in an organization using a methodology like SecSDLC
- Implementation of information security often described as a combination of art and science

The Need For Security

*Our bad neighbor makes us early stirrers,
Which is both healthful and good husbandry.*

**-- William Shakespeare (1564–1616), King Henry, in Henry V,
act 4, sc. 1, l. 6-7.**

Learning Objectives

Upon completion of this lecture, you should be able to:

- Understand the need for information security.
- Understand a successful information security program is the responsibility of an organization's general management and IT management.
- Understand the threats posed to information security and the more common attacks associated with those threats.
- Differentiate threats to information systems from attacks against information systems.

Business Needs First, Technology Needs Last

Information security performs four important functions for an organization:

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

Protecting the Ability to Function

- Management is responsible
- Information security is
 - a management issue
 - a people issue
- Communities of interest must argue for information security in terms of impact and cost

Enabling Safe Operation

- Organizations must create integrated, efficient, and capable applications
- Organization need environments that safeguard applications
- Management must not abdicate to the IT department its responsibility to make choices and enforce decisions

Protecting Data

- One of the most valuable assets is data
- Without data, an organization loses its record of transactions and/or its ability to deliver value to its customers
- An effective information security program is essential to the protection of the integrity and value of the organization's data

Safeguarding Technology Assets

- Organizations must have secure infrastructure services based on the size and scope of the enterprise
- Additional security services may have to be provided
- More robust solutions may be needed to replace security programs the organization has outgrown

Hands-On Exercise (10 Minutes)

You are a security officer working for a medium-sized research company. You have been assigned to guard the facility. Two incidents occur. The first, a well-known manager walks out with a box of papers. The second, someone believed to be an outsider assesses the company information and goes away with the company blue prints for the next generation product.

1. Briefly list all security gaps, vulnerabilities, threats, risks, and exploits.
2. Describe how these incidents can be overcome.

Threats

- Management must be informed of the various kinds of threats facing the organization
- A threat is an object, person, or other entity that represents a constant danger to an asset
- By examining each threat category in turn, management effectively protects its information through policy, education and training, and technology controls



Threats

- The 2002 CSI/FBI survey found:
 - 90% of organizations responding detected computer security breaches within the last year
 - 80% 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



Threats to Information Security

TABLE 2-1 Threats to Information Security⁴

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

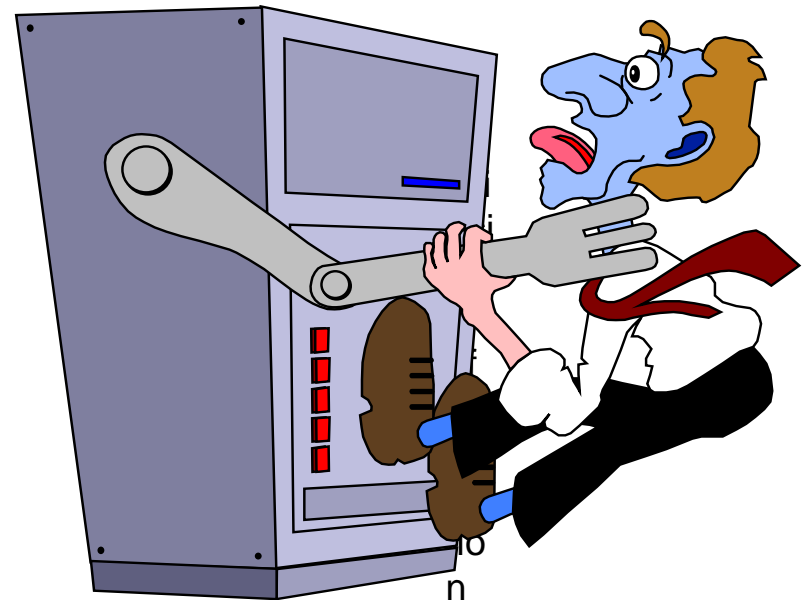
Acts of Human Error or Failure

- Includes acts done without malicious intent
- Caused by:
 - Inexperience
 - Improper training
 - Incorrect assumptions
 - Other circumstances
- Employees are greatest threats to information security – They are closest to the organizational data



Acts of Human Error or Failure

- 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
 - failure to protect information
- Many of these threats can be prevented with controls



Who is the biggest threat to your organization?



Tom Twostory
convicted burglar



Dick Davis a.k.a.
"wannabe amateur hacker"



Harriet Allthumbs
Employee
accidentally
deleted the one copy
of a critical report

FIGURE 2-1 Acts of Human Error or Failure

Deviations in Quality of Service by Service Providers

- Situations of product or services not delivered as expected
- Information system depends on many inter-dependent support systems
- Three sets of service issues that dramatically affect the availability of information and systems are
 - Internet service
 - Communications
 - Power irregularities

Internet Service Issues

- Loss of Internet service can lead to considerable loss in the availability of information
 - organizations have sales staff and telecommuters working at remote locations
- When an organization outsources its web servers, the outsourcer assumes responsibility for
 - All Internet Services
 - The hardware and operating system software used to operate the web site

Communications and Other Services

- Other utility services have potential impact
- Among these are
 - telephone
 - water & wastewater
 - trash pickup
 - cable television
 - natural or propane gas
 - custodial services
- The threat of loss of services can lead to inability to function properly

Power Irregularities

Voltage levels can increase, decrease, or cease:

- spike – momentary increase
- surge – prolonged increase
- sag – momentary low voltage
- brownout – prolonged drop
- fault – momentary loss of power
- blackout – prolonged loss
- Electronic equipment is susceptible to fluctuations, controls can be applied to manage power quality

Espionage/Trespass

Broad category of activities that breach confidentiality

- Unauthorized accessing of information
- Competitive intelligence vs. espionage
- Shoulder surfing can occur any place a person is accessing confidential information

Controls implemented to mark the boundaries of an organization's virtual territory giving notice to trespassers that they are encroaching on the organization's cyberspace

Hackers uses skill, guile, or fraud to steal the property of someone else



of
ma
tio
n
Se
cur
ity
-
Ch
apt
er
2

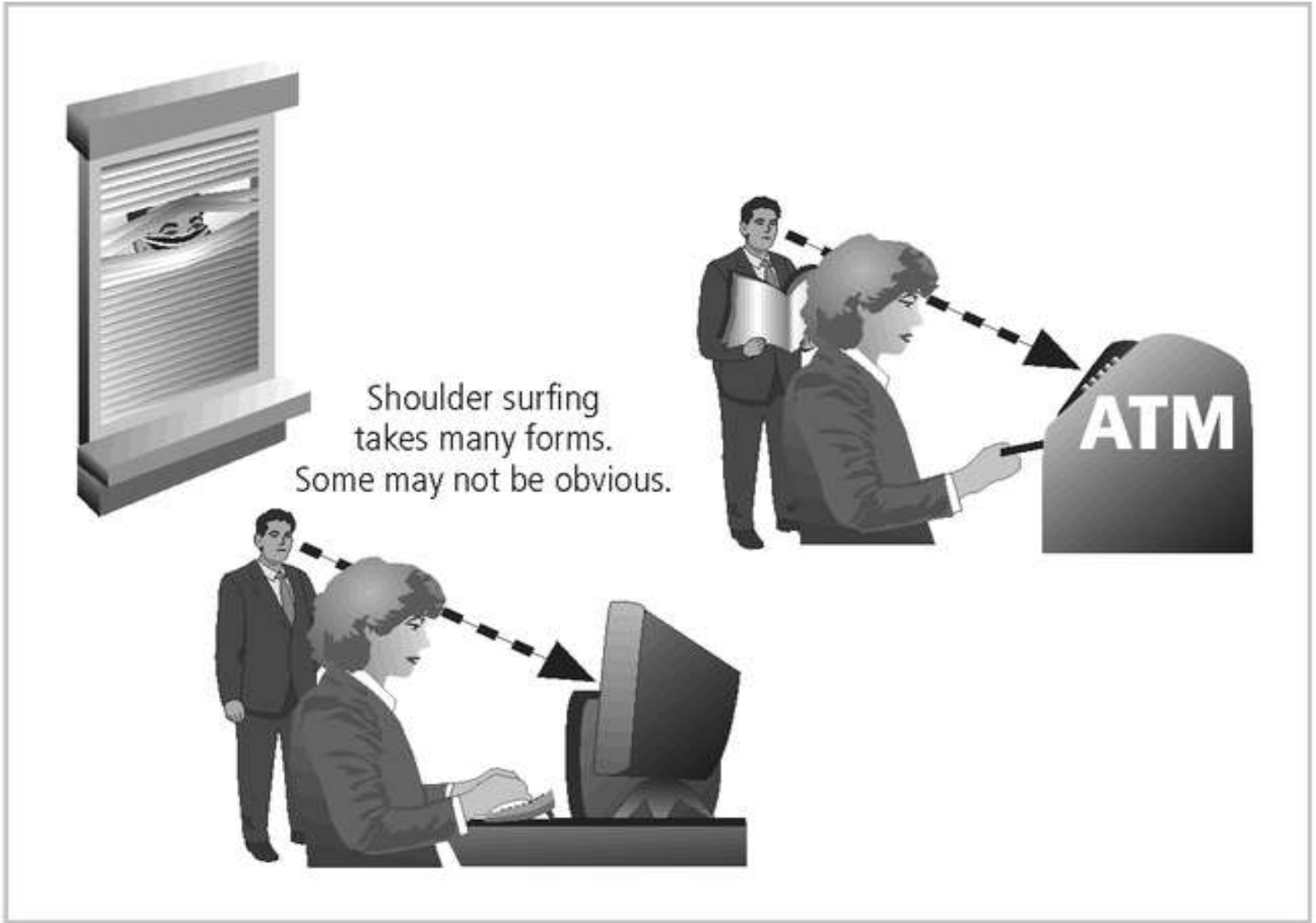


FIGURE 2-2 Shoulder Surfing



Traditional hacker profile:
Age 13-18, male with limited
parental supervision spends all his
free time at the computer



Modern hacker profile:
Age 12-60, male or female, unknown
background, with varying technological
skill levels; may be internal or external
to the organization

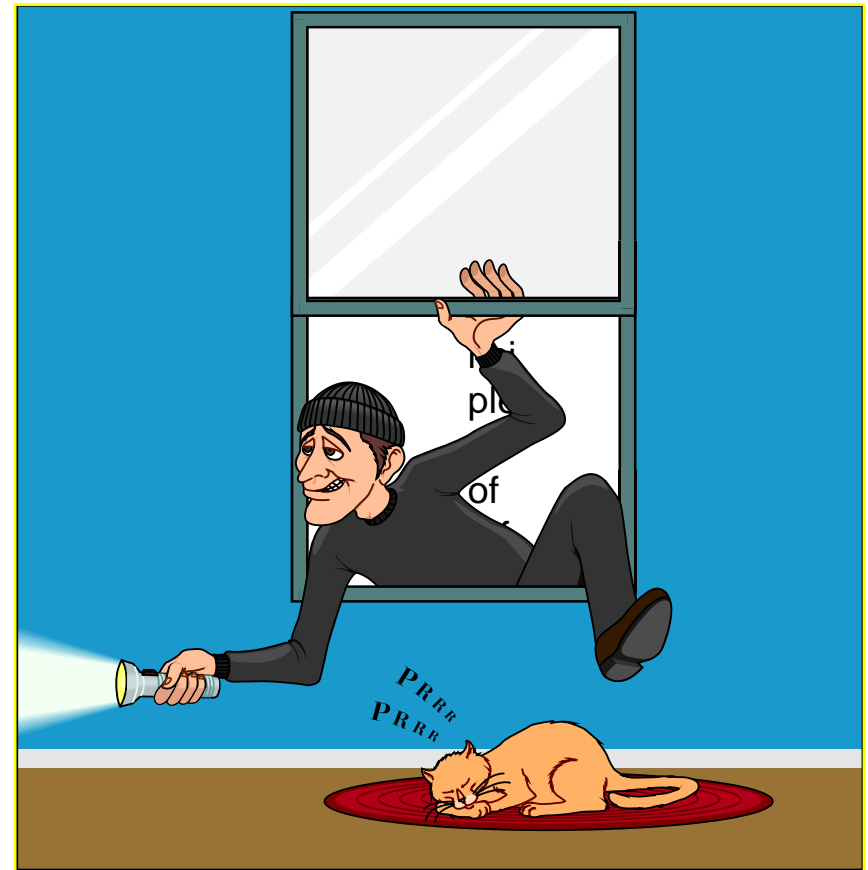
FIGURE 2-3 Hacker Profiles

Espionage/Trespass

- Generally two skill levels among hackers:
 - Expert hacker
 - develops software scripts and codes exploits
 - usually a master of many skills
 - will often create attack software and share with others
 - Script kiddies
 - hackers of limited skill
 - use expert-written software to exploit a system
 - do not usually fully understand the systems they hack
- Other terms for system rule breakers:
 - Cracker - an individual who “cracks” or removes protection designed to prevent unauthorized duplication
 - Phreaker - hacks the public telephone network

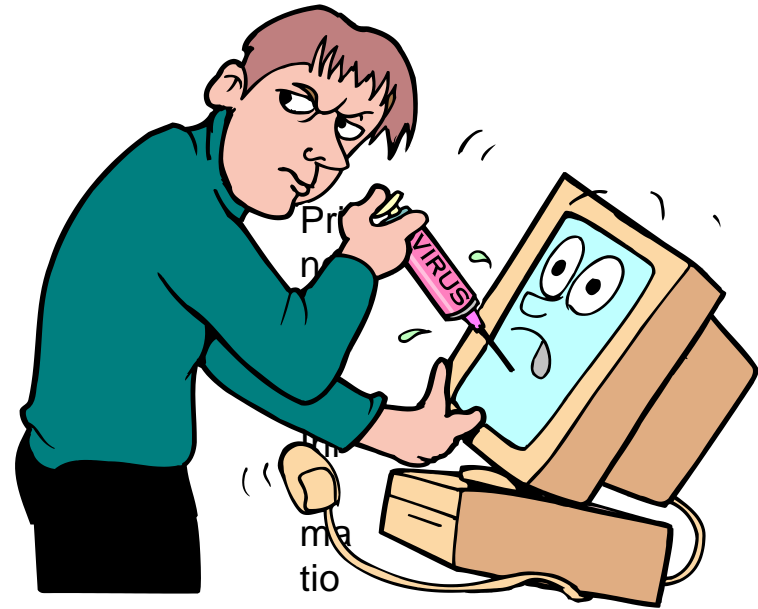
Information Extortion

- Information extortion is an attacker or formerly trusted insider stealing information from a computer system and demanding compensation for its return or non-use
- Extortion found in credit card number theft



Sabotage or Vandalism

- Individual or group 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 to organized sabotage
- Organizations rely on image so Web defacing can lead to dropping consumer confidence and sales
- Rising threat of hacktivist or cyber-activist operations – the most extreme version is cyber-terrorism



Pr
n
ma
tio
n
Se
cur
ity
-
Ch
apt
er
2

Deliberate Acts of Theft

- Illegal taking of another's property - 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 - a wide variety of measures used from locked doors to guards or alarm systems
- Electronic theft is a more complex problem to manage and control - organizations may not even know it has occurred

Deliberate Software Attacks

- When an individual or group designs software to attack systems, they create malicious code/software called malware
 - Designed to damage, destroy, or deny service to the target systems
- Includes:
 - macro virus
 - boot virus
 - worms
 - Trojan horses
 - logic bombs
 - back door or trap door
 - denial-of-service attacks
 - polymorphic
 - hoaxes



Bomb

cur
ity

-
Ch
apt
er
2

Deliberate Software Attacks

- Virus is a computer program that attaches itself to an executable file or application.
- It can replicate itself, usually through an executable program attached to an e-mail.
- The keyword is “attaches”. A virus can not stand on its own.
- You must prevent viruses from being installed on computers in your organizations.

Deliberate Software Attacks

- Learn about OS and application vulnerabilities.
- The Mitre Corporation's Common Vulnerabilities and Exposures. www.cve.mitre.org

Deliberate Software Attacks

- There is no foolproof method of preventing them from attaching themselves to your computer
- Antivirus software compares virus signature files against the programming code of known viruses.
- Regularly update virus signature files is crucial.

Deliberate Software Attacks

- A worm is a computer program that replicates and propagates itself without having to attach itself to a host.
- Most infamous worms are Code Red and Nimda.
- Cost businesses millions of dollars in damage as a result of lost productivity
- Computer downtime and the time spent recovering lost data, reinstalling programming's, operating systems, and hiring or contracting IT personnel.

Pr
ci
ple
of
Inf
or
ma
tio
n
se
cur
ity
-
Ch
apt
er
2

Deliberate Software Attacks

- Trojan Programs disguise themselves as useful computer programs or applications and can install a backdoor or rootkit on a computer.
- Backdoors or rootkits are computer programs that give attackers a means of regaining access to the attacked computer later.

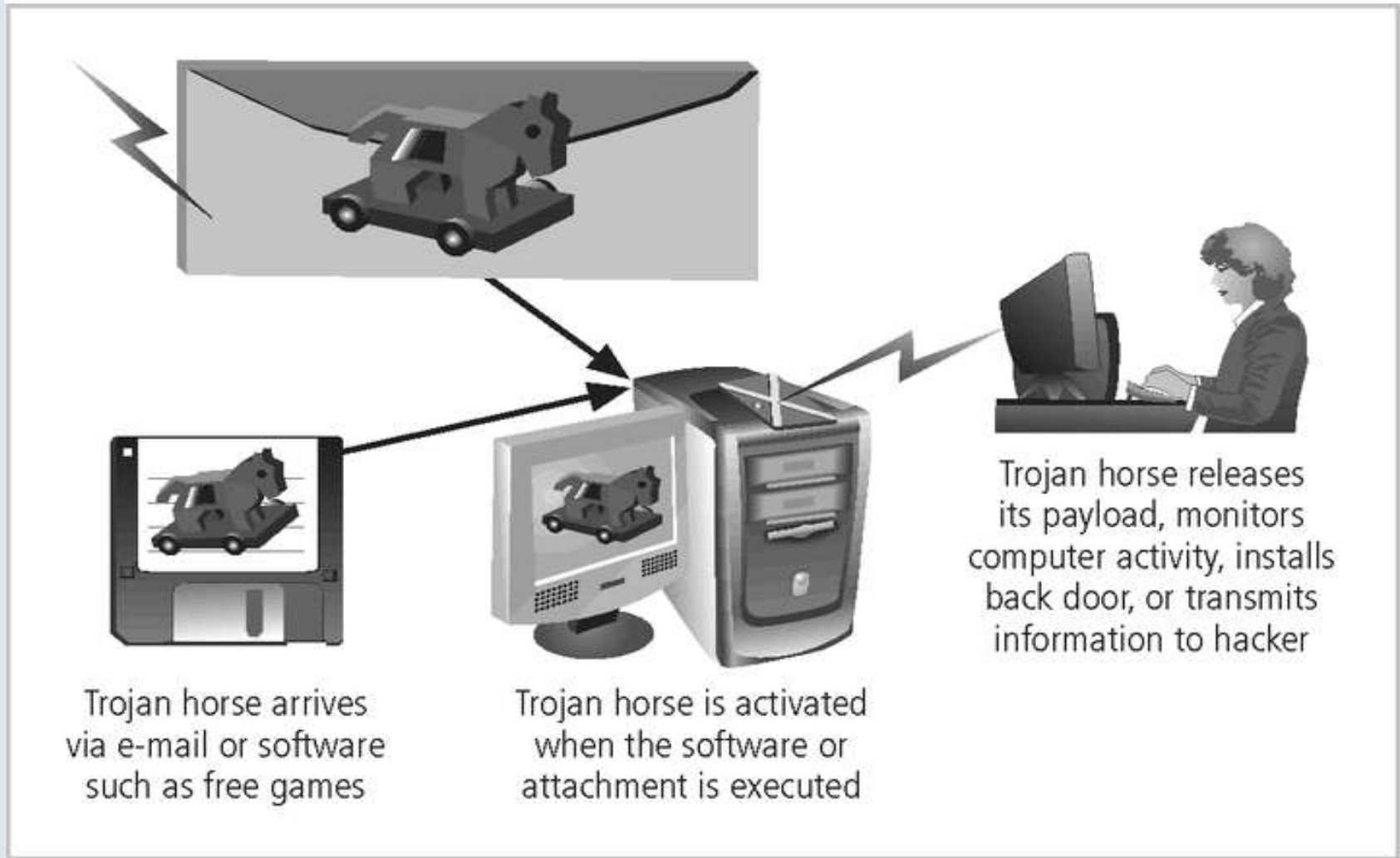


FIGURE 2-8 Trojan Horse Attack

Deliberate Software Attacks

■ Challenges:

- Trojan programs that use common ports, such as TCP 80, or UDP 53, are more difficult to detect.
- Many software firewalls can recognize port scanning program or information leaving a questionable port.
- However, they prompt user to allow or disallow, and users are not aware.
- Educate your network users.
- Many Trojan programs use standard ports to conduct their exploits.

Deliberate Software Attacks

■ Spyware

- A Spyware program sends info from the infected computer to the person who initiated the spyware program on your computer
- Spyware program can register each keystroke entered.
- www.spywareguide.com

■ Adware

- Main purpose is to determine a user's purchasing habits so that Web browsers can display advertisements tailored to that user.
- Slow down the computer it's running on.
- Adware sometimes displays a banner that notifies the user of its presence
- Both programs can be installed without the user being aware of their presence

Pri
nci
ple
s
of
Inf
er
ma
tio

n
Se
cur
ity
-
Ch
apt
er
2

Protecting against Deliberate Software Attacks

■ Educating Your Users

- Many U.S. government organizations make security awareness programs mandatory, and many private-sector companies are following their example.
- Email monthly security updates to all employees.
- Update virus signature files as soon as possible.
- Protect a network by implementing a firewall.

■ Avoiding Fear Tactics

- Your approach to users or potential customers should be promoting awareness rather than instilling fear.
- When training users, be sure to build on the knowledge they already have.

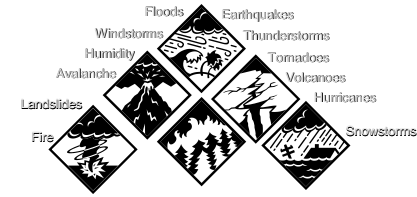
Compromises to Intellectual Property

- Intellectual property is “the ownership of ideas and control over the tangible or virtual representation of those ideas”
- Many organizations are in business to create intellectual property
 - trade secrets
 - copyrights
 - trademarks
 - patents

Compromises to Intellectual Property

- Most common IP breaches involve software piracy
- Watchdog organizations investigate:
 - Software & Information Industry Association (SIIA)
 - Business Software Alliance (BSA)
- Enforcement of copyright has been attempted with technical security mechanisms

Forces of Nature



- Forces of nature, *force majeure*, or acts of God are dangerous because they are unexpected and can occur with very little warning
- Can disrupt not only the lives of individuals, but also the storage, transmission, and use of information
- 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

Pr
ici
ple
s
of
Inf
or
ma
tio
n
Se
cur
ity
-
Ch
apt
er
2

Technical Hardware Failures or Errors

- Technical hardware failures or errors occur when a manufacturer distributes to users equipment containing flaws
- 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 Hardware Failures or Errors

- This category of threats comes from purchasing software with unrevealed 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 obsolescence, but when obsolescence is identified, management must take 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
 - A 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 using up to six attack vectors to exploit a variety of vulnerabilities in commonly found information system devices



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** – Compromised 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

Attack Descriptions

- **Unprotected Shares** - using file shares to copy viral component to all reachable locations
- **Mass Mail** - sending e-mail infections to addresses found in address book
- **Simple Network Management Protocol** - SNMP vulnerabilities used to compromise and infect
- **Hoaxes** - A more devious approach to attacking computer systems is the transmission of a virus hoax, with a real virus attached

Attack Descriptions

- **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 guide guesses

Attack Descriptions

- **Denial-of-service (DoS)** –

- 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
- 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

In a denial-of-service attack, a hacker compromises a system and uses that system to attack the target computer, flooding it with more requests for services than the target can handle.

In a distributed denial-of-service attack, dozens or even hundreds of computers (known as zombies) are compromised, loaded with DoS attack software and then remotely activated by the hacker to conduct a coordinated attack.

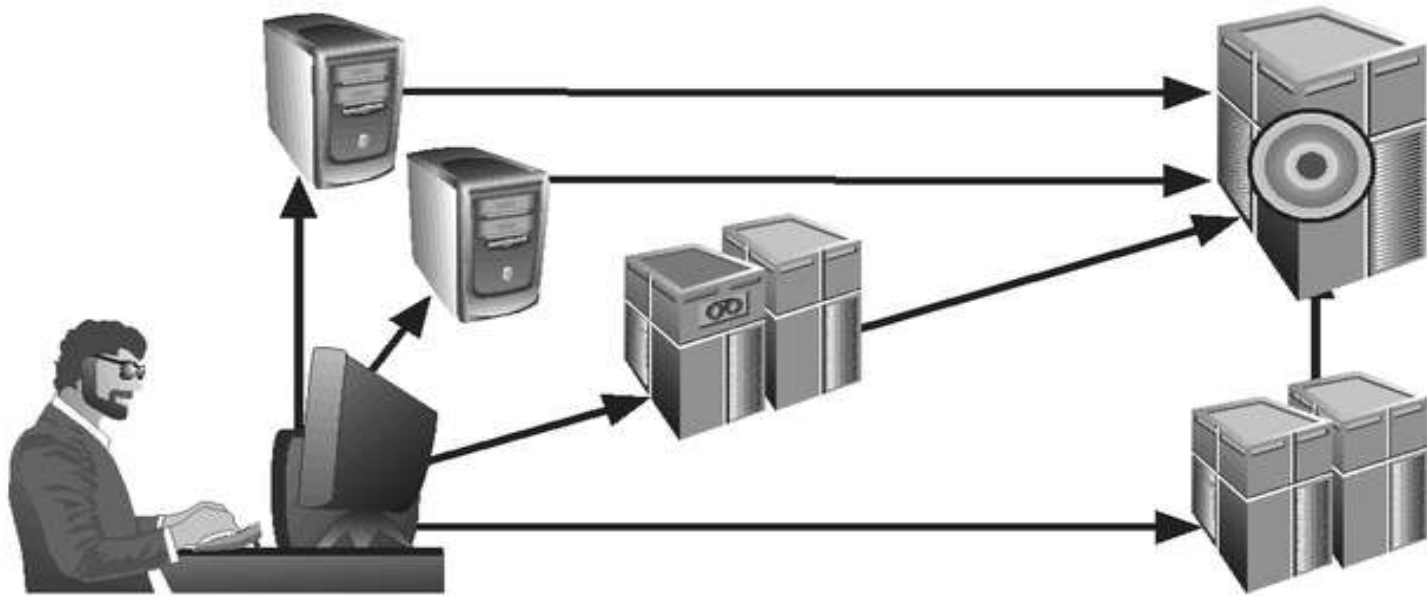


FIGURE 2-9 Denial-of-Service Attacks

Attack Descriptions

- **Spoofing** - technique used to gain unauthorized access 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** - 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

Principles of Security

Chapter 2

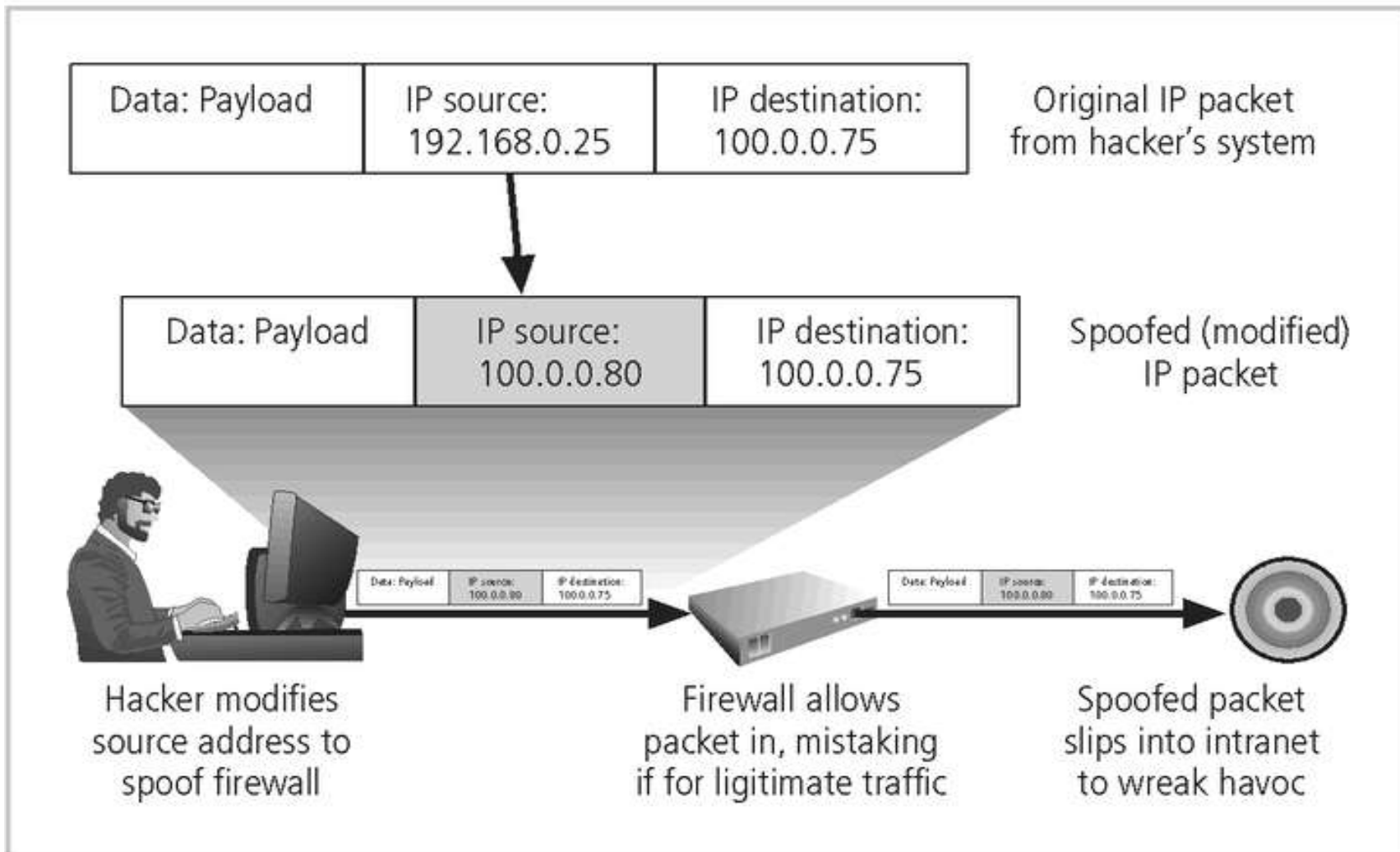


FIGURE 2-10 IP Spoofing

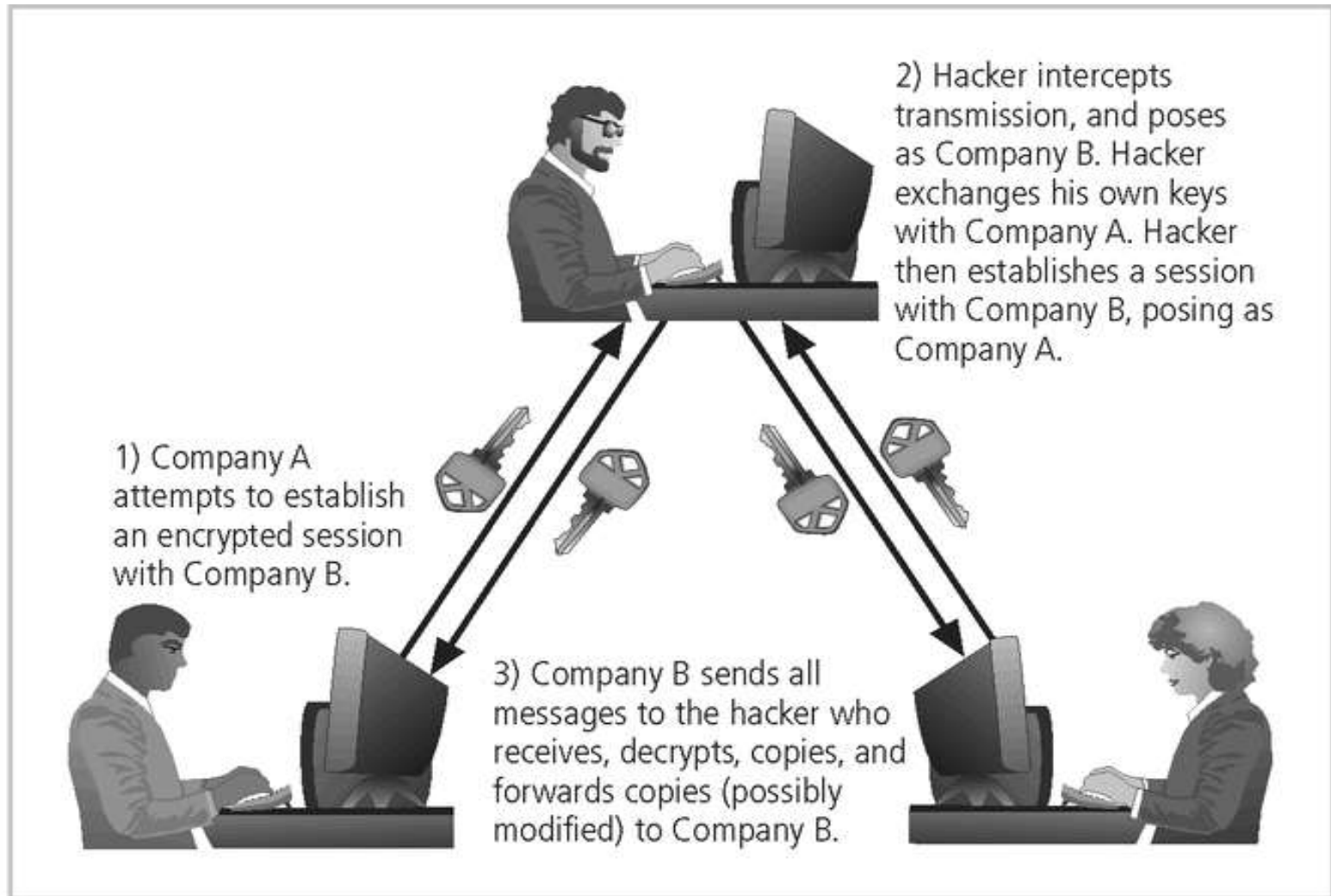


FIGURE 2-11 Man-in-the-Middle Attack

Attack Descriptions

- **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

Principles of Information Security - Chapter 2

Attack Descriptions

- “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

Attack Descriptions

- **Buffer Overflow** –
 - application error 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
 - Usually the attacker fill the overflow buffer with executable program code to elevate the attacker's permission to that of an administrator.

Attack Descriptions

- **Ping of Death Attacks --**
 - A type of DoS attack
 - Attacker creates an ICMP packet that is larger than the maximum allowed 65,535 bytes.
 - The large packet is fragmented into smaller packets and reassembled at its destination.
 - Destination user cannot handle the reassembled oversized packet, thereby causing the system to crash or freeze.

Attack Descriptions

- **Timing Attack –**
 - relatively new
 - works by exploring the contents of a web browser's cache
 - can allow collection of 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

Summary


- Unlike any other aspect of IT, information security's primary mission to ensure things stay the way they are
- Information security performs four important functions:
 - Protects organization's ability to function
 - Enables safe operation of applications implemented on organization's IT systems
 - Protects data the organization collects and uses
 - Safeguards the technology assets in use at the organization

Summary

- Threat: object, person, or other entity representing a constant danger to an asset
- Management effectively protects its information through policy, education, training, and technology controls
- Attack: a deliberate act that exploits vulnerability

Readings and Assignment

- Check out the following White House site for the document on “The National Strategy to Secure Cyberspace”
- http://www.whitehouse.gov/pcipb/priority_1.pdf
- As your hand-in exercise:
 - read this document
 - Using a minimum of about 3 pages (double spaced) write about how this document enhances national security.
- Due February 1, 2007.
 - Must have a cover page with a title, class, and name
 - Must have references.



Legal, Ethical, and Professional Issues in Information Security

3

Learning Objectives

Upon completion of this material, you should be able to:

- Use this chapter as a guide for future reference on laws, regulations, and professional organizations
- Differentiate between laws and ethics
- Identify major national laws that relate to the practice of information security
- Understand the role of culture as it applies to ethics in information security

Introduction

- You must understand scope of an organization's legal and ethical responsibilities
- To minimize liabilities/reduce risks, the information security practitioner must:
 - Understand current legal environment
 - Stay current with laws and regulations
 - Watch for new issues that emerge

Law and Ethics in Information Security

- Laws: rules that mandate or prohibit certain societal behavior
- Ethics: define socially acceptable behavior
- Cultural mores: fixed moral attitudes or customs of a particular group; ethics based on these
- Laws carry sanctions of a governing authority; ethics do not

Types of Law

- Civil
- Criminal
- Tort
- Private
- Public

Relevant U.S. Laws (General)

- Computer Fraud and Abuse Act of 1986 (CFA Act)
- National Information Infrastructure Protection Act of 1996
- USA Patriot Act of 2001
- Telecommunications Deregulation and Competition Act of 1996
- Communications Decency Act of 1996 (CDA)

Privacy

- One of the hottest topics in information security
- Is a “state of being free from unsanctioned intrusion”
- Ability to aggregate data from multiple sources allows creation of information databases previously unheard of

Privacy of Customer Information

- Privacy of Customer Information Section of common carrier regulation
- Federal Privacy Act of 1974
- Electronic Communications Privacy Act of 1986
- Health Insurance Portability and Accountability Act of 1996 (HIPAA), aka Kennedy-Kassebaum Act
- Financial Services Modernization Act, or Gramm-Leach-Bliley Act of 1999

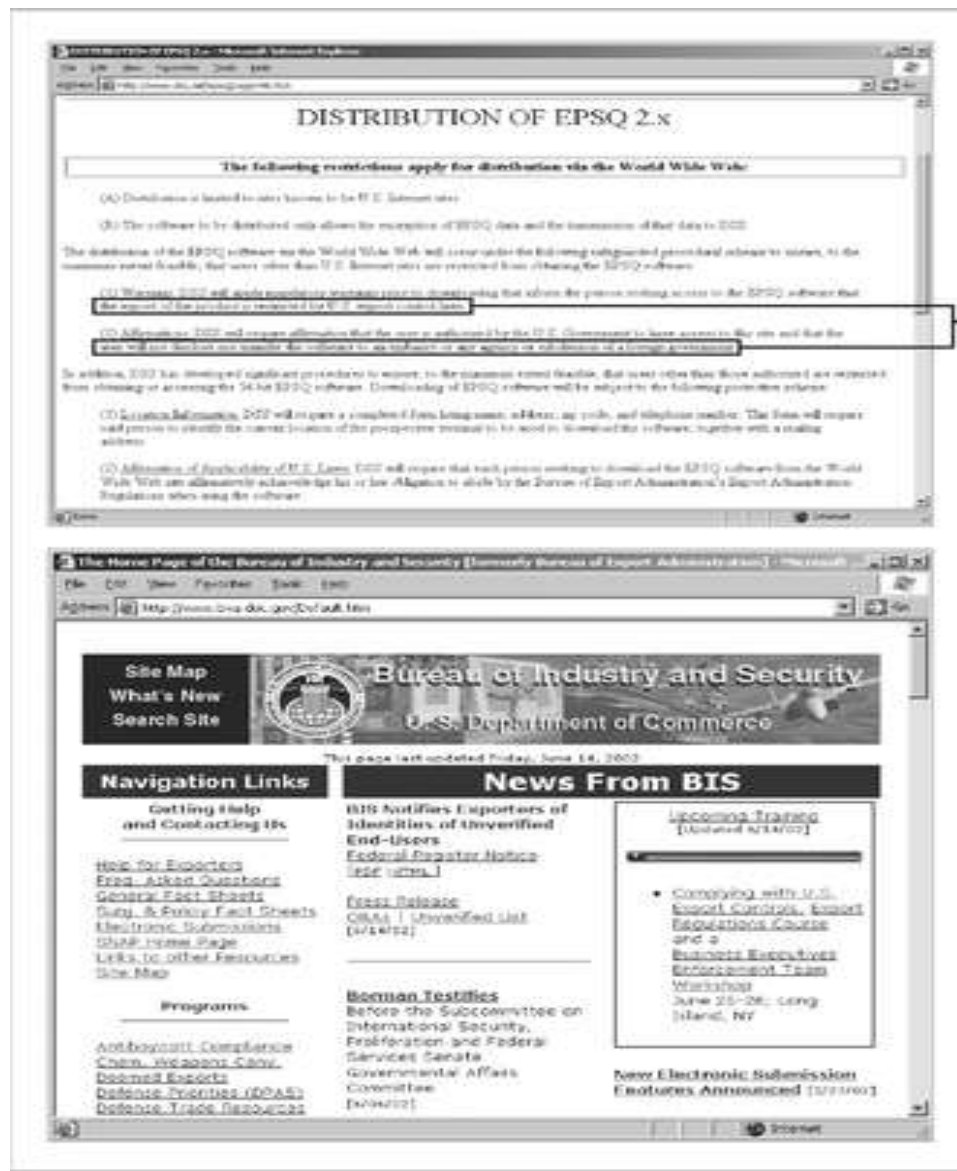


FIGURE 3-2 Export and Espionage



FIGURE 3-2 The U.S. Copyright Office Web Site

Export and Espionage Laws

- Economic Espionage Act of 1996 (EEA)
- Security And Freedom Through Encryption Act of 1999 (SAFE)

U.S. Copyright Law

- Intellectual property recognized as protected asset in the U.S.; copyright law extends to electronic formats
- With proper acknowledgement, permissible to include portions of others' work as reference
- U.S. Copyright Office Web site: www.copyright.gov

Freedom of Information Act of 1966 (FOIA)

- Allows access to federal agency records or information not determined to be matter of national security
- U.S. government agencies required to disclose any requested information upon receipt of written request
- Some information protected from disclosure

State and Local Regulations

- Restrictions on organizational computer technology use exist at international, national, state, local levels
- Information security professional responsible for understanding state regulations and ensuring organization is compliant with regulations

International Laws and Legal Bodies

- European Council Cyber-Crime Convention:
 - Establishes international task force overseeing Internet security functions for standardized international technology laws
 - Attempts to improve effectiveness of international investigations into breaches of technology law
 - Well received by intellectual property rights advocates due to emphasis on copyright infringement prosecution

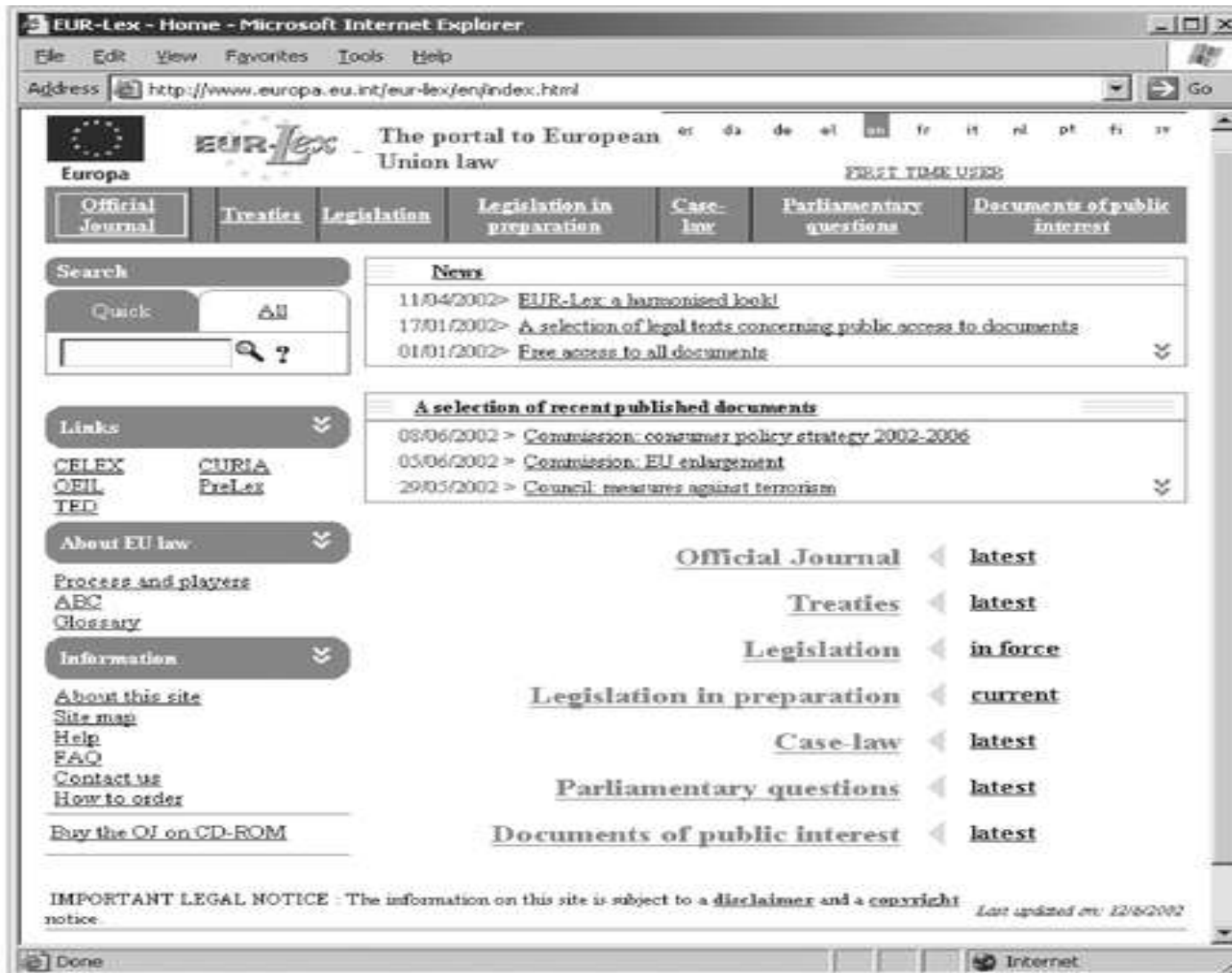


FIGURE 3-5 EU Law Portal

Digital Millennium Copyright Act (DMCA)

- U.S. contribution to international effort to reduce impact of copyright, trademark, and privacy infringement
- A response to European Union Directive 95/46/EC, which adds protection to individuals with regard to processing and free movement of personal data

United Nations Charter

- Makes provisions, to a degree, for information security during information warfare (IW)
- IW involves use of information technology to conduct organized and lawful military operations
- IW is relatively new type of warfare, although military has been conducting electronic warfare operations for decades



FIGURE 3-6 UN International Law Web site

Policy Versus Law

- Most organizations develop and formalize a body of expectations called policy
- Policies serve as organizational laws
- To be enforceable, policy must be distributed, readily available, easily understood, and acknowledged by employees

Ethics and Information Security

The Ten Commandments of Computer Ethics⁶

From The Computer Ethics Institute

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

Ethical Differences Across Cultures

- Cultural differences create difficulty in determining what is and is not ethical
- Difficulties arise when one nationality's ethical behavior conflicts with ethics of another national group
- Example: many of ways in which Asian cultures use computer technology is software piracy

Ethics and Education

- Overriding factor in leveling ethical perceptions within a small population is education
- Employees must be trained in expected behaviors of an ethical employee, especially in areas of information security
- Proper ethical training vital to creating informed, well prepared, and low-risk system user

Deterrence to Unethical and Illegal Behavior

- Deterrence: best method for preventing an illegal or unethical activity; e.g., laws, policies, technical controls
- Laws and policies only deter if three conditions are present:
 - Fear of penalty
 - Probability of being caught
 - Probability of penalty being administered

Codes of Ethics and Professional Organizations

- Several professional organizations have established codes of conduct/ethics
- Codes of ethics can have positive effect; unfortunately, many employers do not encourage joining of these professional organizations
- Responsibility of security professionals to act ethically and according to policies of employer, professional organization, and laws of society

Association of Computing Machinery (ACM)

- ACM established in 1947 as “the world's first educational and scientific computing society”
- Code of ethics contains references to protecting information confidentiality, causing no harm, protecting others’ privacy, and respecting others’ intellectual property

International Information Systems Security Certification Consortium, Inc. (ISC)²

- Non-profit organization focusing on development and implementation of information security certifications and credentials
- Code primarily designed for information security professionals who have certification from (ISC)²
- Code of ethics focuses on four mandatory canons

System Administration, Networking, and Security Institute (SANS)

- Professional organization with a large membership dedicated to protection of information and systems
- SANS offers set of certifications called Global Information Assurance Certification (GIAC)

Information Systems Audit and Control Association (ISACA)

- Professional association with focus on auditing, control, and security
- Concentrates on providing IT control practices and standards
- ISACA has code of ethics for its professionals

Computer Security Institute (CSI)

- Provides information and training to support computer, networking, and information security professionals
- Though without a code of ethics, has argued for adoption of ethical behavior among information security professionals

Information Systems Security Association (ISSA)

- Nonprofit society of information security (IS) professionals
- Primary mission to bring together qualified IS practitioners for information exchange and educational development
- Promotes code of ethics similar to (ISC)², ISACA and ACM

Other Security Organizations

- Internet Society (ISOC): promotes development and implementation of education, standards, policy and education to promote the Internet
- Computer Security Division (CSD): division of National Institute for Standards and Technology (NIST); promotes industry best practices and is important reference for information security professionals

Other Security Organizations (continued)

- CERT Coordination Center (CERT/CC): center of Internet security expertise operated by Carnegie Mellon University
- Computer Professionals for Social Responsibility (CPSR): public organization for anyone concerned with impact of computer technology on society

Key U.S. Federal Agencies

- Department of Homeland Security (DHS)
- Federal Bureau of Investigation's National Infrastructure Protection Center (NIPC)
- National Security Agency (NSA)
- U.S. Secret Service

Organizational Liability and the Need for Counsel

- Liability is legal obligation of an entity; includes legal obligation to make restitution for wrongs committed
- Organization increases liability if it refuses to take measures known as due care
- Due diligence requires that an organization make valid effort to protect others and continually maintain that level of effort

Summary

- Laws: rules that mandate or prohibit certain behavior in society; drawn from ethics
- Ethics: define socially acceptable behaviors; based on cultural mores (fixed moral attitudes or customs of a particular group)
- Types of law: civil, criminal, tort law, private, public

Summary

- Relevant U.S. laws:
 - Computer Fraud and Abuse Act of 1986 (CFA Act)
 - National Information Infrastructure Protection Act of 1996
 - USA Patriot Act of 2001
 - Telecommunications Deregulation and Competition Act of 1996
 - Communications Decency Act of 1996 (CDA)
 - Computer Security Act of 1987

Homework

- Relevant U.S. laws:
 - Computer Fraud and Abuse Act of 1986 (CFA Act)
 - National Information Infrastructure Protection Act of 1996
 - USA Patriot Act of 2001
 - Telecommunications Deregulation and Competition Act of 1996
 - Communications Decency Act of 1996 (CDA)
 - Computer Security Act of 1987
- These are relevant U.S. Laws on Information Security. Pick one law and prepare a 10 minutes presentation on it. One week.

Summary

- Many organizations have codes of conduct and/or codes of ethics
- Organization increases liability if it refuses to take measures known as due care
- Due diligence requires that organization make valid effort to protect others and continually maintain that effort

PRINCIPLES OF INFORMATION SECURITY

Second Edition

Chapter 4 Risk Management

Once we know our weaknesses, they cease to do us any harm

G.C. (GEORG CHRISTOPH) LICHTENBERG (1742-1799)

GERMAN PHYSICIST, PHILOSOPHER

Learning Objectives

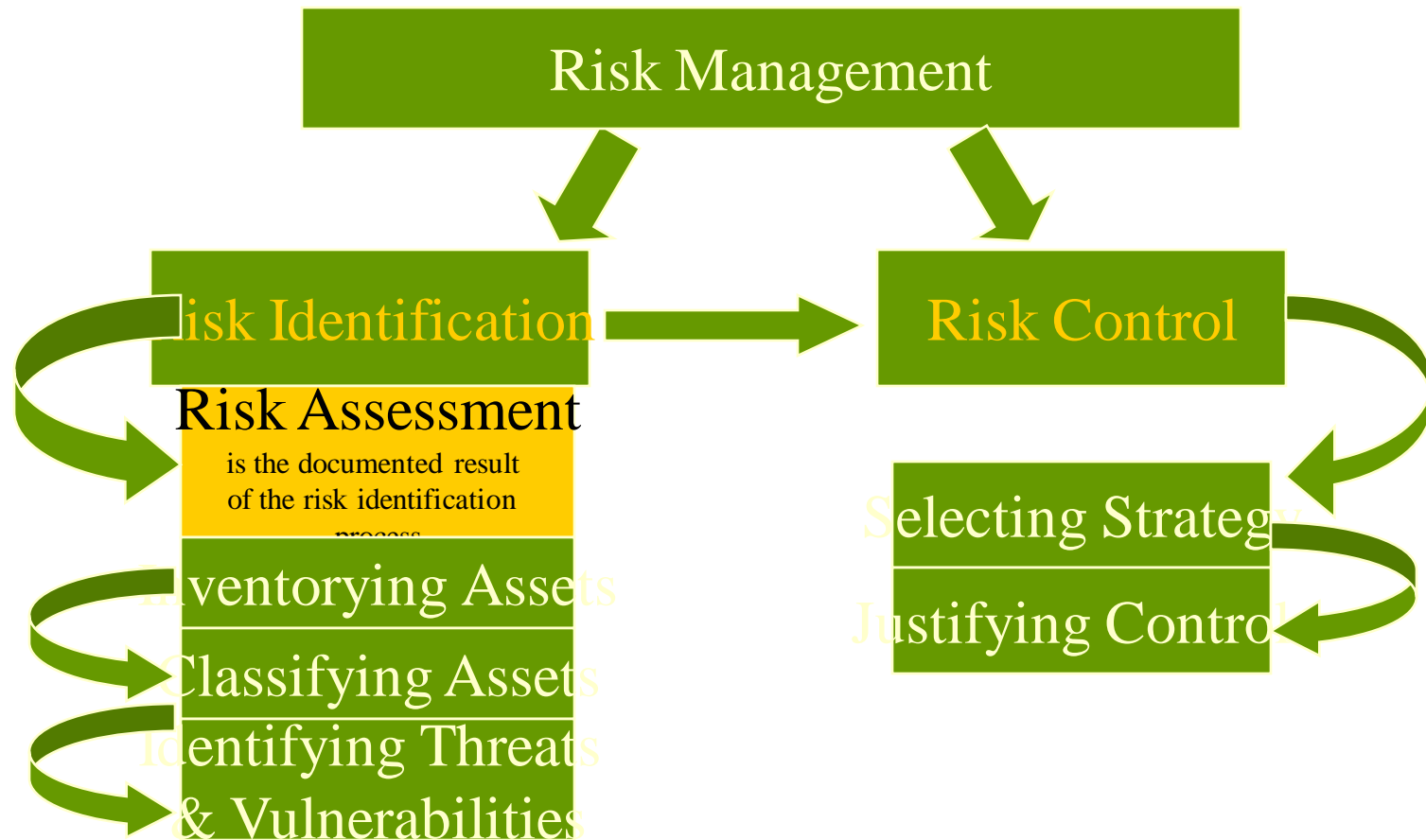
Upon completion of this material, you should be able to:

- Define risk management: risk identification, and risk control
- Understand how risk is identified and assessed
- Describe the risk mitigation strategy options for controlling risks
- Evaluate risk controls and formulate a cost benefit analysis
- Understand how to maintain and perpetuate risk controls

Introduction

- **Risk management**: process of identifying and controlling risks facing an organization
- **Risk identification**: process of examining an organization's current information technology security situation
- **Risk control**: applying controls to reduce risks to an organizations data and information systems

Components of Risk Management



Competitiveness

- Information Technology Role
 - Began as a advantage
 - Now falling behind is a disadvantage
- Availability is a necessity

An Overview of Risk Management

- Know yourself
 - Understand the technology and systems in your organization
- Know the enemy
 - Identify, examine, understand threats
- Role of Communities of Interest
 - Information Security
 - Management and Users
 - Information Technology

The Roles of the Communities of Interest

- 1) *Information security*, 2) *management and users*, 3) *information technology* all must work together
- Management review:
 - Verify completeness/accuracy of asset inventory
 - Review and verify threats as well as controls and mitigation strategies
 - Review cost effectiveness of each control
 - Verify effectiveness of controls deployed

Risk Identification

- *Assets* are targets of various threats and threat agents
- Risk management involves identifying *organization's assets* and identifying *threats/vulnerabilities*
- Risk identification begins with identifying organization's assets and assessing their value

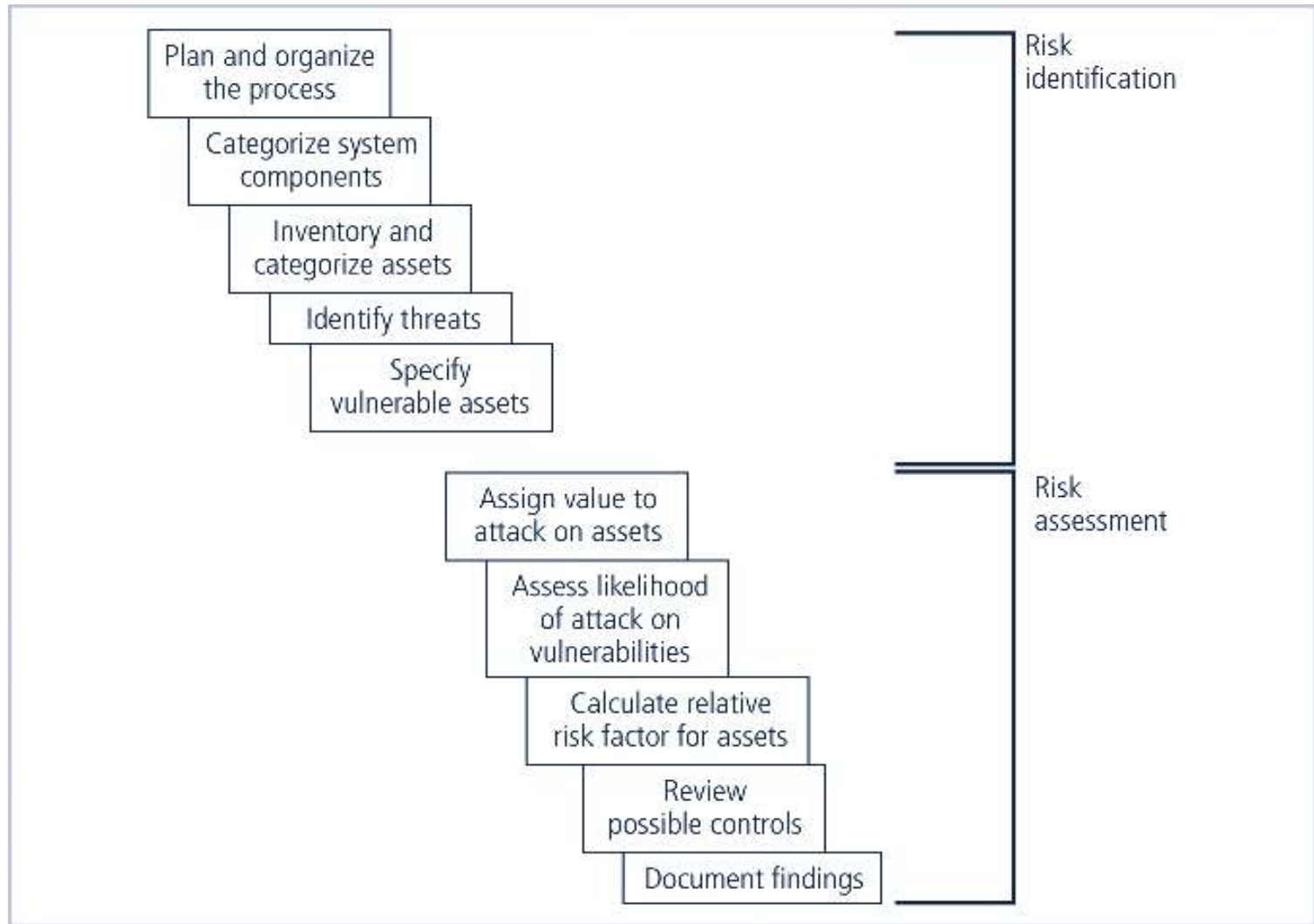


FIGURE 4-2 Components of Risk Identification

Asset Identification and Valuation

- Iterative process; begins with identification of assets, including all elements of an organization's system (people, procedures, data and information, software, hardware, networking)
- Assets are then classified and categorized

Asset Identification & Valuation

Traditional System Components	SecSDLC and risk management system components	
People	Employee	Trusted employees Other staff
	Non-employees	People at trusted organizations / Strangers
Procedures	Procedures	IT & business standards procedures IT & business standards procedures
Data	Information	Transmission, Processing, Storage
Software	Software	Applications, Operating systems, Security components
Hardware	System devices and peripherals	Systems and peripherals Security devices
	Networking components	Intranet components Internet or DMZ components

People, Procedures, and Data Asset Identification

- Human resources, documentation, and data information assets are more difficult to identify
- People with knowledge, experience, and good judgment should be assigned this task
- These assets should be recorded using reliable data-handling process

People, Procedures, and Data Asset Identification

- Asset attributes for *people*: position name/number/ID; supervisor; security clearance level; special skills
 - Try to avoid names
- Asset attributes for *procedures*
 - Intended purpose
 - Relationship to software, hardware, network elements
 - Storage location
- Asset attributes for data
 - classification; owner/creator/manager; data structure size; data structure used; online/offline; location; backup procedures employed

Hardware, Software, and Network Asset Identification

- What information attributes to track depends on:
 - Needs of organization/risk management efforts
 - Management needs of information security/information technology communities
- Asset attributes to be considered are:
 - Name (device or program name)
 - IP address
 - Media access control (MAC) address
 - Element type – server, desktop, etc. Device Class, Device OS, Device Capacity

Hardware, Software, and Network Asset Identification

- serial number
- manufacturer name; model/part number
- software versions
- physical or logical location
- Software version, update revision
- Physical location
- Logical location
 - Where on network
- Controlling entity
 - Organization unit to which it belongs

Information Asset Classification

- Many organizations have data classification schemes (e.g., confidential, internal, public data)
- Classification must be specific enough to allow determination of priority
- Comprehensive – all info fits in list somewhere
- Mutually exclusive – fits in one place

Information Asset Valuation

- Questions help develop criteria for asset valuation: which information asset
 - is most critical to organization's success?
 - generates the most revenue?
 - generates the most profit?
 - would be most expensive to replace?

Information Asset Valuation

- Questions help develop criteria for asset valuation:
which information asset
 - would be most expensive to protect?
 - would be most embarrassing or cause the greatest liability is revealed?

System Name: SLS E-Commerce

Date Evaluated: February 2003

Evaluated By: D. Jones

Information assets	Data classification	Impact to profitability
Information Transmitted:		
EDI Document Set 1 —Logistics BOL to outsourcer (outbound)	Confidential	High
EDI Document Set 2—Supplier orders (Outbound)	Confidential	High
EDI Document Set 2—Supplier fulfillment advice (inbound)	Confidential	Medium
Customer order via SSL (inbound)	Confidential	Critical
Customer service Request via e-mail (inbound)	Private	Medium
DMZ Assets:		
Edge Router	Public	Critical
Web server #1—home page and core site	Public	Critical
Web server #2—Application server	Private	Critical

Notes: BOL: Bill of Lading:

DMZ: Demilitarized Zone

EDI: Electronic Data Interchange

SSL: Secure Sockets Layer

Example Worksheet for the Asset Identification of Information Systems

Listing Assets in Order of Importance

- Weighted factor analysis
 - Calculate the relative importance of each asset
- Each info asset assigned score for each critical factor (0.1 to 1.0)
 - Impact to revenue
 - Impact to profitability
 - Impact to public image
- Each critical factor is assigned a weight (1-100)
- Multiply and add

TABLE 4-2 Example of a Weighted Factor Analysis Worksheet

Information asset	Criteria 1: impact to revenue	Criteria 2: impact to profitability	Criteria 3: public image impact	Weighted score
<i>Criterion Weight (1-100)</i> <i>Must total 100</i>	30	40	30	
EDI Document Set 1— Logistics BOL to outsourcer (outbound)	0.8	0.9	0.5	75
EDI Document Set 2— Supplier orders (outbound)	0.8	0.9	0.6	78
EDI Document Set 2— Supplier fulfillment advice (inbound)	0.4	0.5	0.3	41
Customer order via SSL (inbound)	1.0	1.0	1.0	100
Customer service request via e-mail (inbound)	0.4	0.4	0.9	55

Notes: EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

Data Classification and Management

- Variety of classification schemes used by corporate and military organizations
- Georgia-Pacific Corporation (G-P) scheme
 - Confidential, sensitive or proprietary
 - Internal, G-P employee, authorized contractors
 - External, public
- U.S. military classification scheme
 - Unclassified Data
 - Sensitive by unclassified data
 - Confidential data
 - Secret data
 - Top secret data

Data Classification and Management

- Information owners responsible for classifying their information assets
- Information classifications must be reviewed periodically
- Most organizations do not need detailed level of classification used by military or federal agencies.

Data Classification and Management

- Organizations may need to classify data to provide protection
 - Public
 - For official use only
 - Sensitive
 - classified

Data Classification and Management

- Assign classification to all data
- Grant access to data based on classification and need
- Devise some method of managing data relative to classification

Security Clearances

- Security clearance structure: each data user assigned a single level of authorization indicating classification level
- Before accessing specific set of data, employee must meet *need-to-know* requirement
- Extra level of protection ensures information confidentiality is maintained

Management of Classified Data

- Storage, distribution, portability, and destruction of classified data
- Information not unclassified or public must be clearly marked as such
- Clean desk policy requires all information be stored in appropriate storage container daily; unneeded copies of classified information are destroyed
- Dumpster diving can compromise information security

Threat and Prioritize Threats & Threat Agents

Threat	Example
Acts of human error or failure	Accidents, employee mistakes
Compromises to intellectual property	Piracy, copyright infringement
Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
Deliberate acts of information extortion	Blackmail or information disclosure
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate acts of sabotage or vandalism	Destruction of systems or information

Threat and Prioritize Threats & Threat Agents

Categories of Threat	Examples
Deliberate acts of software attacks	Viruses, worms, macros, denial-of-service
Forces of nature	Fire, flood, earthquake, lightning
Deviations in quality of service	ISP, power, WAN service issues from service providers
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

Threat Assessment

- Realistic threats need investigation; unimportant threats are set aside
 - Each of the threats must be examined to assess potential damage
 - Which threats present a danger to an organization's assets?
 - Which threats represent the most danger -probability of attack
 - How much would it cost to recover
 - Which threat requires the greatest expenditure to prevent?

Vulnerability Identification

- Identify each asset and each threat it faces
- Create a list of vulnerabilities
- Examine how each of the threats are likely to be perpetrated

Risk Assessment

- Risk assessment evaluates the relative risk for each vulnerability
- Assigns a risk rating or score to each information asset

Risk Assessment

$$\begin{aligned} \text{Risk} = & \\ & \text{likelihood of occurrence of vulnerability} \\ & * \\ & \text{value of the information asset} \\ & - \\ & \% \text{ of risk mitigated by current controls} \\ & + \\ & \text{uncertainty of current knowledge of vulnerability.} \end{aligned}$$

Likelihood

- Probability that a specific vulnerability within an organization will be successfully attacked
- Assign number between 0.1 – 1
- Data is available for some factors
 - Likelihood of fire
 - Likelihood of receiving infected email
 - Number of network attacks

Valuation of Information Assets

- Using info from asset identification assign weighted score for the value
 - 1 -100
 - 100 – stop company operations
 - May use broad categories
 - NIST has some predefined

Identify Possible Controls

- For each threat and associated vulnerabilities that have residual risk, create preliminary list of control ideas

- Residual risk – risk remaining after controls are applied

Access Controls

- Mandatory
 - Gives user and data owners limited control over access to information
 - Lattice-based
 - Users are assigned a matrix of authorizations for particular areas of access
- Nondiscretionary
 - Role or task based controls
 - Centralized
- Discretionary

Problem

- Information asset A has a value score of 50 and has one vulnerability. Vulnerability 1 has a likelihood of 1.0 with no current controls, & you estimate the assumptions and data are 90% accurate
- Information asset B has a value score of 100 and has 2 vulnerability. Vulnerability 2 has a likelihood of 0.5 with current controls address 50% of its risk, vulnerability 3 has a likelihood of 0.1 with no current controls, & you estimate the assumptions and data are 80% accurate

Solutions

likelihood of occurrence of vulnerability * value of the information asset - % of risk mitigated by current controls + uncertainty of current knowledge of vulnerability

- Asset A = $(50 \times 1.0) - (50 \times 1.0) \times 0\% + (50 \times 1.0) \times 10\%$

$$= (50 \times 1.0) - ((50 \times 1.0) \times 0) + ((50 \times 1.0) \times .1)$$

$$= 50 - 0 + 5$$

$$= 55$$

- Asset B (V2) = $(100 \times .5) - (100 \times .5) \times 50\% + (100 \times .5) \times 20\%$

$$= 50 - 25 + 10 = 35$$

- Asset B (V3) = $(100 \times .1) - 0\% + (100 \times .1) \times 20\%$

$$= 10 - 0 + 2$$

$$= 12$$

Documenting Results of Risk Assessment

- Final summary comprised in **ranked vulnerability risk worksheet**. Table 4-8, relate to table 4-2.
- Worksheet details *asset, asset impact, vulnerability, vulnerability likelihood, and risk-rating factor*.
- Order by risk-rating factor
- Ranked vulnerability risk worksheet is initial working document for next step in risk management process: assessing and controlling risk

Risk Identification and Assessment Deliverables

Deliverables	Purpose
Information assess classification worksheet	Assembles information about information assets and their impact on or value to the organization
Weighted criteria analysis worksheet	Assigns ranked value or impact weight to each information asset
Ranked vulnerability risk worksheet	Assigns ranked value of risk rating for each uncontrolled asset-vulnerability pair



Risk Control Strategies

Risk Control Strategies

- Once ranked vulnerability risk worksheet complete, must choose one of four strategies to control each risk:
 - Apply safeguards that eliminate or reduce residual risks (avoidance)
 - Transfer the risk to other areas or outside entities (transference)
 - Reduce the impact should the vulnerability be exploited (mitigation)
 - Understand the consequences and accept the risk without control or mitigation (acceptance)

Avoidance

- Attempts to prevent exploitation of the vulnerability
- Preferred approach; accomplished through countering threats, removing asset vulnerabilities, limiting asset access, and adding protective safeguards
- Three common methods of risk avoidance:
 - Application of policy
 - Training and education
 - Applying technology

Transference

- Control approach that attempts to shift risk to other assets, processes, or organizations
 - Rethinking how services are offered
 - Revising deployment models
 - Outsourcing
 - Purchasing insurance
 - Implementing service contracts
- In Search of Excellence
 - Concentrate on what you do best

Mitigation

- Attempts to reduce impact of vulnerability exploitation through planning and preparation
- Approach includes three types of plans:
 - Incident response plan (IRP)
 - Disaster recovery plan (DRP)
 - Business continuity plan (BCP)

Mitigation (continued)

- Disaster recovery plan (DRP) is most common mitigation procedure
- The actions to take while incident is in progress is defined in Incident response plan (IRP)
- Business continuity plan (BCP) encompasses continuation of business activities if catastrophic event occurs

Acceptance

- *Doing nothing* to protect a vulnerability and accepting the outcome of its exploitation
- Valid only when the particular function, service, information, or asset does not justify cost of protection
- *Risk appetite* describes the degree to which organization is willing to accept risk as trade-off to the expense of applying controls

Selecting a Risk Control Strategy

- Level of threat and value of asset play major role in selection of strategy
 - When a vulnerability exists--implement security control to reduce likelihood
 - When a vulnerability can be exploited -- apply layered protections, architectural designs, and administrative controls
 - When attacker's cost is less than potential gain -
- apply protection to increase attackers costs
 - When potential loss is substantial -- redesign, new architecture, controls

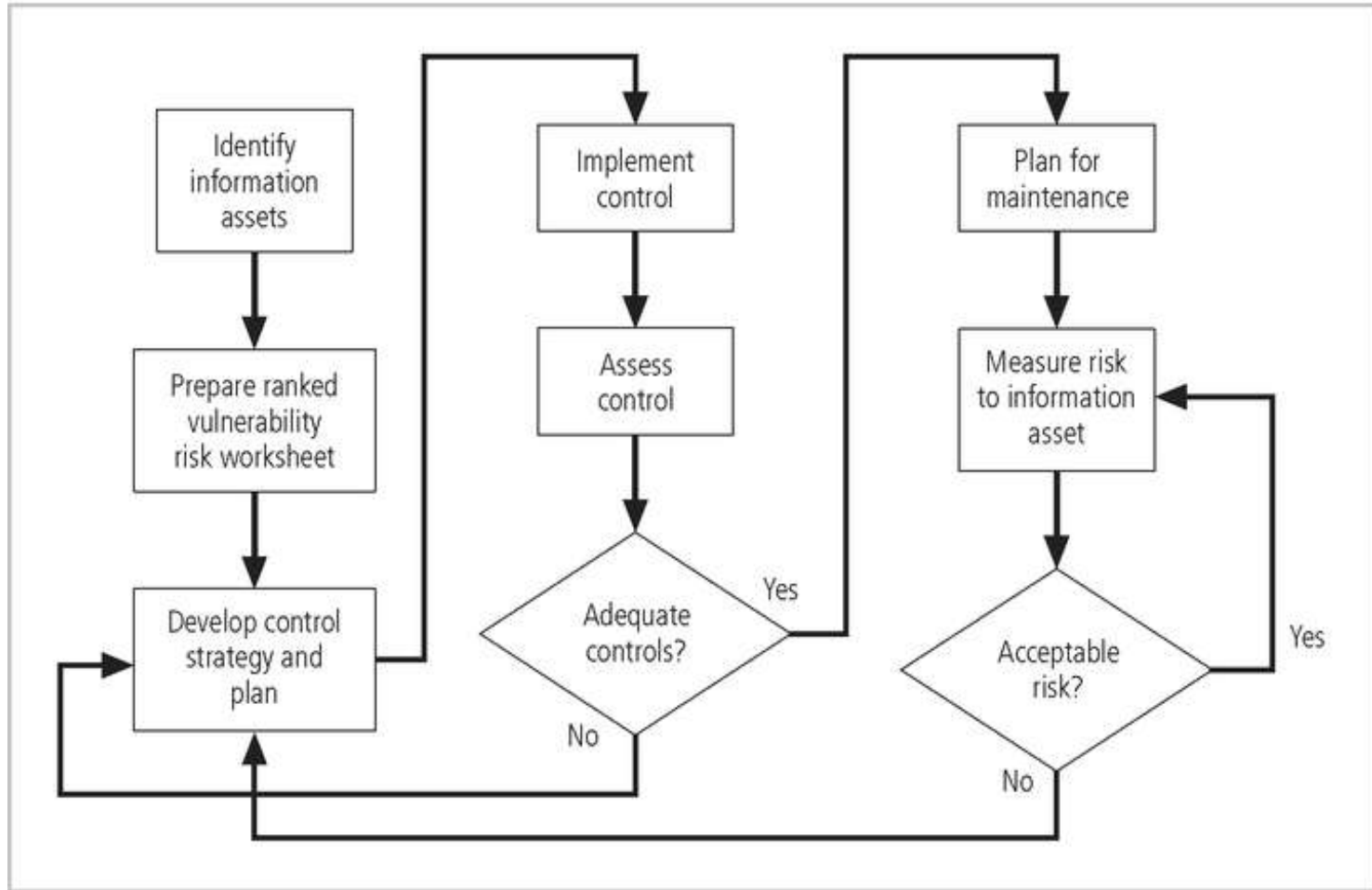


FIGURE 5-3 Risk Control Cycle⁸

Categories of Controls

1. Control function
 - Preventive & detective
2. Architectural layer
 - Organizational policy, external networks, intranets, network devices, systems
3. Strategy layer
 - Avoidance, mitigation, or transference
4. Information security principle
 - Classified by characteristics: Confidentiality, integrity, availability, authentication, authorization, accountability, privacy

Feasibility Studies

- Compare cost to potential loss
- Cost avoidance is the process of avoiding the financial impact of an incident

Cost Benefit Analysis

- Evaluate worth of asset
- Loss of value if asset compromised
- Items affecting **cost of control**
 - Cost of development or acquisition
 - Cost of implementation
 - Services costs
 - Cost of maintenance
- **Benefits** – value gained by using controls

Cost Benefit Analysis

- Assess worth of asset
- Calculate the single loss expectance
 - $SLE = \text{asset value} * \text{exposure factor}$
 - Exposure factor = % loss from exploitation
- Calculate Annualized loss expectancy
 - $ALE = SLE * ARO$ (annualized rate of occurrence)

Cost Benefit Analysis Formula

- CBA determines whether or not control alternative being evaluated is worth cost incurred to control vulnerability
- $CBA = ALE \text{ (prior)} - ALE \text{ (post)} - ACS$
- ALE(prior) is annualized loss expectancy of risk before implementation of control
- ALE(post) is estimated ALE based on control being in place for a period of time
- ACS is the annualized cost of the safeguard

Exercises

- Problem 3, 5 in page 167-168

Benchmarking

- An alternative approach to risk management
- Benchmarking is process of seeking out and studying practices in **other organizations** that one's own organization **desires to duplicate**
- One of two measures typically used to compare practices:
 - Metrics-based measures

Benchmarking --Metrics-based measures

- Metrics-based measures are comparisons based on numerical standards:
 - Number of successful attacks,
 - staff-hours spent of systems protection,
 - dollars spent on protection,
 - number of security personnel,
 - estimated value of info lost in attacks,
 - loss in productivity hours
- Performance gap is the difference between an organization's measures and those of others.

Benchmarking -- Process-based measures

- Less focus on numbers
- More strategic than metrics-based measures
- Examine *activities* an individual company performs
- Focus on *methods* to accomplish a particular process
- Rather than the outcome

Benchmarking

- Standard of due care: when adopting levels of security for a legal defense, organization shows it **has done what any prudent organization would do in similar circumstances**
- Due diligence: demonstration that organization is diligent in ensuring that implemented standards continue to provide required level of protection
- Failure to support standard of due care or due diligence can leave organization open to **legal liability**

Benchmarking – Best Practices

- Best business practices: security efforts that provide a superior level protection of information
- Available Resources
 - Federal Agency Security Project: <http://fasp.nist.gov>
 - CERT web site: www.cert.org/security-improvement/

Seven Key Areas of Best Practice from Microsoft

1. Use antivirus software
2. Use strong passwords
3. Verify your software security settings
4. Update product security
5. Build personal firewalls
6. Back up early and often
7. Protect against power surges and loss

Problems with Applying Benchmarking and Best Practices

- Organizations don't talk to each other (biggest problem)
- No two organizations are identical
- Best practices are a moving target
- Knowing what **was going on** in information security industry in recent years through benchmarking **doesn't** necessarily prepare for **what's next**

Baselining

- Analysis of measures against established standards
- In information security, baselining is comparison of security activities and events against an organization's future performance.
- The information gathered for an organization's first risk assessment becomes the baseline for future comparison.

KEY

- “the goal of information security is not to bring residual risk to zero; it is to bring residual risk into line with an organization’s comfort zone or risk appetite”

Documenting Results

- At minimum, each information **asset-threat pair** should have documented **control strategy** clearly identifying any remaining residual risk, and **feasibility studies** to justify the findings.
- Another option: document **outcome of control strategy** for each information **asset-vulnerability pair** as an action plan

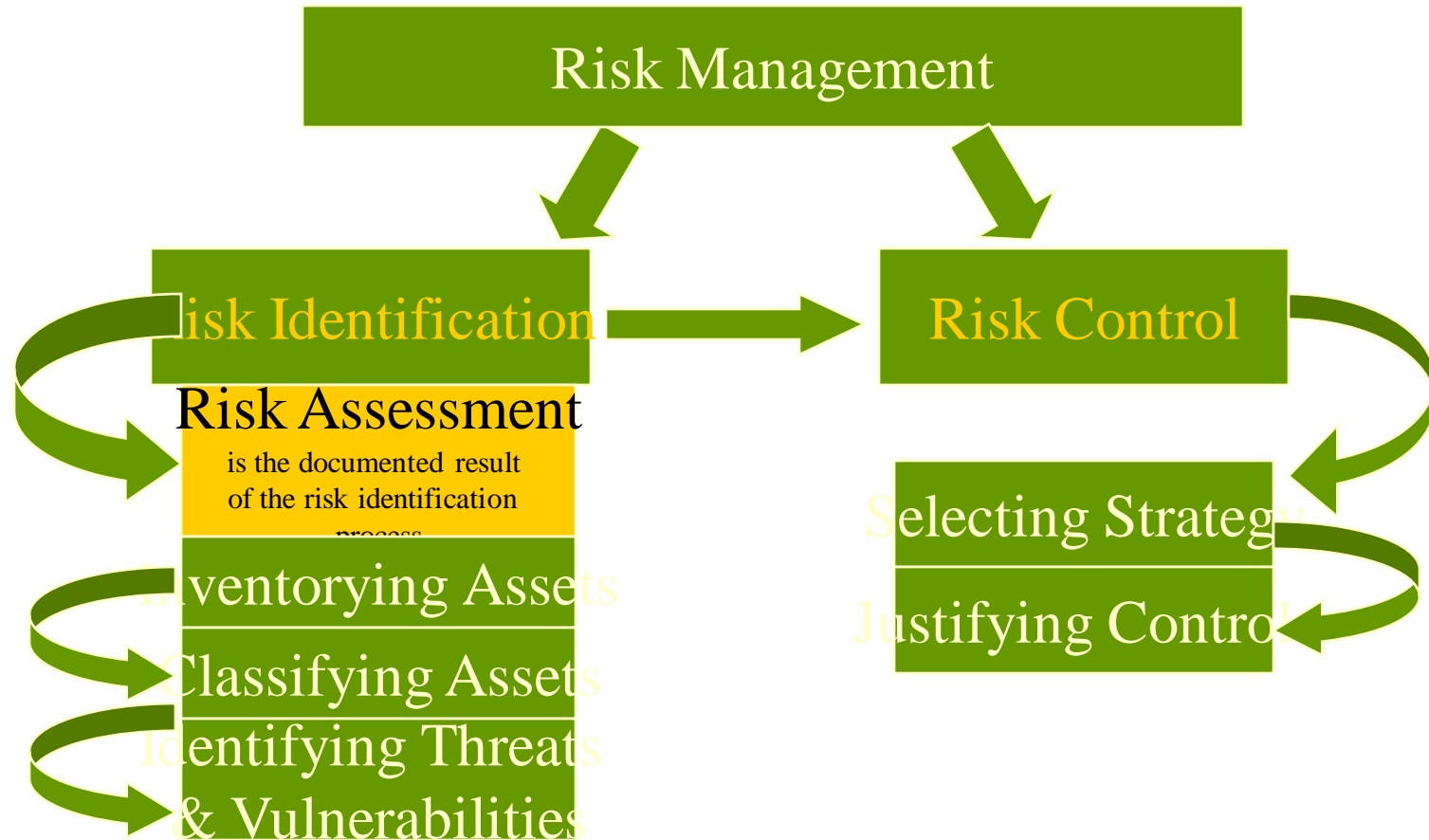
Summary

- Risk identification: formal process of examining and documenting risk present in information systems
- Risk control: process of taking carefully reasoned steps to ensure the confidentiality, integrity, and availability of components in organization's information system
- Risk identification
 - A risk management strategy enables identification, classification, and prioritization of organization's information assets
 - Residual risk: risk that remains to the information asset even after the existing control is applied

Summary

- Risk control: four strategies are used to control risks that result from vulnerabilities:
 - Apply safeguards (avoidance)
 - Transfer the risk (transference)
 - Reduce impact (mitigation)
 - Understand consequences and accept risk (acceptance)

Components of Risk Management



Chapter 5 Planning for Security

Begin with the end in mind.

STEPHEN COVEY, AUTHOR OF SEVEN
HABITS OF HIGHLY EFFECTIVE PEOPLE

PRINCIPLES OF
INFORMATION SECURITY

Second Edition

Introduction

- Creation of information security program includes:
 - Creation of *policies, standards, and practices*, selection or creation of information security architecture and the development
 - Use of a detailed information security *blueprint* creates plan for future success
 - Creation of *contingency planning* consisting of incident response planning, disaster recovery planning, and business continuity plans
- Without policy, blueprints, and planning, organization is unable to meet information security needs of various communities of interest

Information Security Policy, Standards and Practices

- Communities of interest must consider policies as basis for all information security efforts
- Policies direct how issues should be addressed and technologies used
- Security policies are least expensive controls to execute but most difficult to implement

Sp
rin
g
20
07

Shaping Policy Difficult

- Never conflict with laws
- Standup in court if challenged
- Be properly administered through dissemination and documented acceptance

Policy

- Plan or course of action
- Convey instructions
- Organizational laws
- Dictate acceptable and unacceptable behavior

Policy

- Define
 - What is right
 - What is wrong
 - The appeal process
 - What are the penalties for violating policy
- Written to support the mission, vision and strategic plan of organization
- For a policy to be effective, must be properly disseminated, read, understood and agreed to by all members of organization

Standards

- Detail statements of what must be done to comply with policy
- Types
 - Informal – de facto standards
 - Formal – de jure standards

Mission/Vision/Strategic Plan

- Mission – written statement of organization purpose
- Vision – written statement of organization goals
- Strategic Plan - written statement of moving the organization toward its mission

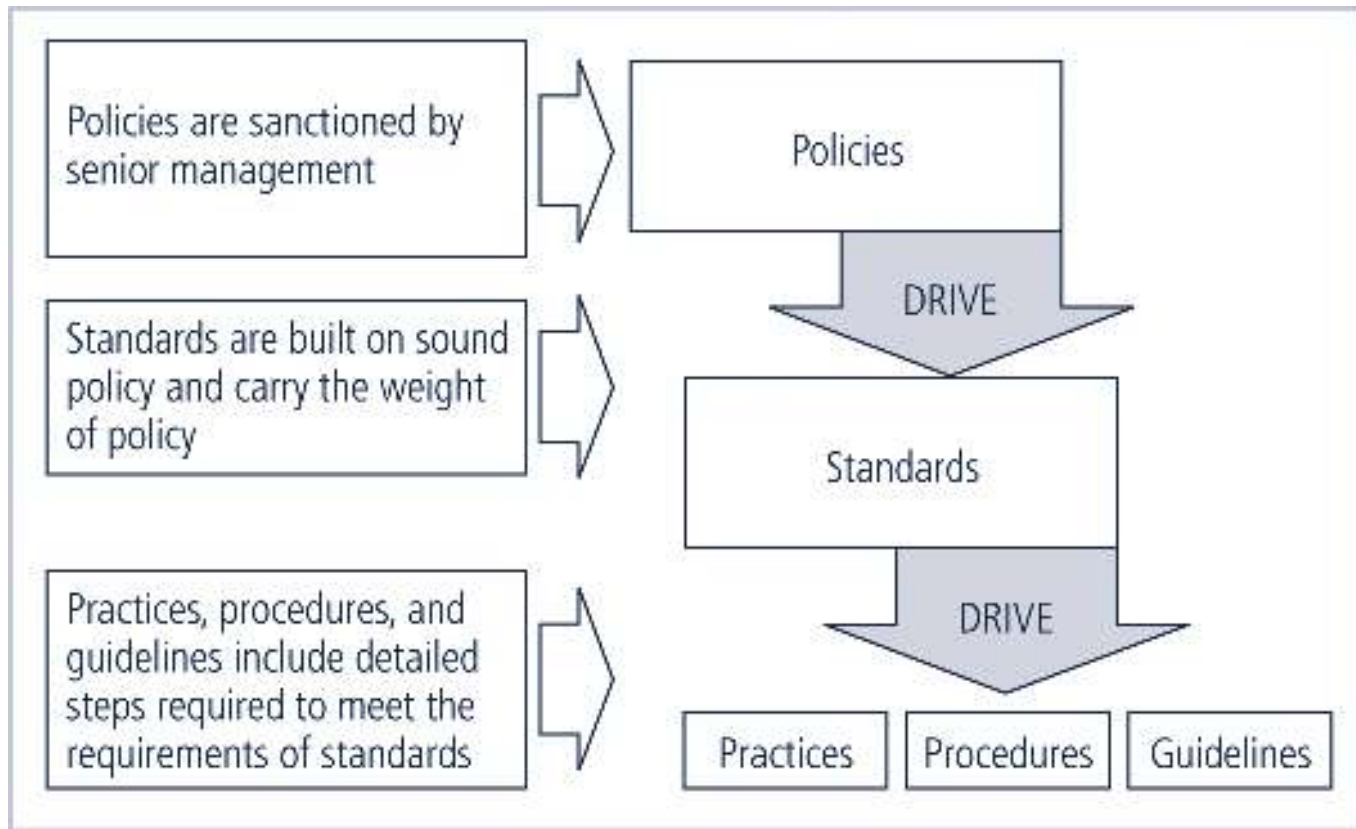


FIGURE 5-1 Policies, Standards, and Practices

Policies

- Security Policy – set of rules that protects and organization's assets
- Information security policy – set of rules that protects an organization's information assets
- Three types
 - General Issue-specific
 - System-specific

Enterprise Information Security Policy (EISP)

- General Information Security Document
- Shapes the philosophy of security in IT
- Executive-level document, usually drafted by or with CIO of the organization, 2-10 pages
- Typically addresses compliance in two areas
 - Ensure *meeting requirements* to establish program
 - *Responsibilities* assigned therein to various organizational components
 - Use of specified *penalties and disciplinary action*

ISSP

- Issue-Specific Security Policy
- Addresses specific areas of technology
- Requires frequent updates
- Contains a statement on the organization's position on a specific issue

3 Approaches to ISSP

- Create independent document tailored to a specific issue
 - Scattered approach
 - Departmentalized
- Create single comprehensive document covering all issues
 - Centralized management and control
 - Tend to over generalize the issue
 - Sip vulnerabilities

3 Approaches to ISSP

- Create a modular plan
 - Unified policy creation and administration
 - Maintain each specific issue's requirements
 - Provide balance

ISSP

- Statement of Policy
- Authorization Access & Equipment Use
- Prohibited Equipment Use
- System Management
 - Focus on user's relationship
- Violations of Policy
- Policy review & modification
- Limitations & Liability

Systems-Specific Policy (SysSP)

- SysSPs frequently codified as standards and procedures
- used when configuring or maintaining systems
- Systems-specific policies fall into two groups
 - Access control lists (ACLs)
 - Configuration rules

ACL Policies

- Restrict access from anyone & anywhere
- Can regulate specific user, computer, time, duration, file
- What regulated
 - Who can use the system
 - What authorization users can access
 - When authorization users can access
 - Where authorization users can access

ACL Policies

- Authorization determined by persons identity
- Can regulated specific computer equipment
- Regulate access to data
 - Read
 - Write
 - Modify
 - Copy
 - Compare

Rule Policies

- Rule policies are more specific to operation of a system than ACLs
- May or may not deal with user directly
- Many security systems require specific configuration scripts telling systems what actions to perform on each set of information they process

Policy Management

- Living documents
- Must be managed as they constantly changed and grow
- Must be properly disseminated
- Must be properly managed
- Responsible individual
 - Policy administrator
 - Champion & manager
 - Not necessarily a technically oriented person

Reviews

- Schedule
 - Retain effectiveness in changing environment
 - Periodically reviewed
 - Should be defined and published
 - Should be reviewed at least annually
- Procedures and practices
 - Recommendations for change
 - Reality one person draft

Document Configuration Management

- Include date of original
- Includes date of revision
- Include expiration date

Information Classification

- Classification of information is an important aspect of policy
- Policies are classified, least for “internal use only”.
- *A clean desk policy* stipulates that at end of business day, classified information must be properly stored and secured

The Information Security Blueprint

- **Security Blueprint** is the basis for design, selection, and implementation of
 - all security policies,
 - education and training programs, and
 - technological controls
- More detailed version of **security framework** (outline of overall information security strategy for organization)
- Should specify tasks to be accomplished and the order in which they are to be realized
- One approach to selecting a methodology by which to develop an information security blueprint is to **adopt a published model or framework** for information security

ISO 17799/BS7799

- Information technology – code of practice for information security management from
 - ISO ([International Organization for Standards](#))
 - IEC ([International Electro-technical Commission](#))
- One of the most widely referenced and often discussed security models
- ISO/IEC 17799
 - Purpose – “give recommendations for information security management for use by those who are responsible for initiating, implementing, or maintaining security in their organization.
 - Provides a common basis
 - Must pay for these

Sp
rin
g
20
07

NIST Security Models

- Another possible approach described in documents available from Computer Security Resource Center of **National Institute for Standards and Technology** (NIST)
- Public ally available at no charge
- Several publications dealing with various aspects

NIST Special Publication 800-14

- Security supports mission of organization; is an integral element of sound management
- Security should be cost-effective; owners have security responsibilities outside their own organizations
- Security responsibilities and accountability should be made explicit; security requires a comprehensive and integrated approach

Sp
rin
g
20
07

IETF Security Architecture

- Internet Engineering Task Force
- Security Area Working Group acts as advisory board for protocols and areas developed and promoted by the Internet Society
- *RFC 2196: Site Security Handbook* covers five basic areas of security with detailed discussions on development and implementation

VISA International Security Model

- VISA Internal
 - Developed two important documents that improve and regulate information systems: “Security Assessment Process”; “Agreed Upon Procedures”
 - Focus on system that can and do integrate with VISA
- Base lining and Best Practices
 - Comparison of your organization security with another

Hybrid Framework for a Blueprint of an Information Security System

- Result of a detailed analysis of components of all documents, standards, and Web-based information described previously
- Offered here as a balanced introductory blueprint for learning the blueprint development process
- People must become a layer of security
- Human firewall
- Information security implementation
 - Policies
 - People
 - Education, training, and awareness
 - Technology

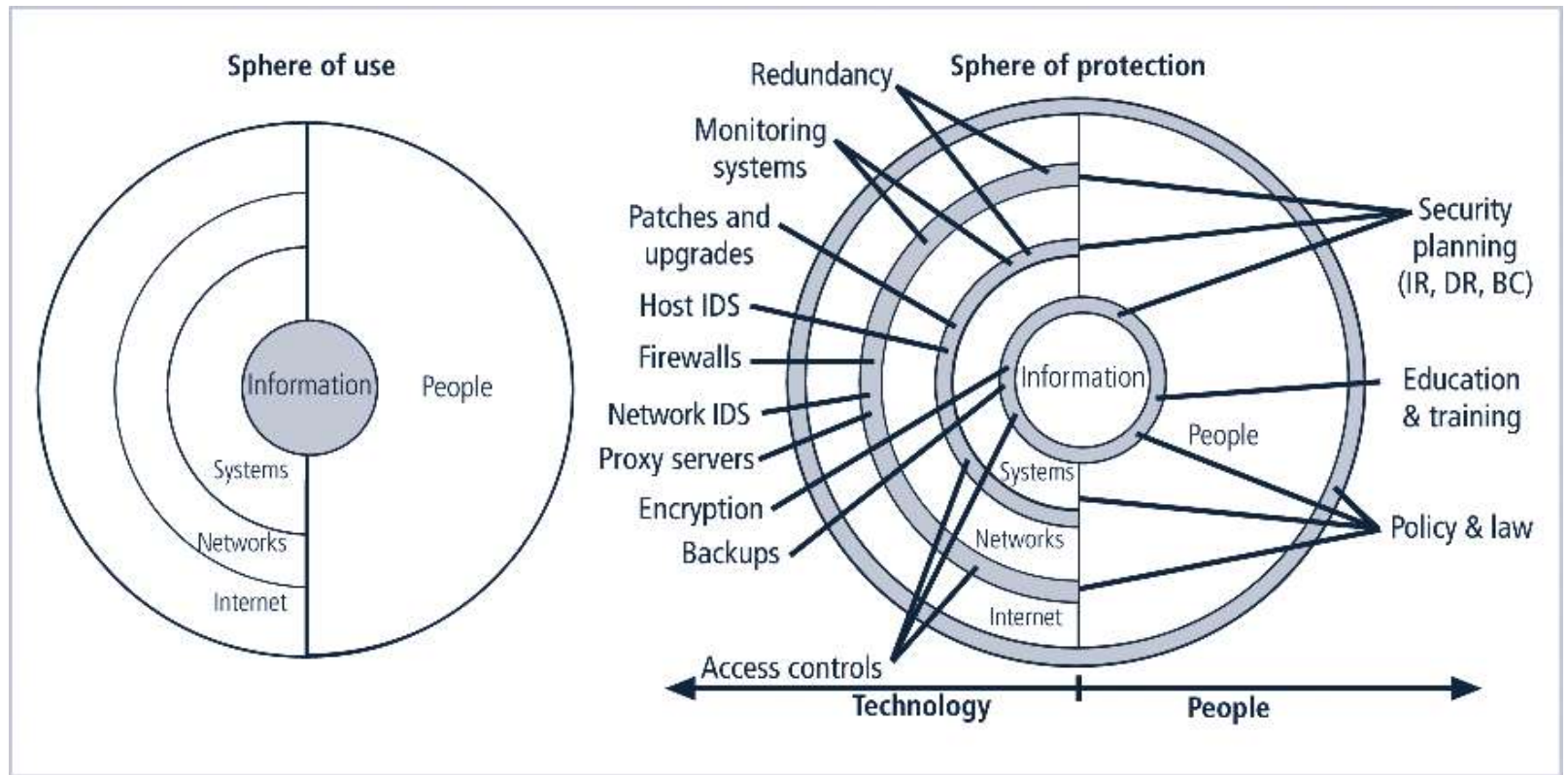


FIGURE 5-15 Spheres of Security

Hybrid Framework

- Managerial Controls
 - Cover security process
 - Implemented by security administrator
 - Set directions and scope
 - Addresses the design and implementation
 - Addresses risk management & security control reviews
 - Necessity and scope of legal compliance

Hybrid Framework

- Operational Controls
 - Operational functionality of security
 - Disaster recovery
 - Incident response planning
 - Personnel and physical security
 - Protection of production inputs and outputs
 - Development of education, training & awareness
 - Addresses hardware and software system maintenance
 - Integrity of data

Hybrid Framework

- Technical Controls
 - Addresses the tactical & technical issues
 - Addresses specifics of technology selection & acquisition
 - Addresses identification
 - Addresses authentication
 - Addresses authorization
 - Addresses accountability

Hybrid Framework

- Technical Controls
 - Addresses development and implementation of audits
 - Covers cryptography
 - Classification of assets and users

Design of Security Architecture

- Security Architecture Components
 - Defenses in Depth,
 - Implementation of security in layers, policy, training, technology.
 - Requires that organization establish sufficient security controls and safeguards so that an intruder faces multiple layers of controls
 - Security Perimeter
 - Point at which an organization's security protection ends and outside world begins
 - Does not apply to internal attacks from employee threats or on-site physical threats

Sp

rin

g

20

07

Design of Security Architecture

- Security Architecture Components
 - First level of security – protects all internal systems from outside threats
 - Multiple technologies segregate the protected information
 - Security domains or areas of trust

Key Technology Components

- Firewall
 - Device that selectively discriminates against information flowing in and out
 - Specially configured computer
 - Usually on perimeter part of or just behind gateway router
- DMZ
 - Buffer against outside attacks
 - No mans land between computer and world
 - Web servers often go here

Key Technology Components

- Proxy Server
 - Performs actions of behalf of another system
 - Configured to look like a web server
 - Assigned the domain name
 - Retrieves and transmits data
 - Cache server

Key Technology Components

- IDS

- Intrusion Detection System

- Host based

- Installed on machines they protect
 - Monitor host machines

- Network based

- Look at patterns of network traffic
 - Attempt to detect unusual activity
 - Requires database of previous activity
 - Uses “machine learning” techniques
 - Can use information from similar networks

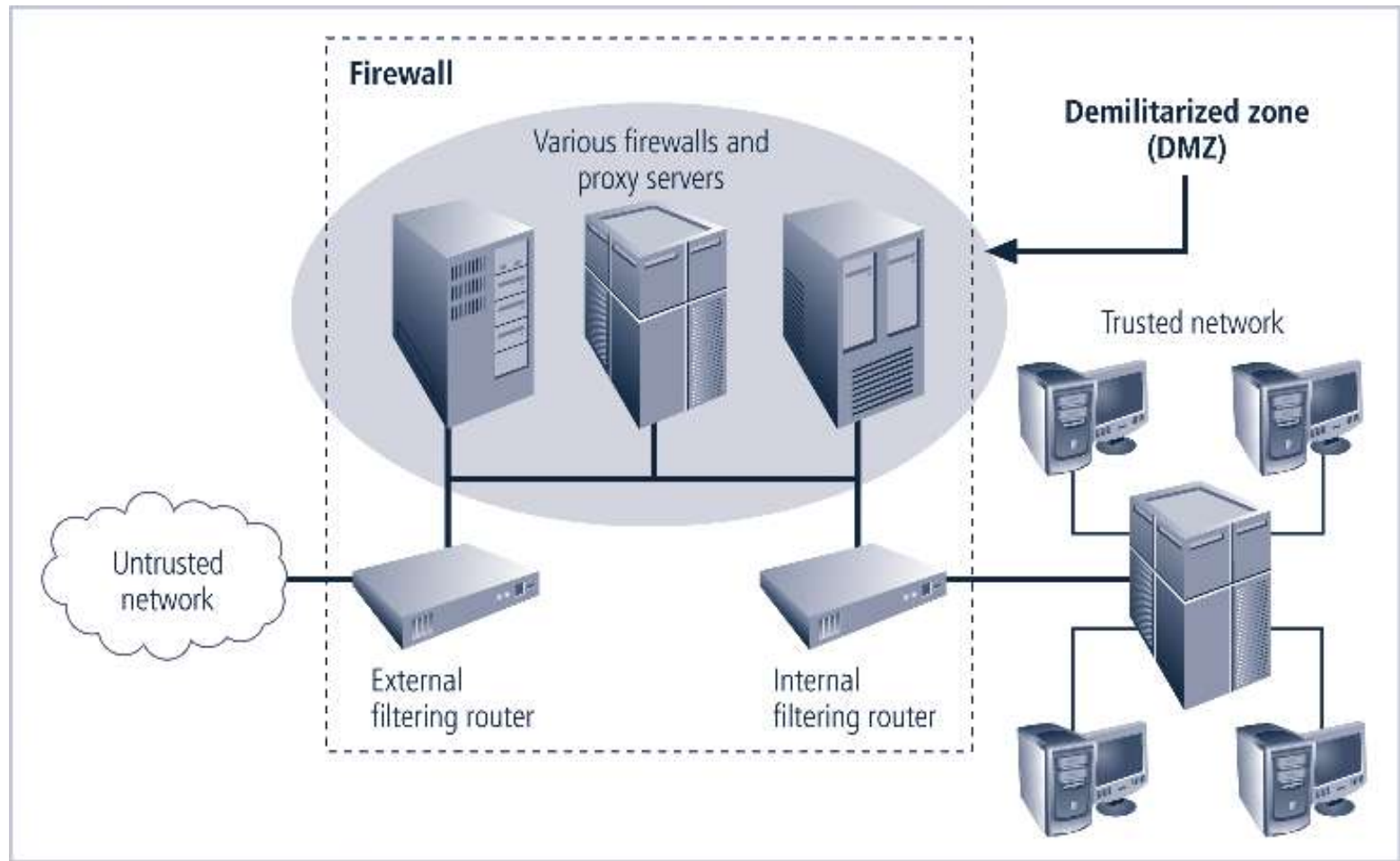


FIGURE 5-18 Firewalls, Proxy Servers, and DMZs

Spring
2007

Key Technology Components

- SETA
 - Security education, training and awareness
 - Employee errors among top threats
 - Purpose
 - Improve awareness of need to protect
 - Develop skills and knowledge
 - Build in-depth knowledge to design, implement, or operate security programs

Security Education

- Everyone in an organization needs to be trained and aware of information security; not every member needs formal degree or certificate in information security
- When formal education for individuals in security is needed, an employee can identify curriculum available from local institutions of higher learning or continuing education

Sp
rin
g
20
07

Security Training

- Involves providing members of organization with detailed information and hands-on instruction designed to prepare them to perform their duties securely
- Management of information security can develop customized in-house training or outsource the training program

Security Awareness

- One of least frequently implemented but most beneficial programs is the security awareness program
- Designed to keep information security at the forefront of users' minds
- Need not be complicated or expensive
- If the program is not actively implemented, employees begin to “tune out” and risk of

Sp
rin
g
20
07

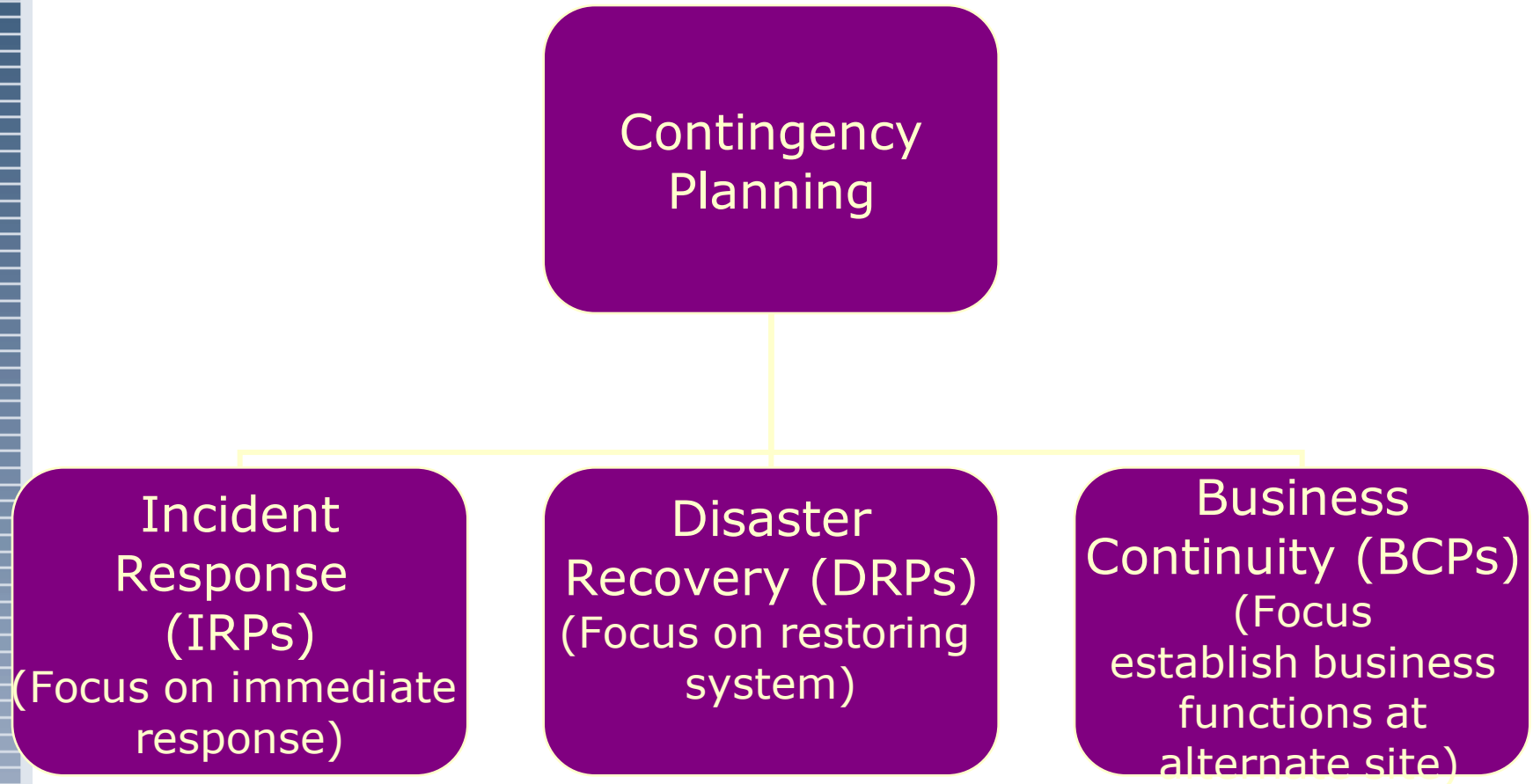


Continuity Strategies

Continuity Strategies

- Continuous availability of info systems
- Probability high for attack
- Managers must be ready to act
- Contingency Plan (CP)
 - Prepared by organization
 - Anticipate, react to, & recover from attacks
 - Restore organization to normal operations

Components of Contingency Plan



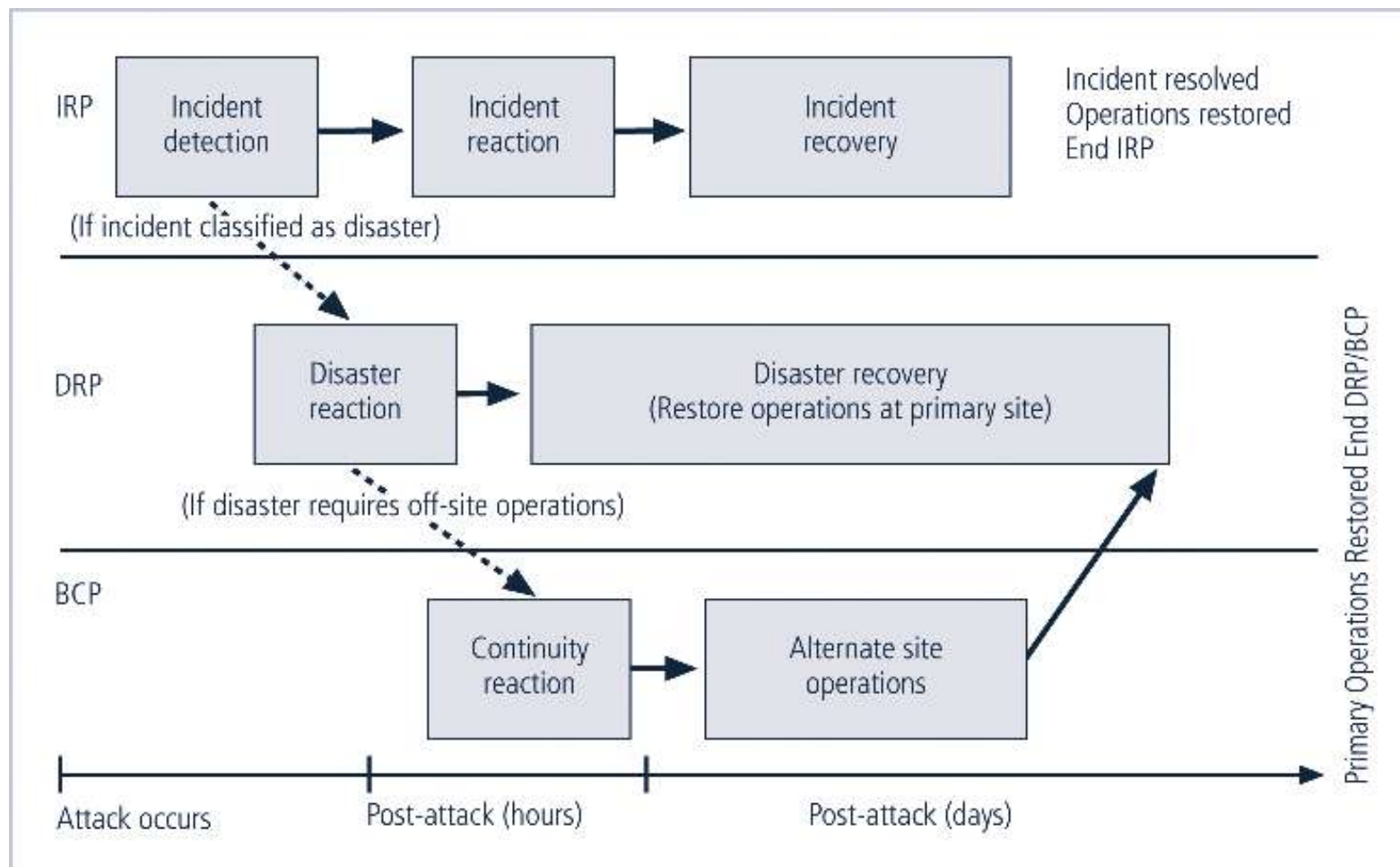


FIGURE 5-22 Contingency Planning Timeline

Continuity Strategies (continued)

- Before planning can begin, a team has to plan effort and prepare resulting documents
- **Champion**: high-level manager to support, promote, and endorse findings of project
- **Project manager**: leads project and makes sure sound project planning process is used, a complete and useful project plan is developed, and project resources are prudently managed
- **Team members**: should be managers or their representatives from various communities of

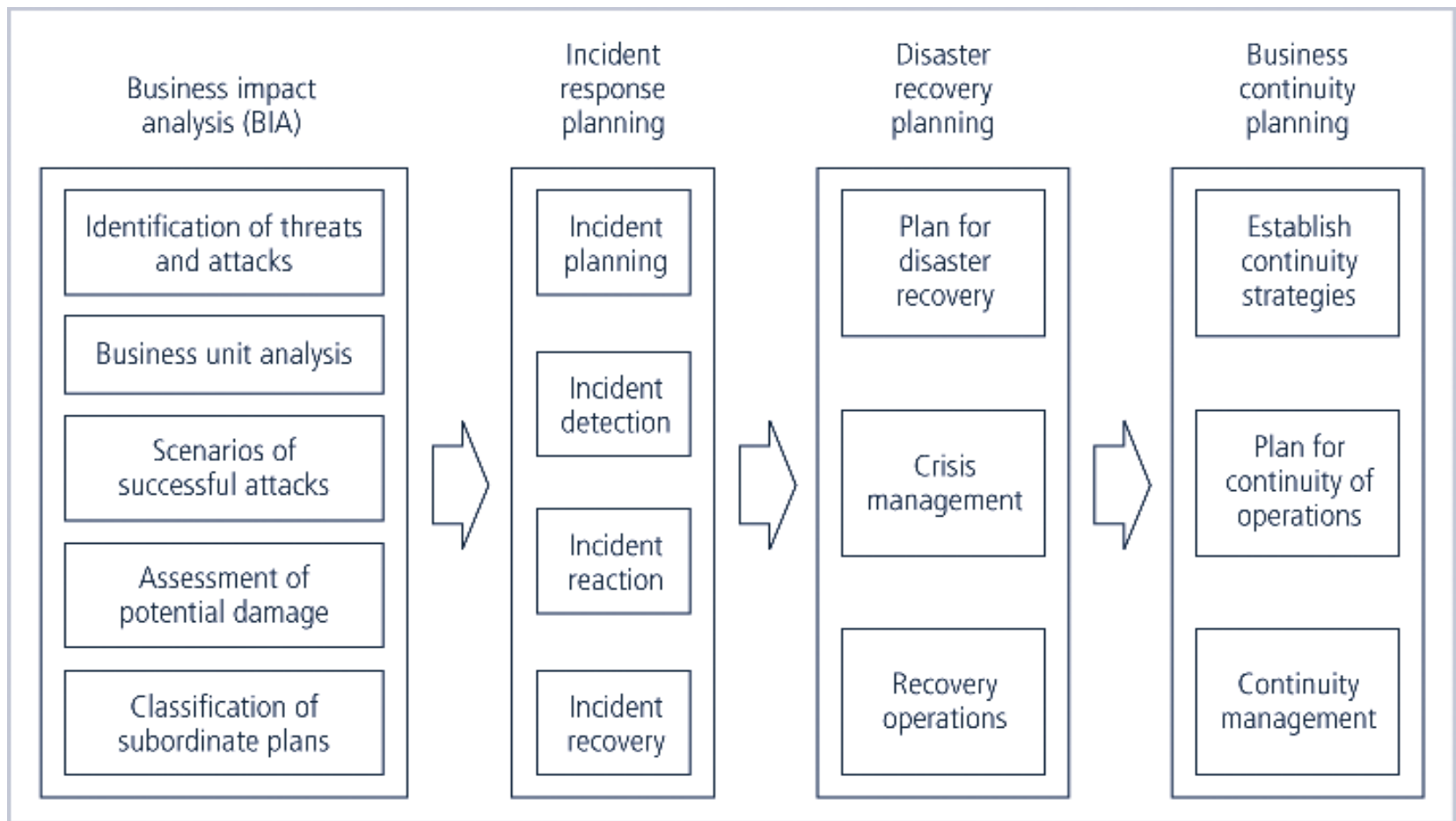


FIGURE 5-23 Major Steps in Contingency Planning

Business Impact Analysis (BIA)

- Investigate & assess impact of various attack
- First risk assessment – then BIA
- Prioritized list of threats & critical info
- Detailed scenarios of potential impact of each attack
- Answers question
 - “if the attack succeeds, what do you do then?”

BIA Sections

- Threat attack identification & prioritization
 - Attack profile – detailed description of activities that occur during an attack
 - Determine the extent of resulting damage
- Business Unit analysis
 - Analysis & prioritization-business functions
 - Identify & prioritize functions w/in orgs units

BIA Sections

- Attack success scenario development
 - Series of scenarios showing impact
 - Each treat on prioritized list
 - Alternate outcomes
 - Best, worst, probable cases
- Potential damage assessment
 - Estimate cost of best, worst, probable
 - What must be done under each
 - Not how much to spend
- Subordinate Plan Classification
 - Basis for classification as disastrous not disastrous

Incident Response Planning (IRPs)

- Incident response planning covers identification of, classification of, and response to an incident
- Attacks classified as **incidents** if they:
 - Are directed against information assets
 - Have a realistic chance of success
 - Could threaten confidentiality, integrity, or availability of information resources
- Incident response (IR) is more reactive, than proactive, with the exception of planning that must occur to prepare IR teams to be ready to react to an incident

Incident Response

- Set of activities taken to plan for, detect, and correct the impact
- Incident planning
 - Requires understanding BIA scenarios
 - Develop series of predefined responses
 - Enables org to react quickly
- Incident detection
 - Mechanisms – intrusion detection systems, virus detection, system administrators, end users

Incident Detection

- Possible indicators
 - Presence of unfamiliar files
 - Execution of unknown programs or processes
 - Unusual consumption of computing resources
 - Unusual system crashes

Incident Detection

- Probable indicators
 - Activities at unexpected times
 - Presence of new accounts
 - Reported attacks
 - Notification from IDS
- Definite indicators
 - Use of dormant accounts
 - Changes to logs
 - Presence of hacker tools
 - Notification by partner or peer
 - Notification by hackers

Incident Detection

- Predefined Situation
 - Loss of availability
 - Loss of integrity
 - Loss of confidentiality
 - Violation of policy
 - Violation of law

Incident Reaction

- Actions outlined in the IRP
- Guide the organization
 - Stop the incident
 - Mitigate the impact
 - Provide information recovery
- Notify key personnel
- Document incident

Incident Containment Strategies

- Sever affected communication circuits
- Disable accounts
- Reconfigure firewall
- Disable process or service
- Take down email
- Stop all computers and network devices
- Isolate affected channels, processes, services, or computers

Incident Recovery

- Get everyone moving and focused
- Assess Damage
- Recovery
 - Identify and resolve vulnerabilities
 - Address safeguards
 - Evaluate monitoring capabilities
 - Restore data from backups
 - Restore process and services
 - Continuously monitor system
 - Restore confidence

Disaster Recovery Plan (DRPs)

- Provide guidance in the event of a disaster
- Clear establishment of priorities
- Clear delegation of roles & responsibilities
- Alert key personnel
- Document disaster
- Mitigate impact
- Evacuation of physical assets

Crisis Management

- Disaster recovery personnel must know their responses *without any supporting documentation*
- Actions taken during and after a disaster *focusing on people involved* and *addressing viability of business*
- Crisis management team responsible for managing event from an enterprise perspective and covers:
 - Support personnel and loved ones
 - Determine impact on normal operations
 - Keep public informed
 - Communicate with major players such as major customers, suppliers, partners, regulatory agencies, industry organizations, the media, and other interested parties

Business Continuity Planning (BCPs)

- Outlines **reestablishment** of critical business operations during a disaster that impacts operations
- If disaster has rendered the business unusable for continued operations, there must be **a plan to allow business to continue functioning**
- Development of BCP somewhat simpler than **IRP or DRP**; consists primarily of **selecting a**

Continuity Strategies

- There are a number of strategies for planning for business continuity
- Determining factor in selecting between options usually cost
- In general there are three exclusive options: hot sites; warm sites; and cold sites
- Three shared functions: time-share; service

Alternative Site Configurations

- Hot sites
 - Fully configured computer facilities
 - All services & communication links
 - Physical plant operations
- Warm sites
 - Does not include actual applications
 - Application may not be installed and configured
 - Required hours to days to become operational
- Cold sites
 - Rudimentary services and facilities
 - No hardware or peripherals
 - empty room

Alternative Site Configurations

- Time-shares
 - Hot, warm, or cold
 - Leased with other orgs
- Service bureau
 - Provides service for a fee
- Mutual agreements
 - A contract between two or more organizations that specifies how each will assist the other in the event of a disaster.

Off-Site Disaster Data Storage

- To get sites up and running quickly, organization must have ability to port data into new site's systems
- Electronic vaulting
 - Transfer of large batches of data
 - Receiving server archives data
 - Fee
- Journaling
 - Transfer of live transactions to off-site
 - Only transactions are transferred
 - Transfer is real time

Off-Site Disaster Data Storage

- Shadowing
 - Duplicated databases
 - Multiple servers
 - Processes duplicated
 - 3 or more copies simultaneously

Model For a Consolidated Contingency Plan

- Single document set supports concise planning and encourages smaller organizations to develop, test, and use IR and DR plans
- Model is based on analyses of disaster recovery and incident response plans of dozens of organizations

The Planning Document

- Six steps in contingency planning process
 - Identifying mission- or business-critical functions
 - Identifying resources that support critical functions
 - Anticipating potential contingencies or disasters
 - Selecting contingency planning strategies
 - Implementing contingency strategies
 - Testing and revising strategy

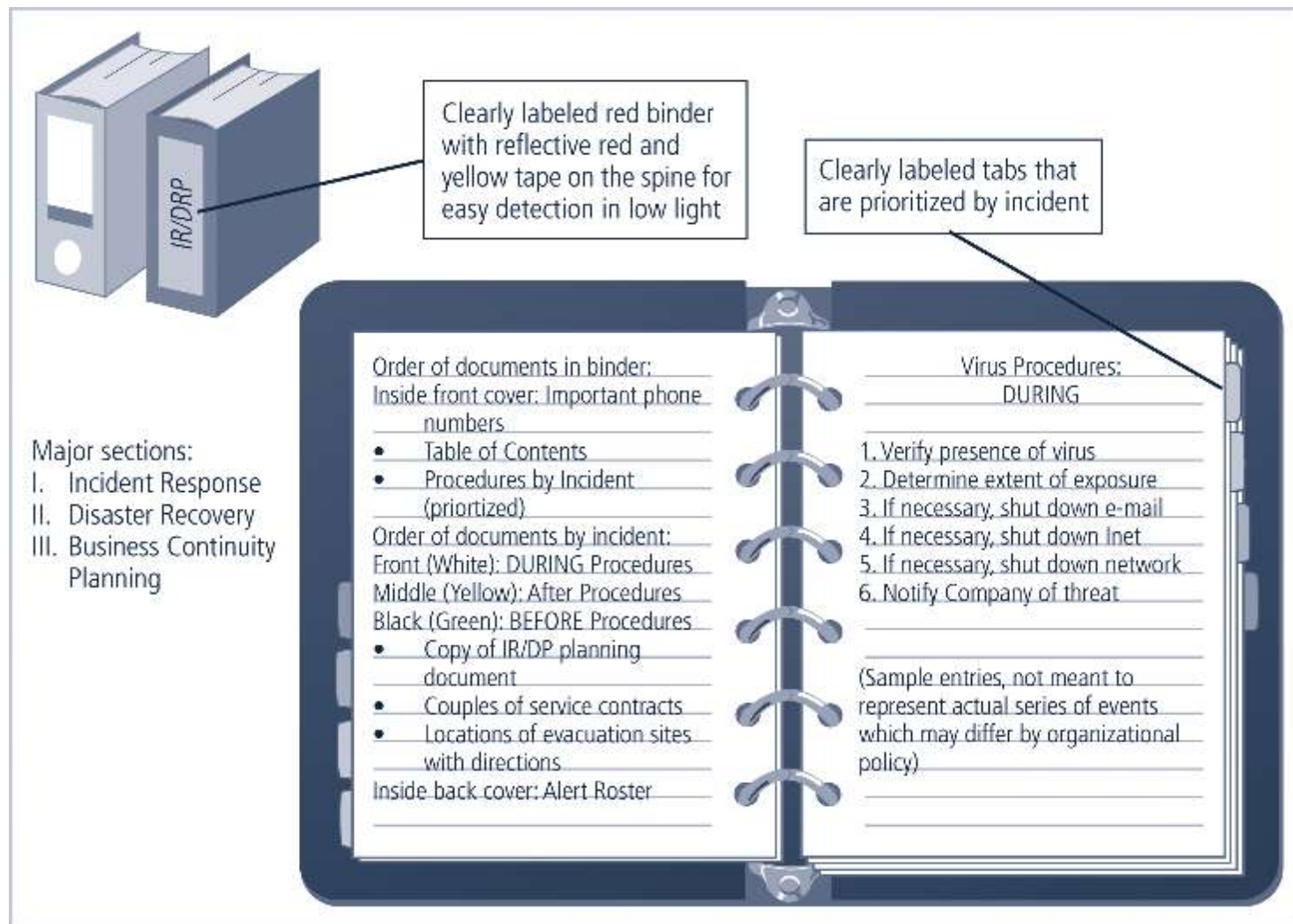


FIGURE 5-24 Contingency Plan Format

Law Enforcement Involvement

- When incident at hand constitutes a violation of law, organization may determine involving law enforcement is necessary
- Questions:
 - When should organization get law enforcement involved?
 - What level of law enforcement agency should be involved (local, state, federal)?
 - What happens when law enforcement agency is involved?
- Some questions are best answered by organization's legal department

Benefits and Drawbacks of Law Enforcement Involvement

- Involving law enforcement agencies has **advantages**:
 - Agencies may be better equipped at processing evidence
 - Organization may be less effective in convicting suspects
 - Law enforcement agencies prepared to handle warrants and subpoenas needed
 - Law enforcement skilled at obtaining witness statements and other information collection

Benefits and Drawbacks of Law Enforcement Involvement (continued)

- Involving law enforcement agencies has **disadvantages**:
 - Once a law enforcement agency takes over case, organization loses complete control over chain of events
 - Organization may not hear about case for weeks or months
 - Equipment vital to the organization's business may be tagged evidence
 - If organization detects a criminal act, it is legally obligated to involve appropriate law enforcement officials

Summary

- Management has essential role in development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines
- Information security blueprint is planning document that is basis for design, selection, and implementation of all security policies, education and training programs, and technological controls

Summary

- Information security education, training, and awareness (SETA) is control measure that reduces accidental security breaches and increases organizational resistance to many other forms of attack
- Contingency planning (CP) made up of three components: incident response planning (IRP), disaster recovery planning (DRP), and business continuity planning (BCP)

Implementing Information Security

10

Change is good. You go first!

DILBERT (BY SCOTT ADAMS)

PRINCIPLES of
INFORMATION
SECURITY

Second Edition

Learning Objectives

Upon completion of this material, you should be able to:

- Understand how an organization's security blueprint becomes a project plan
- Understand the need for professional project management for complex projects
- Follow technical strategies and models for implementing the project plan
- Identify the nontechnical problems that organizations face in times of rapid change

Introduction

- SecSDLC implementation phase accomplished through changing configuration and operation of organization's information systems
- Implementation includes changes to procedures, people, hardware, software, and data
- Organization translates blueprint for information security into a concrete project plan

Project Management for Information Security

- Once organization's vision and objectives are understood, process for creating project plan can be defined
- Major steps in executing project plan are:
 - Planning the project
 - Supervising tasks and action steps
 - Wrapping up
- Each organization must determine its own project management methodology for IT and information security projects

Developing the Project Plan

- Creation of project plan can be done using work breakdown structure (WBS)
- Major project tasks in WBS are work to be accomplished; individuals assigned; start and end dates; amount of effort required; estimated capital and noncapital expenses; and identification of dependencies between/among tasks
- Each major WBS task further divided into smaller tasks or specific action steps

Project Planning Considerations

- As project plan is developed, adding detail is not always straightforward
- Special considerations include financial; priority; time and schedule; staff; procurement; organizational feasibility; and training

Financial Considerations

- No matter what information security needs exist, amount of effort that can be expended depends on funds available
- Cost-benefit analysis must be verified prior to development of project plan
- Both public and private organizations have budgetary constraints, though of a different nature
- To justify an amount budgeted for a security project at either public or for-profit organizations, may be useful to benchmark expenses of similar organizations

Priority Considerations

- In general, most important information security controls should be scheduled first
- Implementation of controls is guided by prioritization of threats and value of threatened information assets

Time and Scheduling Considerations

- Time impacts dozens of points in the development of a project plan, including:
 - Time to order, receive install and configure security control
 - Time to train the users
 - Time to realize return on investment of control

Staffing Considerations

- Lack of enough qualified, trained, and available personnel constrains project plan
- Experienced staff often needed to implement available technologies and develop and implement policies and training programs

Procurement Considerations

- IT and information security planners must consider acquisition of goods and services
- Many constraints on selection process for equipment and services in most organizations, specifically in selection of service vendors or products from manufacturers/suppliers
- These constraints may eliminate a technology from realm of possibilities

Organizational Feasibility Considerations

- Policies require time to develop; new technologies require time to be installed, configured, and tested
- Employees need training on new policies and technology, and how new information security program affects their working lives
- Changes should be transparent to system users, unless the new technology intended to change procedures (e.g., requiring additional authentication or verification)

Training and Indoctrination Considerations

- Size of organization and normal conduct of business may preclude a single large training program on new security procedures/technologies
- Thus, organization should conduct phased-in or pilot approach to implementation

Scope Considerations

- Project scope: concerns boundaries of time and effort-hours needed to deliver planned features and quality level of project deliverables
- In the case of information security, project plans should not attempt to implement entire security system at one time

The Need for Project Management

- Project management requires unique set of skills and thorough understanding of a broad body of specialized knowledge
- Most information security projects require trained project manager (a CISO) or skilled IT manager versed in project management techniques

Supervising Implementation

- Some organizations may designate champion from general management community of interest to supervise implementation of information security project plan
- An alternative is to designate senior IT manager or CIO to lead implementation
- Optimal solution is to designate a suitable person from information security community of interest
- Up to each organization to find most suitable leadership for a successful project implementation

Executing the Plan

- Negative feedback ensures project progress is measured periodically
 - Measured results compared against expected results
 - When significant deviation occurs, corrective action taken
- Often, project manager can adjust one of three parameters for task being corrected: effort and money allocated; scheduling impact; quality or quantity of deliverable

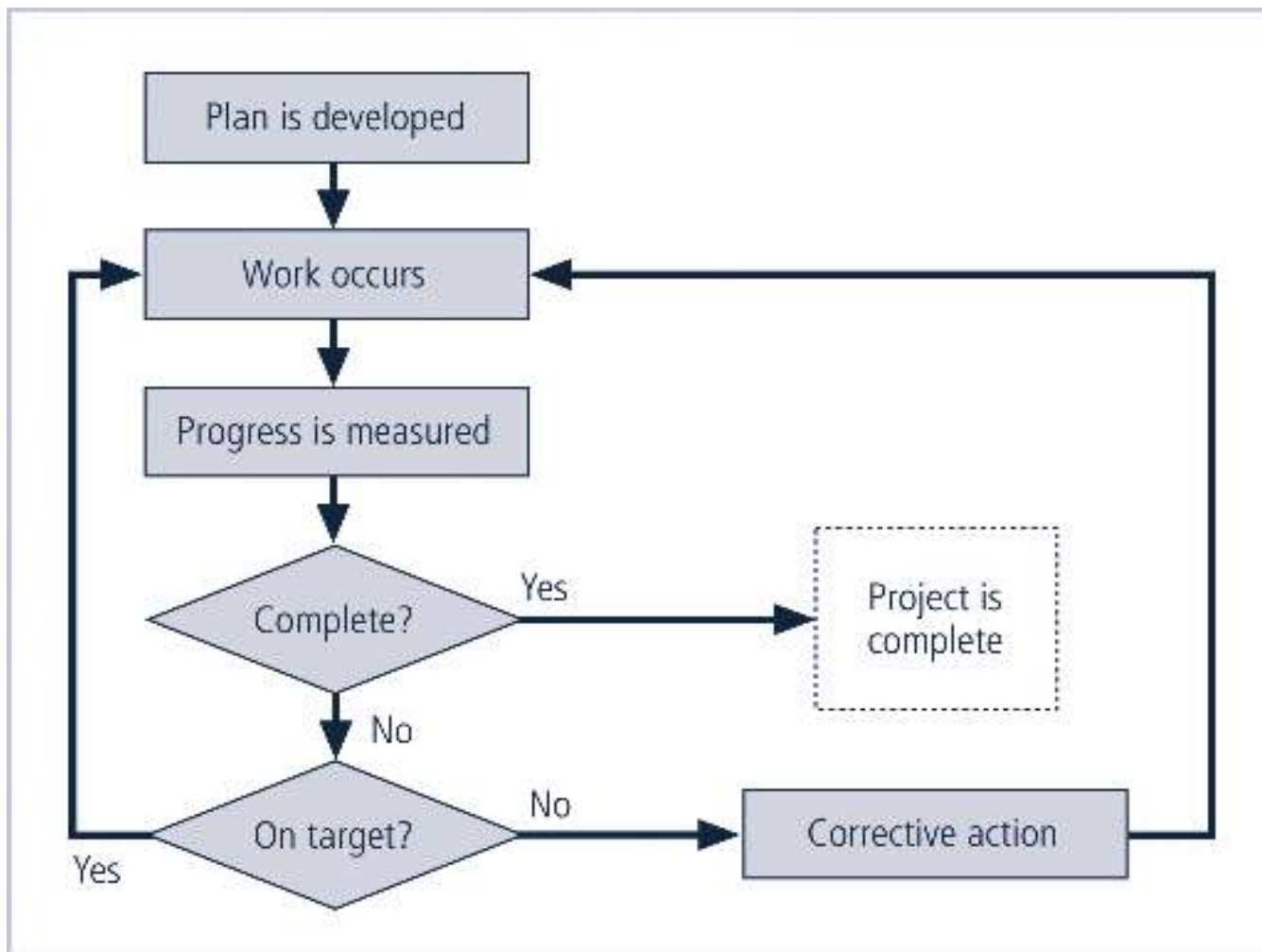


FIGURE 10-1 Negative Feedback Loop

Project Wrap-up

- Project wrap-up usually handled as procedural task and assigned to mid-level IT or information security manager
- Collect documentation, finalize status reports, and deliver final report and presentation at wrap-up meeting
- Goal of wrap-up to resolve any pending issues, critique overall project effort, and draw conclusions about how to improve process

Technical Topics of Implementation

- Some parts of implementation process are technical in nature, dealing with application of technology
- Others are not, dealing instead with human interface to technical systems

Conversion Strategies

- As components of new security system are planned, provisions must be made for changeover from previous method of performing task to new method
- Four basic approaches
 - Direct changeover
 - Phased implementation
 - Pilot implementation
 - Parallel operations

The Bull's-Eye Model for Information Security

Project Planning

- Proven method for prioritizing program of complex change
- Issues addressed from general to specific; focus is on systematic solutions and not individual problems
- Relies on process of evaluating project plans in progression through four layers: policies; networks; systems; applications

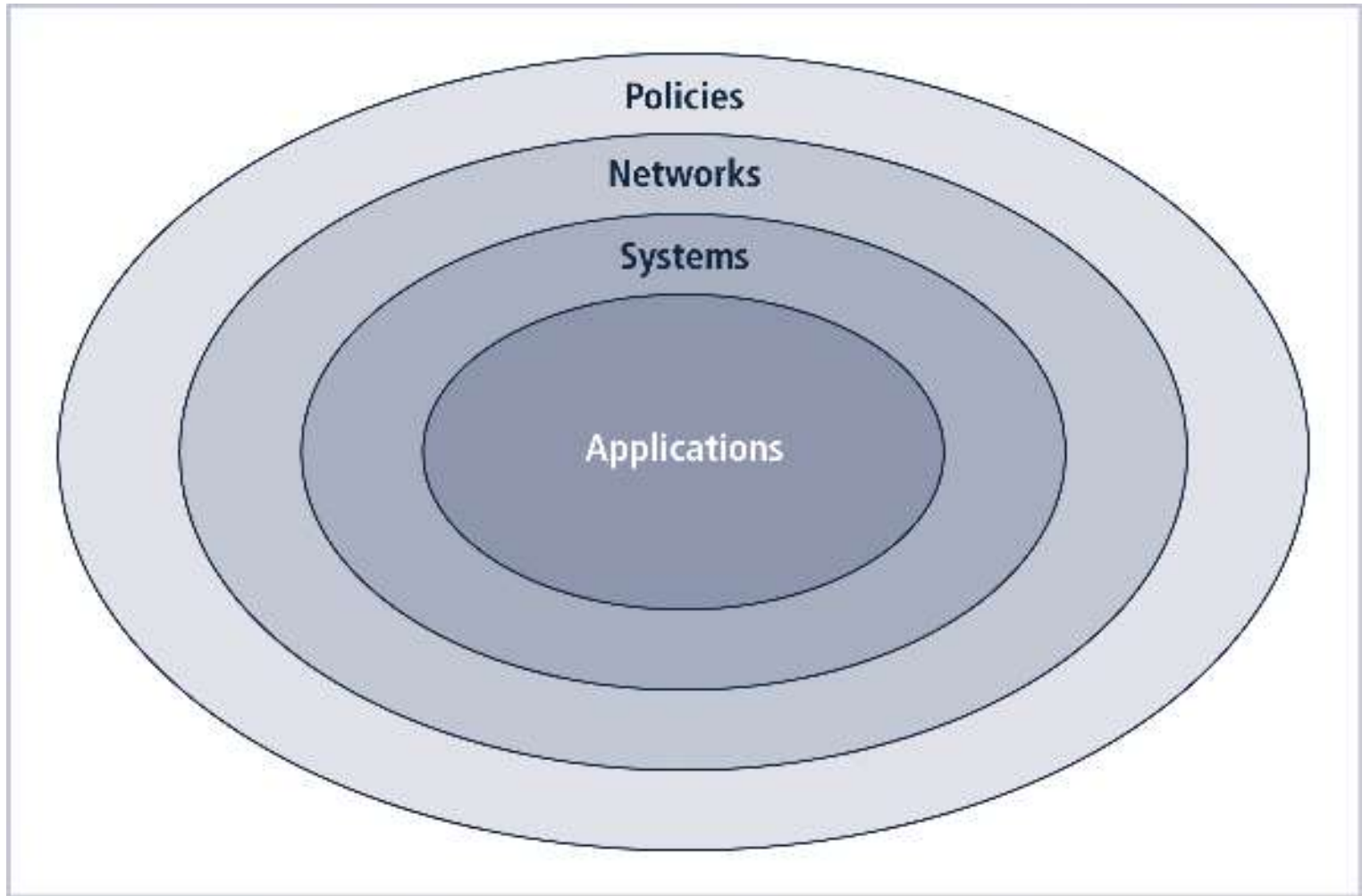


FIGURE 10-2 The Bull's-eye Model

To Outsource or Not

- Just as some organizations outsource IT operations, organizations can outsource part or all of information security programs
- Due to complex nature of outsourcing, advisable to hire best outsourcing specialists and retain best attorneys possible to negotiate and verify legal and technical intricacies

Technology Governance and Change Control

- Technology governance: complex process an organization uses to manage impact and costs from technology implementation, innovation, and obsolescence
- By managing the process of change, organization can improve communication; enhance coordination; reduce unintended consequences; improve quality of service; and ensure groups are complying with policies

Nontechnical Aspects of Implementation

- Other parts of implementation process are not technical in nature, dealing with the human interface to technical systems
- Include creating a culture of change management as well as considerations for organizations facing change

The Culture of Change Management

- Prospect of change can cause employees to build up resistance to change
- The stress of change can increase the probability of mistakes or create vulnerabilities
- Resistance to change can be lowered by building resilience for change
- Lewin change model: unfreezing; moving; refreezing

Considerations for Organizational Change

- Steps can be taken to make organization more amenable to change:
 - Reducing resistance to change from beginning of planning process
 - Develop culture that supports change

Reducing Resistance to Change from the Start

- The more ingrained the previous methods and behaviors, the more difficult the change
- Best to improve interaction between affected members of organization and project planners in early project phases
- Three-step process for project managers: communicate, educate, and involve

Developing a Culture that Supports Change

- Ideal organization fosters resilience to change
- Resilience: organization has come to expect change as a necessary part of organizational culture, and embracing change is more productive than fighting it
- To develop such a culture, organization must successfully accomplish many projects that require change

Summary

- Moving from security blueprint to project plan
- Organizational considerations addressed by project plan
- Project manager's role in success of an information security project
- Technical strategies and models for implementing project plan
- Nontechnical problems that organizations face in times of rapid change

Security and Personnel

11

I think we need to be paranoid optimists.

**ROBERT J. EATON, CHAIRMAN OF THE BOARD OF
MANAGEMENT OF DAIMLERCHRYSLER AG
(RETIRED)**

PRINCIPLES of
INFORMATION
SECURITY

Second Edition

Learning Objectives

Upon completion of this material, you should be able to:

- Understand where and how the information security function is positioned within organizations
- Understand the issues and concerns related to staffing the information security function
- Identify the credentials that professionals in the information security field may acquire to gain recognition in the field
- Appreciate how an organization's employment

Learning Objectives (continued)

- Understand the special security precautions that must be taken when contracting nonemployees
- Recognize the need for the separation of duties
- Understand the special requirements needed for the privacy of personnel data

Introduction

- When implementing information security, there are many human resource issues that must be addressed
 - Positioning and naming
 - Staffing
 - Evaluating impact of information security across every role in IT function
 - Integrating solid information security concepts into personnel practices
- Employees often feel threatened when organization is creating or enhancing overall information security

Positioning and Staffing the Security Function

- The security function can be placed within:
 - IT function
 - Physical security function
 - Administrative services function
 - Insurance and risk management function
 - Legal department
- Organizations balance needs of enforcement with needs for education, training, awareness, and

Staffing The Information Security Function

- Selecting personnel is based on many criteria, including supply and demand
- Many professionals enter security market by gaining skills, experience, and credentials
- At present, information security industry is in period of high demand

Qualifications and Requirements

- The following factors must be addressed:
 - Management should learn more about position requirements and qualifications
 - Upper management should learn about budgetary needs of information security function
 - IT and management must learn more about level of influence and prestige the information security function should be given to be effective
- Organizations typically look for technically qualified information security generalist

Qualifications and Requirements (continued)

- Organizations look for information security professionals who understand:
 - How an organization operates at all levels
 - Information security usually a management problem, not a technical problem
 - Strong communications and writing skills
 - The role of policy in guiding security efforts

Qualifications and Requirements (continued)

- Organizations look for (continued):
 - Most mainstream IT technologies
 - The terminology of IT and information security
 - Threats facing an organization and how they can become attacks
 - How to protect organization's assets from information security attacks
 - How business solutions can be applied to solve specific information security problems

Entry into the Information Security Profession

- Many information security professionals enter the field through one of two career paths:
 - Law enforcement and military
 - Technical, working on security applications and processes
- Today, students select and tailor degree programs to prepare for work in information security
- Organizations can foster greater professionalism by matching candidates to clearly defined

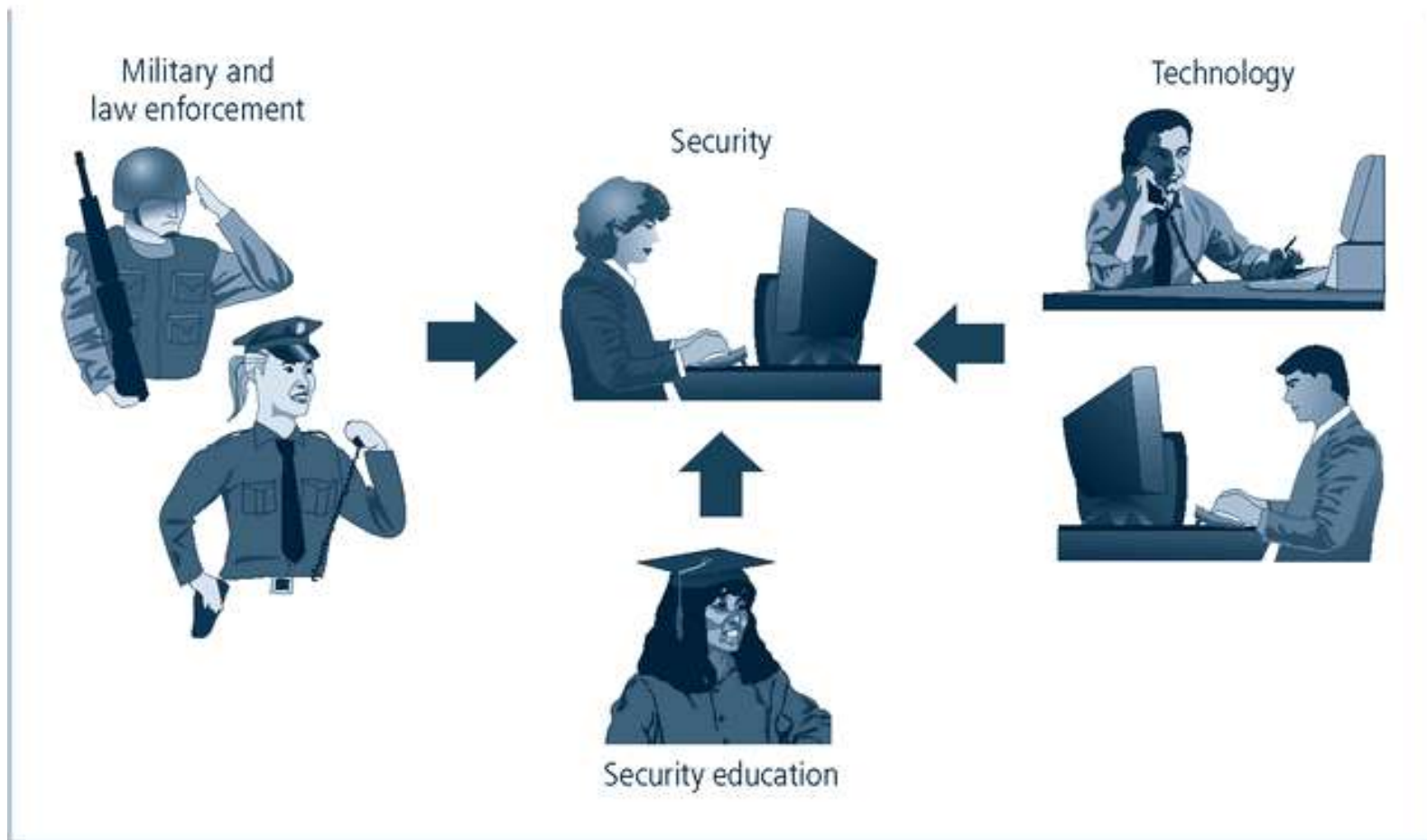


FIGURE 11-1 Career Paths to Information Security Positions

Information Security Positions

- Use of standard job descriptions can increase degree of professionalism and improve the consistency of roles and responsibilities between organizations
- Charles Cresson Wood's book *Information Security Roles and Responsibilities Made Easy* offers set of model job descriptions

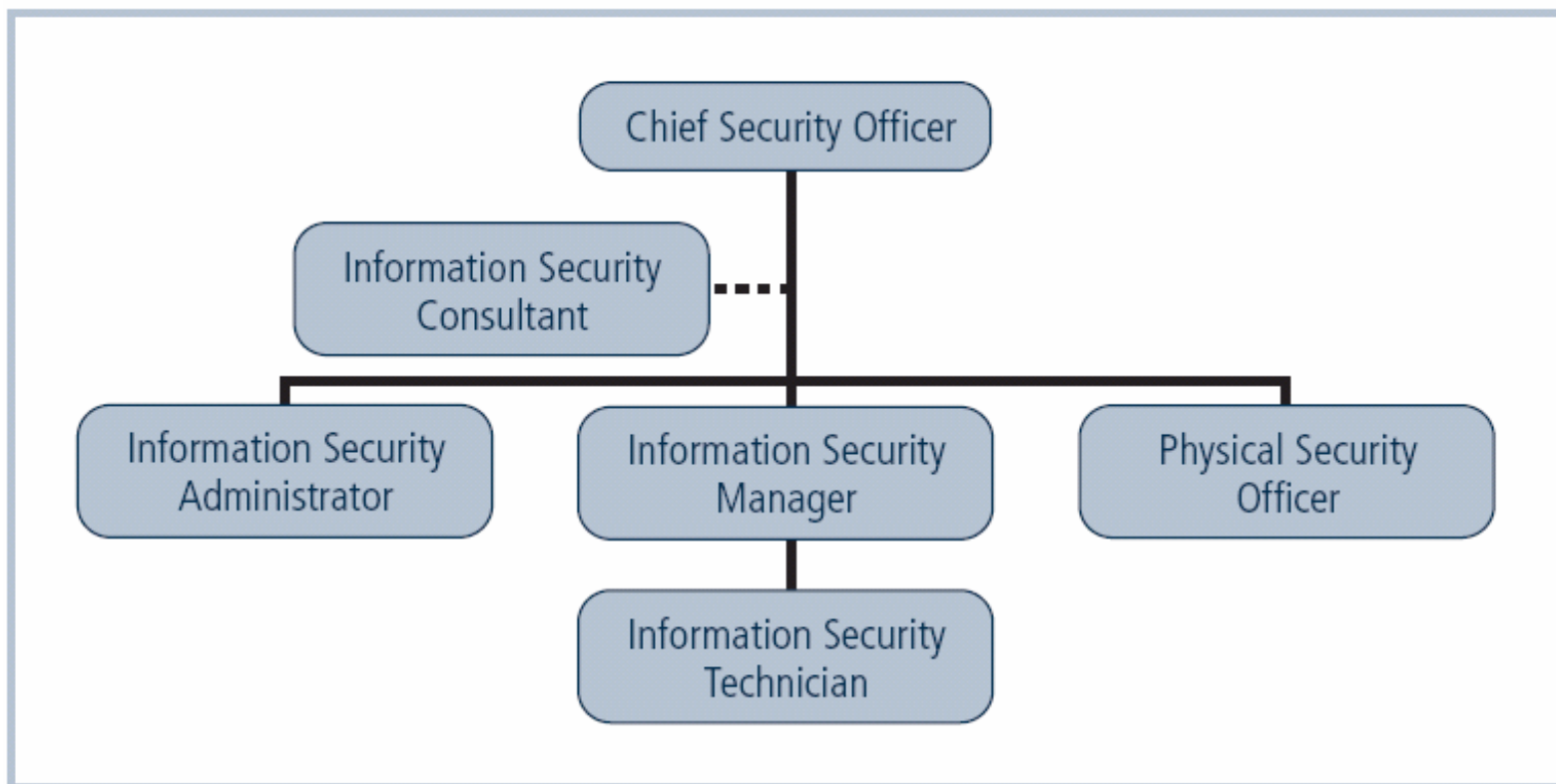


FIGURE 11-2 Positions in Information Security

Information Security Positions (continued)

- Chief Information Security Officer (CISO or CSO)
 - Top information security position; frequently reports to Chief Information Officer
 - Manages the overall information security program
 - Drafts or approves information security policies
 - Works with the CIO on strategic plans

Information Security Positions (continued)

- Chief Information Security Officer (CISO or CSO)
(continued)
 - Develops information security budgets
 - Sets priorities for information security projects and technology
 - Makes recruiting, hiring, and firing decisions or recommendations
 - Acts as spokesperson for information security team
 - Typical qualifications: accreditation; graduate degree; experience

Information Security Positions (continued)

- Security Manager
 - Accountable for day-to-day operation of information security program
 - Accomplish objectives as identified by CISO
 - Typical qualifications: not uncommon to have accreditation; ability to draft middle and lower level policies, standards and guidelines; budgeting, project management, and hiring and firing; manage technicians

Security Technician

- Technically qualified individuals tasked to configure security hardware and software
- Tend to be specialized
- Typical qualifications:
 - Varied; organizations prefer expert, certified, proficient technician
 - Some experience with a particular hardware and software package
 - Actual experience in using a technology usually

Credentials of Information Security Professionals

- Many organizations seek recognizable certifications
- Most existing certifications are relatively new and not fully understood by hiring organizations
- Certifications include: CISSP and SSCP; CISA and CISM; GIAC; SCP; TICSA; Security+; Certified Information Forensics Investigator

Cost of Being Certified

- Better certifications can be very expensive
- Even experienced professionals find it difficult to take an exam without some preparation
- Many candidates teach themselves through trade press books; others prefer structure of formal training
- Before attempting a certification exam, do all homework and review exam criteria, its purpose, and requirements in order to ensure that the time

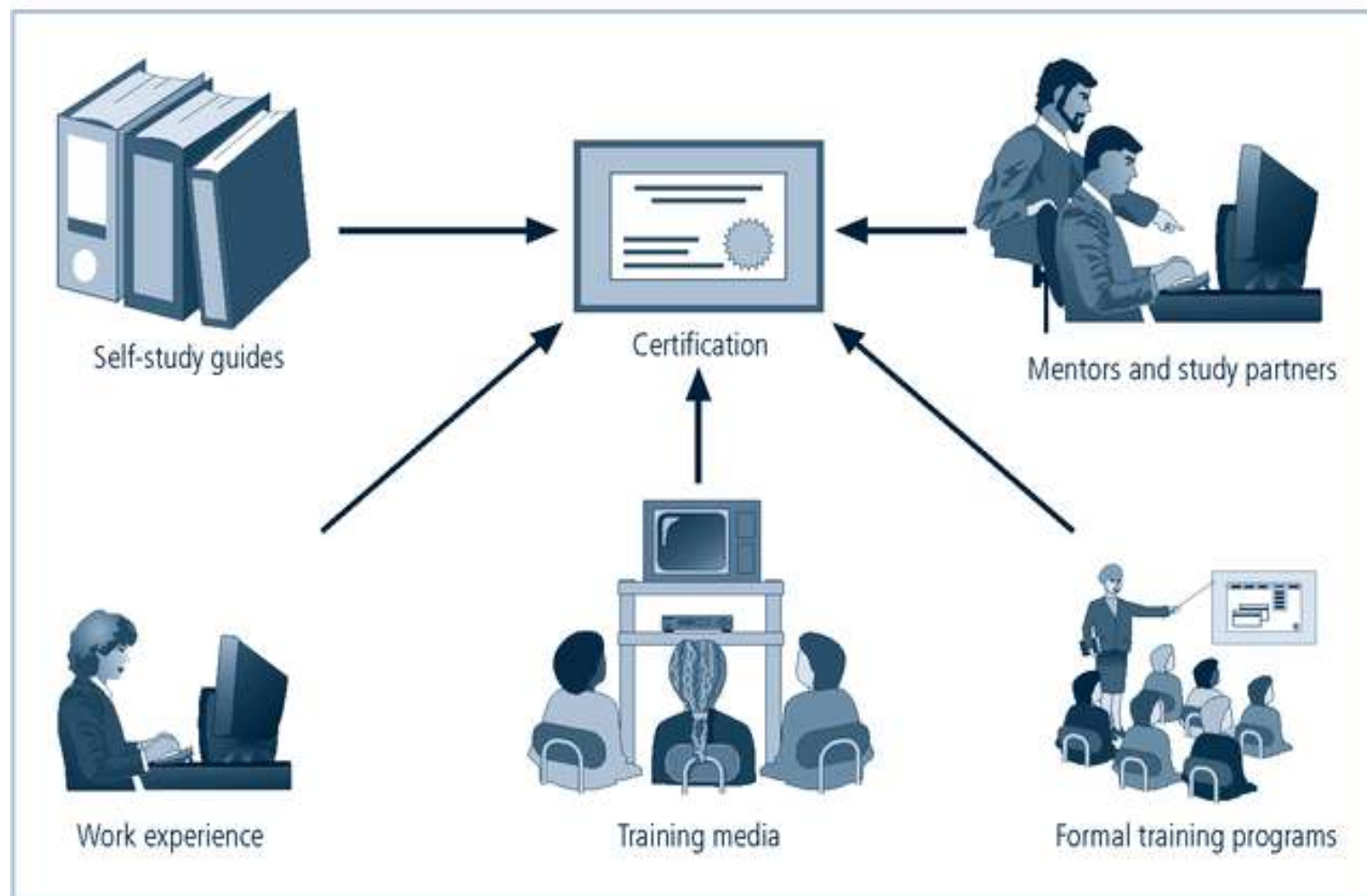


FIGURE 11-3 Preparing for Security Certification

Advice for Information Security Professionals

- Always remember: business before technology
- Technology provides elegant solutions for some problems, but adds to difficulties for others
- Never lose sight of goal: protection
- Be heard and not seen
- Know more than you say; be more skillful than you let on
- Speak to users, not at them

Employment Policies and Practices

- Management community of interest should integrate solid information security concepts into organization's employment policies and practices
- Organization should make information security a documented part of every employee's job description

Employment Policies and Practices (continued)

- From information security perspective, hiring of employees is a responsibility laden with potential security pitfalls
- CISO and information security manager should provide human resources with information security input to personnel hiring guidelines



FIGURE 11-4 Hiring Issues

Job Descriptions

- Integrating information security perspectives into hiring process begins with reviewing and updating all job descriptions
- Organization should avoid revealing access privileges to prospective employees when advertising open positions

Interviews

- An opening within the information security department creates unique opportunity for the security manager to educate HR on certifications, experience, and qualifications of a good candidate
- Information security should advise HR to limit information provided to the candidate on the responsibilities and access rights the new hire would have
- For organizations that include on-site visits as part of interviews, important to use caution when

Background Checks

- Investigation into a candidate's past
- Should be conducted before organization extends offer to candidate
- Background checks differ in level of detail and depth with which candidate is examined
- May include identity check, education and credential check, previous employment verification, references check, drug history, credit history, and

Employment Contracts

- Once a candidate has accepted the job offer, employment contract becomes important security instrument
- Many security policies require an employee to agree in writing
- New employees may find policies classified as “employment contingent upon agreement,” whereby employee is not offered the position unless binding organizational policies are agreed

New Hire Orientation

- New employees should receive extensive information security briefing on policies, procedures and requirements for information security
- Levels of authorized access are outlined; training provided on secure use of information systems
- By the time employees start, they should be thoroughly briefed and ready to perform duties securely

On-the-Job Security Training

- Organization should conduct periodic security awareness training
- Keeping security at the forefront of employees' minds and minimizing employee mistakes is important part of information security awareness mission
- External and internal seminars also increase level of security awareness for all employees, particularly security employees

Performance Evaluation

- Organizations should incorporate information security components into employee performance evaluations
- Employees pay close attention to job performance evaluations; if evaluations include information security tasks, employees are more motivated to perform these tasks at a satisfactory level

Termination

- When employee leaves organization, there are a number of security-related issues
- Key is protection of all information to which employee had access
- Once cleared, the former employee should be escorted from premises
- Many organizations use an exit interview to remind former employee of contractual obligations and to obtain feedback

Termination (continued)

- Hostile departures include termination for cause, permanent downsizing, temporary lay-off, or some instances of quitting
 - Before employee is aware, all logical and keycard access is terminated
 - Employee collects all belongings and surrenders all keys, keycards, and other company property
 - Employee is then escorted out of the building

Termination (continued)

- Friendly departures include resignation, retirement, promotion, or relocation
 - Employee may be notified well in advance of departure date
 - More difficult for security to maintain positive control over employee's access and information usage
 - Employee access usually continues with new expiration date

Termination (continued)

- Offices and information used by the employee must be inventoried; files stored or destroyed; and property returned to organizational stores
- Possible that employees foresee departure well in advance and begin collecting organizational information for their future employment
- Only by scrutinizing systems logs after employee has departed can organization determine if there has been a breach of policy or a loss of information
- If information has been copied or stolen, action should be declared an incident and the appropriate

Security Considerations For Nonemployees

- Individuals not subject to screening, contractual obligations, and eventual secured termination often have access to sensitive organizational information
- Relationships with these individuals should be carefully managed to prevent possible information leak or theft

Temporary Employees

- Hired by organization to serve in temporary position or to supplement existing workforce
- Often not subject to contractual obligations or general policies; if temporary employees breach a policy or cause a problem, possible actions are limited
- Access to information for temporary employees should be limited to that necessary to perform duties

Contract Employees

- Typically hired to perform specific services for organization
- Host company often makes contract with parent organization rather than with individual for a particular task
- In secure facility, all contract employees escorted from room to room, as well as into and out of facility

Consultants

- Should be handled like contract employees, with special requirements for information or facility access integrated into contract
- Security and technology consultants must be prescreened, escorted, and subjected to non-disclosure agreements to protect organization.
- Just because security consultant is paid doesn't make the protection of organization's information the consultant's number one priority

Business Partners

- Businesses find themselves in strategic alliances with other organizations, desiring to exchange information or integrate systems
- There must be meticulous, deliberate process of determining what information is to be exchanged, in what format, and to whom
- Non-disclosure agreements and the level of security of both systems must be examined before any physical integration takes place

Separation of Duties and Collusion

- Cornerstone in protection of information assets and against financial loss
- Separation of duties: control used to reduce chance of individual violating information security; stipulates that completion of significant task requires at least two people
- Collusion: unscrupulous workers conspiring to commit unauthorized task
- Two-man control: two individuals review and approve each other's work before the task is

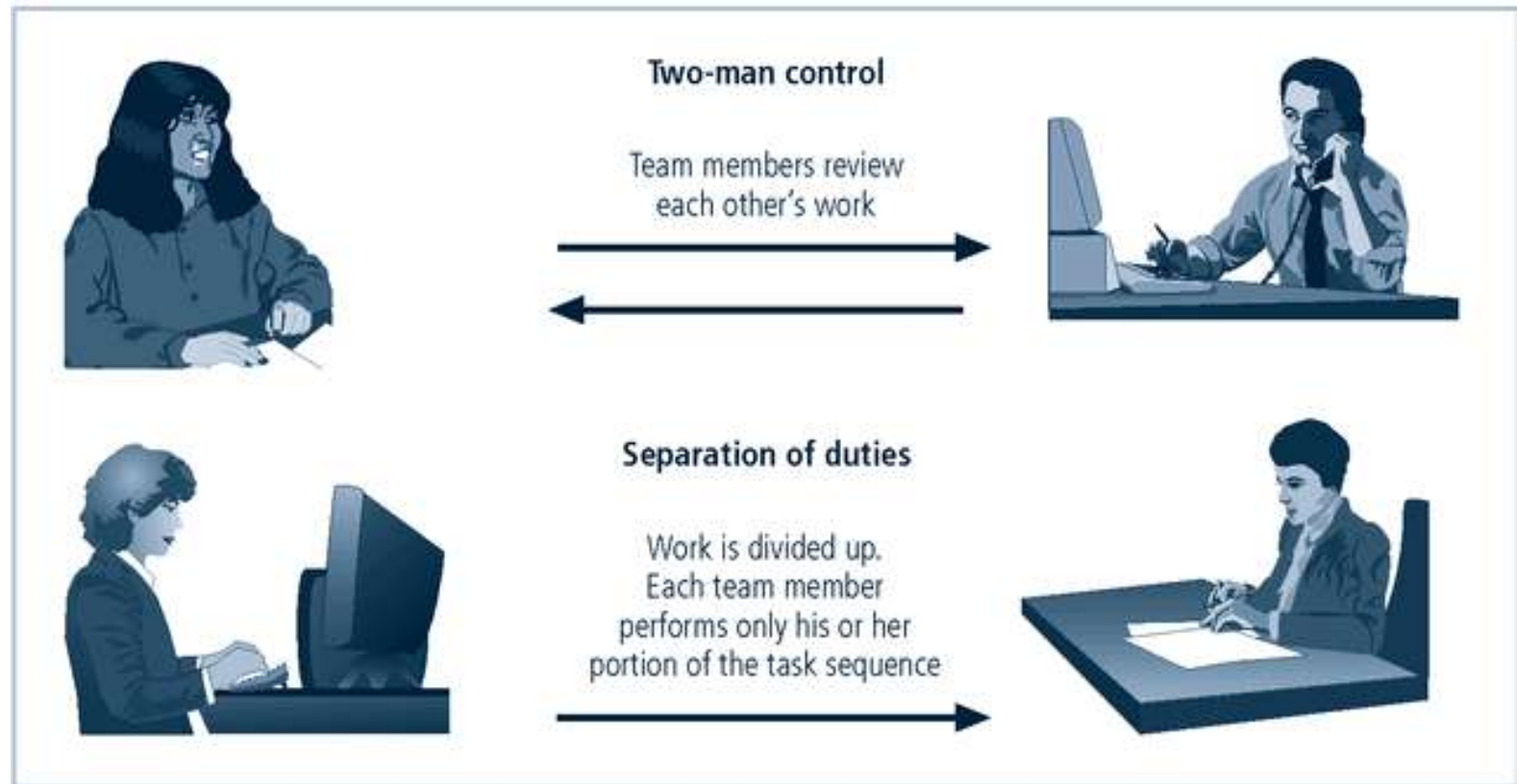


FIGURE 11-6 Preventing Collusion

Privacy and the Security of Personnel Data

- Organizations required by law to protect sensitive or personal employee information
- Includes employee addresses, phone numbers, social security numbers, medical conditions, and family names and addresses
- This responsibility also extends to customers, patients, and business relationships

Summary

- Positioning the information security function within organizations
- Issues and concerns about staffing information security
- Professional credentials of information security professionals
- Organizational employment policies and practices related to successful information security

Summary

- Special security precautions for nonemployees
- Separation of duties
- Special requirements needed for the privacy of personnel data

Information Security Maintenance

The only thing we can predict with certainty
is change.

JAYNE SPAIN, DEPARTMENT OF CHILDREN AND
FAMILY LEARNING, STATE OF MINNESOTA

PRINCIPLES of
INFORMATION
SECURITY
Second Edition

Learning Objectives

Upon completion of this material, you should be able to:

- Understand why maintenance of the information security program is needed on an ongoing basis
- Recognize recommended security management models
- Define a model for a full maintenance program
- Identify the key factors involved in monitoring the external and internal environment

Learning Objectives (continued)

- Understand how planning and risk assessment tie into information security maintenance
- Understand how vulnerability assessment and remediation tie into information security maintenance
- Understand how to build readiness and review procedures into information security maintenance

Introduction

- Organization should avoid overconfidence after implementation of improved information security profile
- Organizational changes that may occur include: new assets acquired; new vulnerabilities emerge; business priorities shift; partnerships form or dissolve; organizational divestiture and acquisition; employee hire and turnover
- If program does not adjust, may be necessary to begin cycle again

Security Management Models

- Management model must be adopted to manage and operate ongoing security program
- Models are frameworks that structure tasks of managing particular set of activities or business functions

The ISO Network Management Model

- Five-layer approach that provides structure to administration and management of networks and systems
- Addresses management and operation thorough five areas: fault management; configuration and name management; accounting management; performance management; and security management

The ISO Network Management Model (continued)

- Five areas of ISO model transformed into five areas of security management:
 - Fault management
 - Configuration and change management
 - Accounting and auditing management
 - Performance management
 - Security program management

Fault Management

- Identifying, tracking, diagnosing, and resolving faults in system
- Vulnerability assessment most often accomplished with penetration testing (simulated attacks exploiting documented vulnerabilities)
- Another aspect is monitoring and resolution of user complaints
- Help desk personnel must be trained to recognize security problem as distinct from other system

Configuration and Change Management

- Configuration management: administration of the configuration of security program components
- Change management: administration of changes in strategy, operation, or components
- Each involve non-technical as well as technical changes:
 - Non-technical changes impact procedures and people
 - Technical changes impact the technology implemented to support security efforts in the hardware, software,

Nontechnical Change Management

- Changes to information security may require implementing new policies and procedures
- Document manager should maintain master copy of each document; record and archive revisions made; and keep copies of revisions
- Policy revisions not implemented and enforceable until they have been disseminated, read, understood, and agreed to
- Software available to make creation, modification, dissemination, and agreement documentation

Technical Configuration and Change Management

- Terms associated with management of technical configuration and change: configuration item; version; build
- Four steps associated with configuration management
 - Configuration identification
 - Configuration control
 - Configuration status accounting
 - Configuration audit

Accounting and Auditing Management

- Chargeback accounting enables organizations to internally charge for system use
- Some resource usage is commonly tracked
- Accounting management involves monitoring use of particular component of a system
- Auditing is process of reviewing use of a system, not to check performance, but to determine misuse or malfeasance; automated tools can

Performance Management

- Important to monitor performance of security systems and underlying IT infrastructure to determine if they are working effectively
- Common metrics are applicable in security, especially when components being managed are associated with network traffic
- To evaluate ongoing performance of security system, performance baselines are established

Security Program Management

- ISO five-area-based framework supports a structured management model by ensuring various areas are addressed
- Two standards are designed to assist in this effort
- Part 2 of the British Standard (BS) 7799 introduces process model: plan; do; check; act

The Maintenance Model

- Designed to focus organizational effort on maintaining systems
- Recommended maintenance model based on five subject areas
 - External monitoring
 - Internal monitoring
 - Planning and risk assessment
 - Vulnerability assessment and remediation
 - Readiness and review

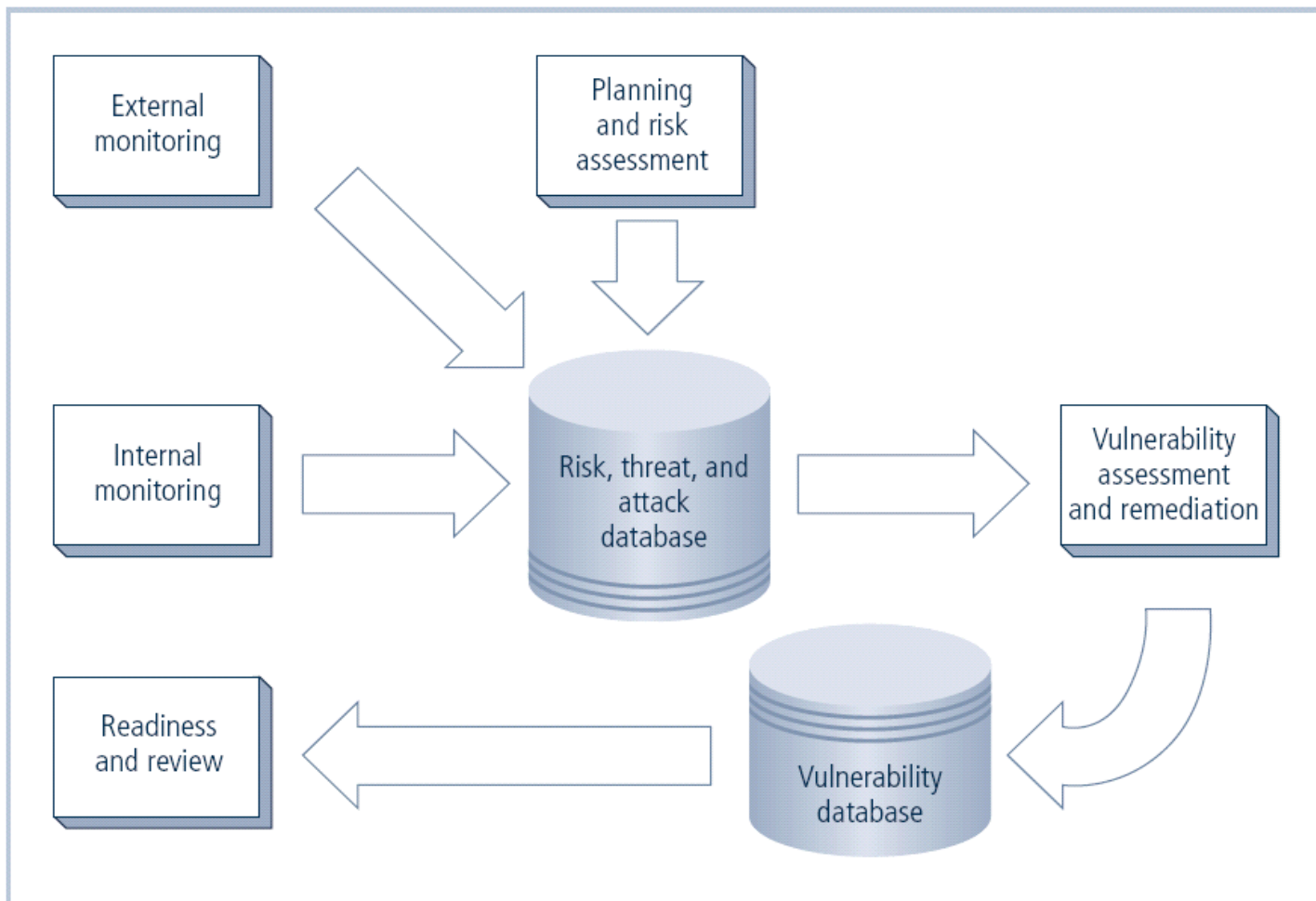


FIGURE 12-1 The Maintenance Model

Monitoring the External Environment

- Objective to provide early awareness of new threats, threat agents, vulnerabilities, and attacks that is needed to mount an effective defense
- Entails collecting intelligence from data sources and giving that intelligence context and meaning for use by organizational decision makers

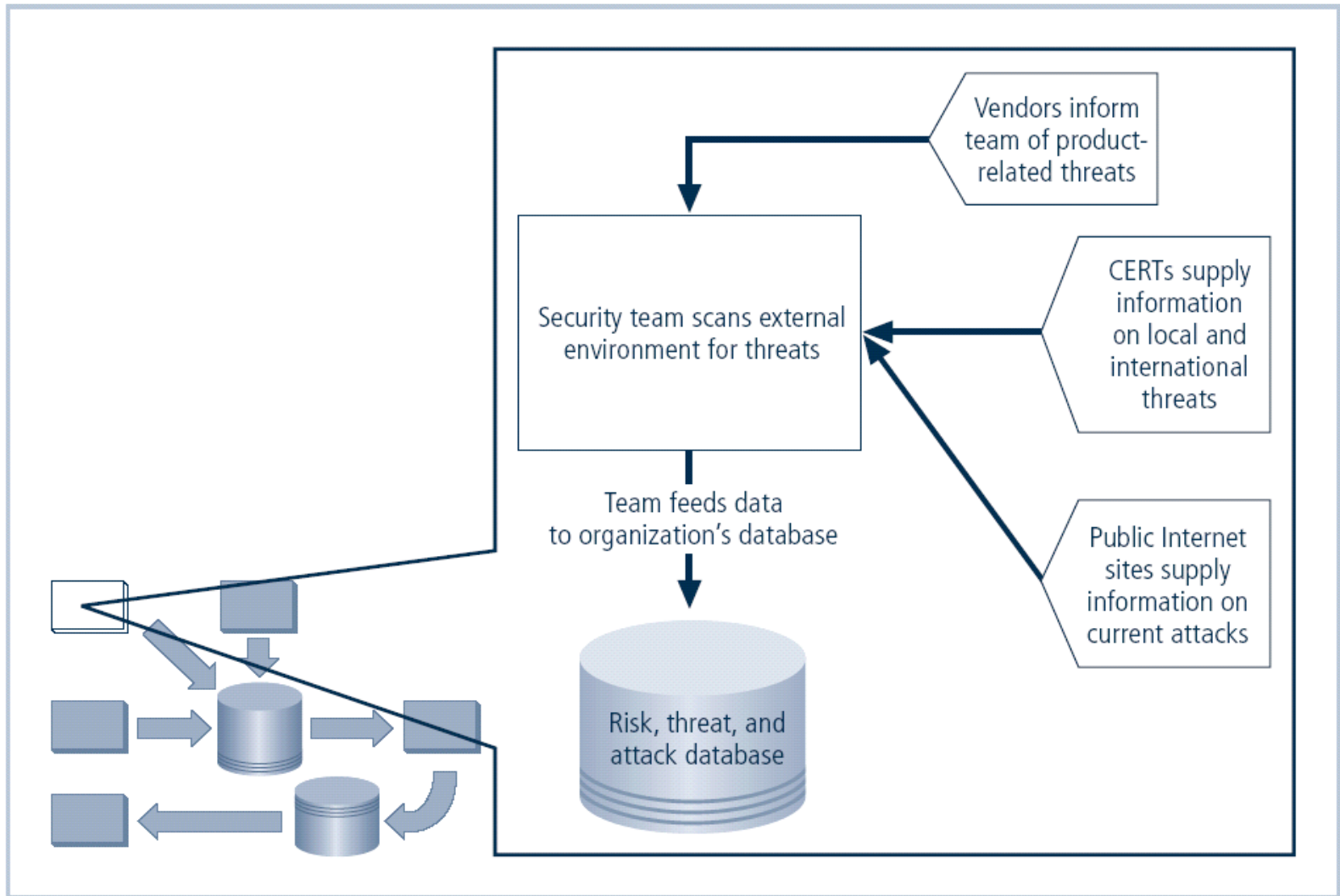


FIGURE 12-2 External Monitoring

Data Sources

- Acquiring threat and vulnerability data is not difficult
- Turning data into information decision makers can use is the challenge
- External intelligence comes from three classes of sources: vendors; computer emergency response teams (CERTs); public network sources
- Regardless of where or how external monitoring data is collected, must be analyzed in context of organization's security environment to be useful

Monitoring, Escalation, and Incident Response

- Function of external monitoring process is to monitor activity, report results, and escalate warnings
- Monitoring process has three primary deliverables
 - Specific warning bulletins issued when developing threats and specific attacks pose measurable risk to organization
 - Periodic summaries of external information

Data Collection and Management

- Over time, external monitoring processes should capture knowledge about external environment in appropriate formats
- External monitoring collects raw intelligence, filters for relevance, assigns a relative risk impact, and communicates to decision makers in time to make a difference

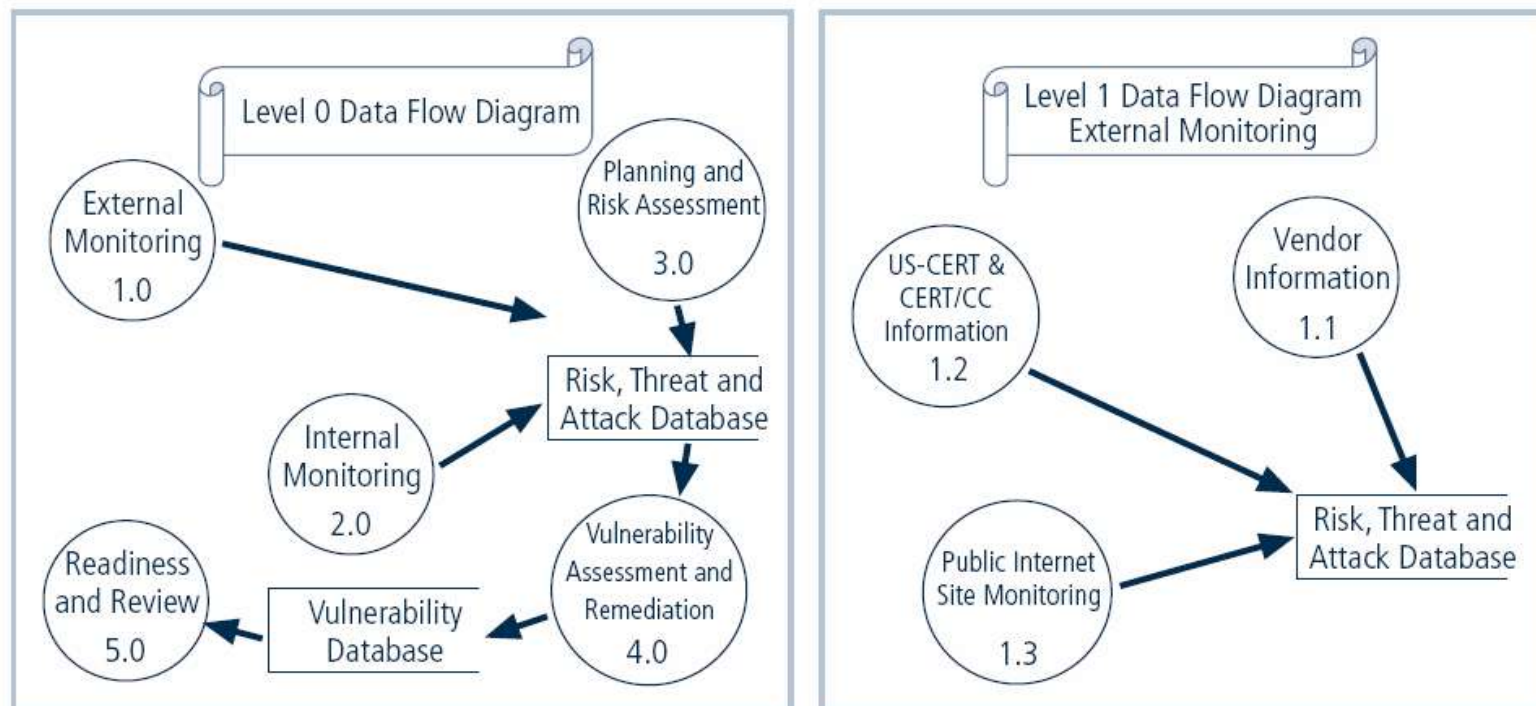


FIGURE 12-3 Data Flow Diagrams for External Data Collection

Monitoring the Internal Environment

- Maintain informed awareness of state of organization's networks, systems, and defenses by maintaining inventory of IT infrastructure and applications
- Internal monitoring accomplished by:
 - Active participation in, or leadership of, IT governance process
 - Real-time monitoring of IT activity using intrusion detection systems
 - Automated difference detection methods that identify variances introduced to network or system hardware

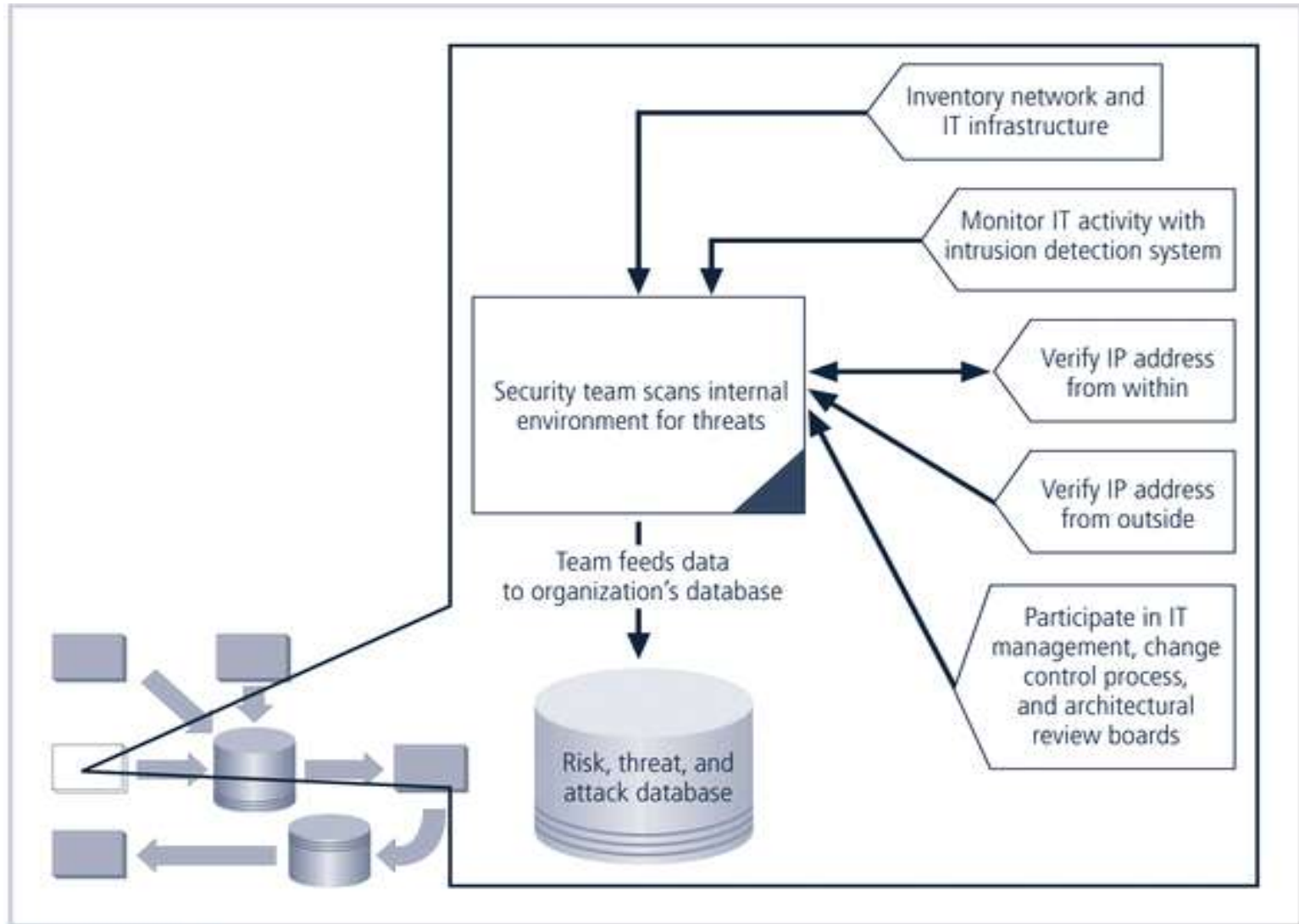


FIGURE 12-4 Internal monitoring

Network Characterization and Inventory

- Organizations should have carefully planned and fully populated inventory for network devices, communication channels, and computing devices
- Once characteristics identified, they must be carefully organized and stored using a mechanism (manual or automated) that allows timely retrieval and rapid integration of disparate facts

The Role of IT Governance

- Primary value is increased awareness of the impact of change
- Awareness must be translated into description of risk that is caused by change through operational risk assessment
- Awareness of change based on two primary activities within IT governance process
 - Architecture review boards

Making Intrusion Detection Systems Work

- The most important value of raw intelligence provided by intrusion detection systems (IDS) is providing indicators of current or imminent vulnerabilities
- Log files from IDS engines can be mined for information
- Another IDS monitoring element is traffic analysis

Detecting Differences

- Difference analysis: procedure that compares current state of network segment against known previous state of same segment
- Differences between the current state and the baseline state that are unexpected could be a sign of trouble and need investigation

Planning and Risk Assessment

- Primary objective to keep lookout over entire information security program
- Accomplished by identifying and planning ongoing information security activities that further reduce risk

Planning and Risk Assessment (continued)

- Primary objectives
 - Establishing a formal information security program review
 - Instituting formal project identification, selection, planning and management processes
 - Coordinating with IT project teams to introduce risk assessment and review for all IT projects
 - Integrating a mindset of risk assessment across

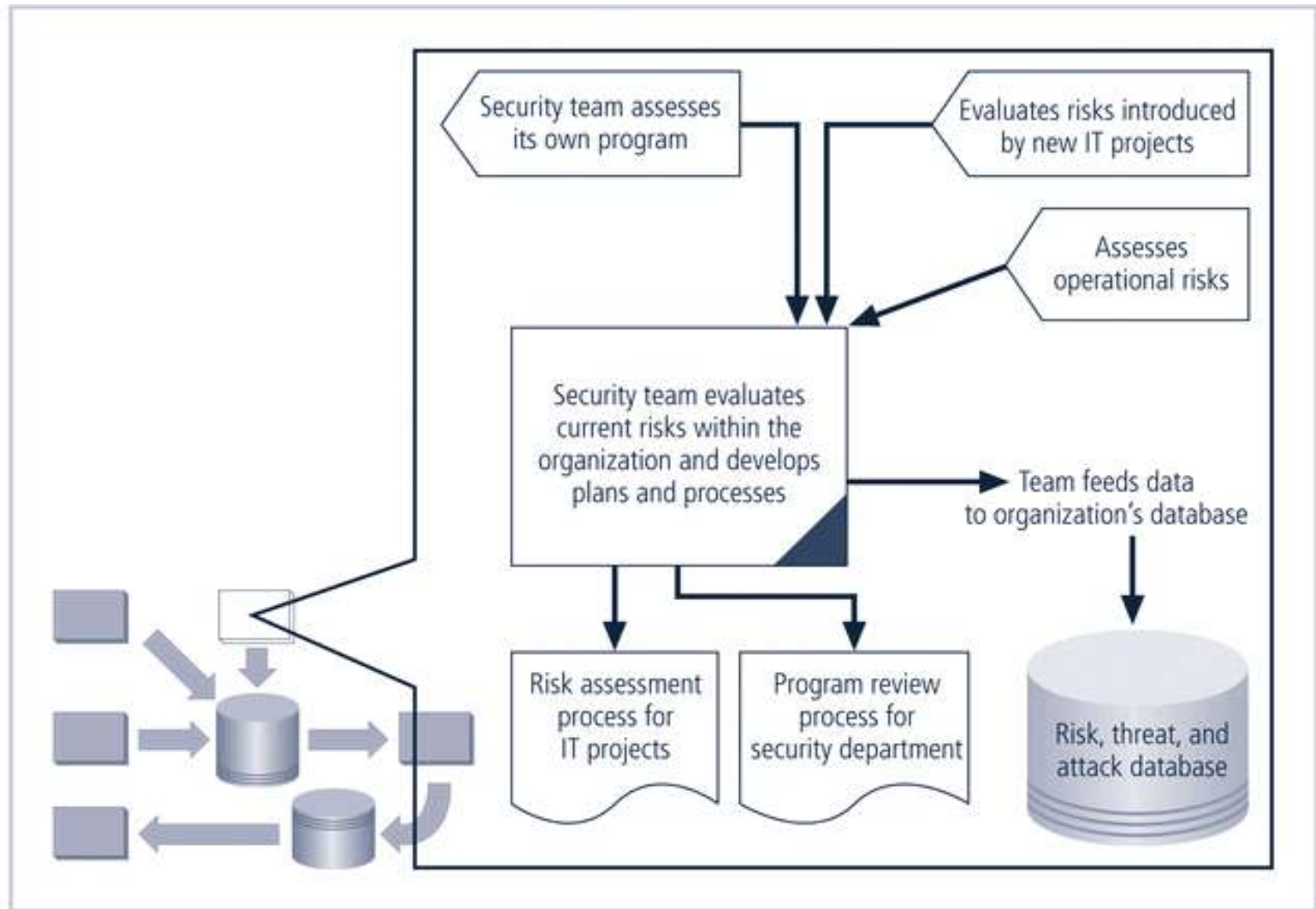


FIGURE 12-5 Planning and risk assessments

Information Security Program Planning and Review

- Periodic review of ongoing information security program coupled with planning for enhancements and extensions is recommended
- Should examine IT needs of future organization and impact those needs have on information security
- A recommended approach takes advantage of the fact most organizations have annual capital budget planning cycles and manage security

Information Security Program Planning and Review (continued)

- Large projects should be broken into smaller projects for several reasons
 - Smaller projects tend to have more manageable impacts on networks and users
 - Larger projects tend to complicate change control process in implementation phase
 - Shorter planning, development, and implementation schedules reduce uncertainty
 - Most large projects can easily be broken down into smaller projects, giving more opportunities to change direction and gain flexibility

Security Risk Assessments

- A key component for driving security program change is information security operational risk assessment (RA)
- RA identifies and documents risk that project, process, or action introduces to organization and offers suggestions for controls
- Information security group coordinates preparation of many types of RA documents

Vulnerability Assessment and Remediation

- Primary goal is identification of specific, documented vulnerabilities and their timely remediation
- Accomplished by:
 - Using vulnerability assessment procedures
 - Documenting background information and providing tested remediation procedures for reported vulnerabilities
 - Tracking vulnerabilities from when they are identified

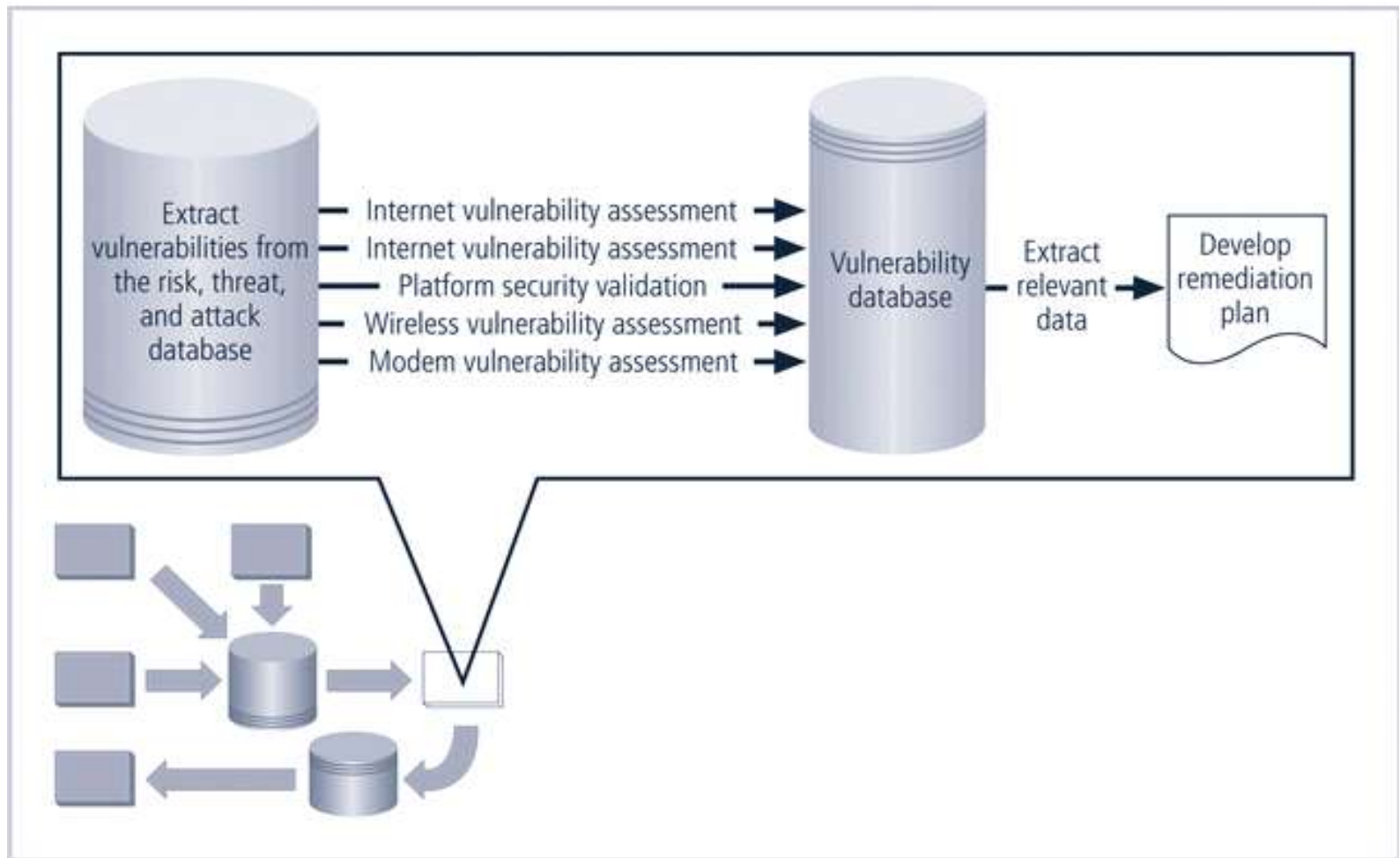


FIGURE 12-6 Vulnerability Assessment and Remediation

Vulnerability Assessment

- Process of identifying and documenting specific and provable flaws in organization's information asset environment
- Five vulnerability assessment processes that follow can serve many organizations as they attempt to balance intrusiveness of vulnerability assessment with need for stable and productive production environment

Internet Vulnerability Assessment

- Designed to find and document vulnerabilities present in organization's public-facing network
- Steps in the process include:
 - Planning, scheduling and notification
 - Target selection
 - Test selection
 - Scanning
 - Analysis
 - Record keeping

Intranet Vulnerability Assessment

- Designed to find and document selected vulnerabilities present on the internal network
- Attackers often internal members of organization, affiliates of business partners, or automated attack vectors (such as viruses and worms)
- This assessment is usually performed against selected critical internal devices with a known, high value by using selective penetration testing
- Steps in process almost identical to steps in Internet vulnerability assessment

Platform Security Validation

- Designed to find and document vulnerabilities that may be present because of misconfigured systems in use within organization
- These misconfigured systems fail to comply with company policy or standards
- Fortunately, automated measurement systems are available to help with the intensive process of validating compliance of platform configuration with

Wireless Vulnerability Assessment

- Designed to find and document vulnerabilities that may be present in wireless local area networks of organization
- Since attackers from this direction are likely to take advantage of any loophole or flaw, assessment is usually performed against all publicly accessible areas using every possible wireless penetration testing approach

Modem Vulnerability Assessment

- Designed to find and document any vulnerability present on dial-up modems connected to organization's networks
- Since attackers from this direction take advantage of any loophole or flaw, assessment usually performed against all telephone numbers owned by the organization
- One elements of this process, often called war

Documenting Vulnerabilities

- Vulnerability tracking database should provide details as well as a link to the information assets
- Low-cost and ease of use makes relational databases a realistic choice
- Vulnerability database is an essential part of effective remediation

Remediating Vulnerabilities

- Objective is to repair flaw causing a vulnerability instance or remove risk associated with vulnerability
- As last resort, informed decision makers with proper authority can accept risk
- Important to recognize that building relationships with those who control information assets is key to success
- Success depends on organization adopting team

Acceptance or Transference of Risk

- In some instances, risk must simply be acknowledged as part of organization's business process
- Management must be assured that decisions made to assume risk the organization are made by properly informed decision makers
- Information security must make sure the right people make risk assumption decisions with complete knowledge of the impact of the decision

Threat Removal

- In some circumstances, threats can be removed without repairing vulnerability
- Vulnerability can no longer be exploited, and risk has been removed
- Other vulnerabilities may be amenable to other controls that do not allow an expensive repair and still remove risk from situation

Vulnerability Repair

- Optimum solution in most cases is to repair vulnerability
- Applying patch software or implementing a workaround often accomplishes this
- In some cases, simply disabling the service removes vulnerability; in other cases, simple remedies are possible

Readiness and Review

- Primary goal to keep information security program functioning as designed and continuously improving
- Accomplished by:
 - Policy review
 - Program review
 - Rehearsals

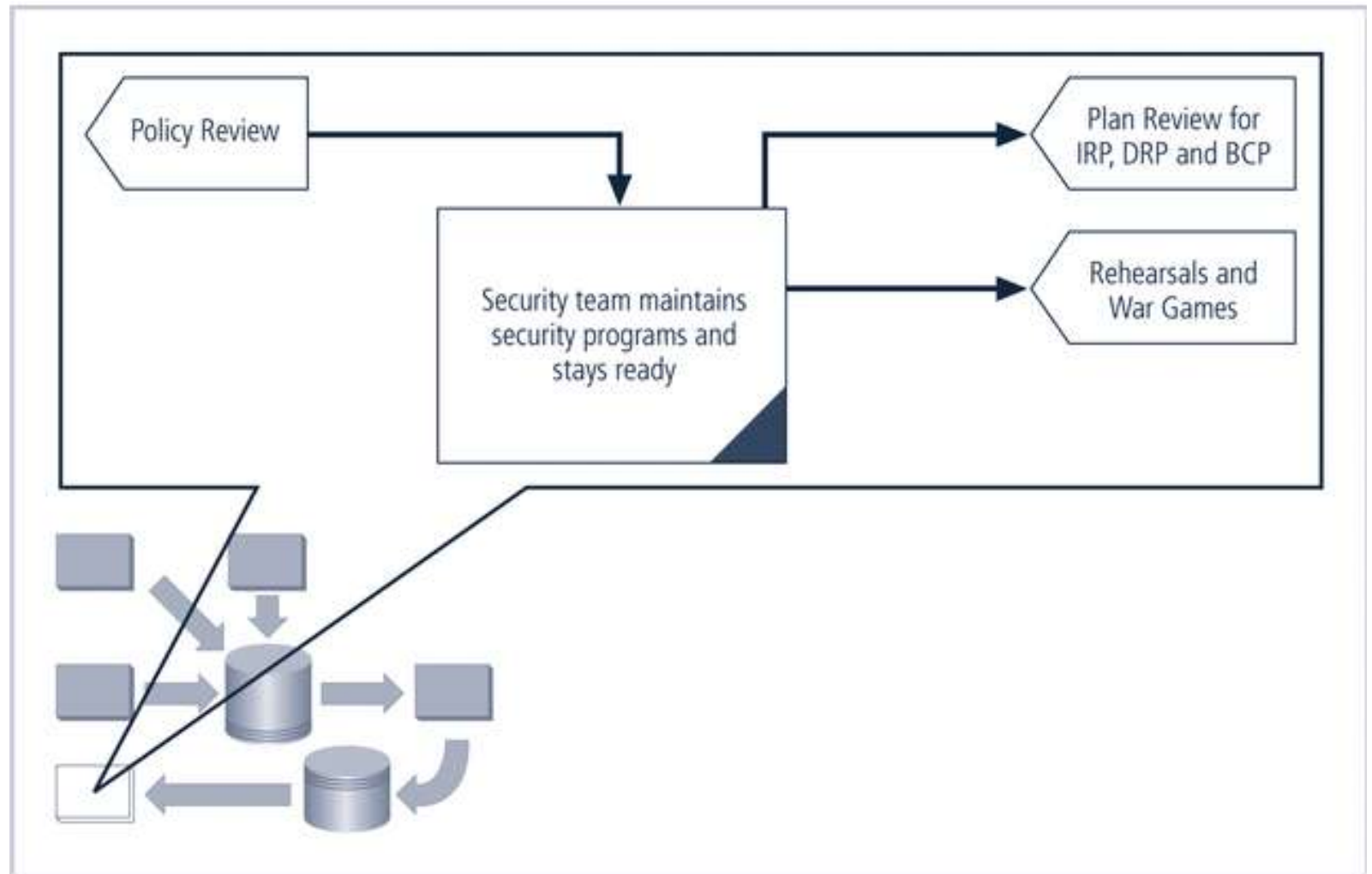


FIGURE 12-7 Readiness and review

Summary

- Maintenance of information security program is essential
- Security management models assist in planning for ongoing operations
- It is necessary to monitor external and internal environment

Summary

- Planning and risk assessment essential parts of information security maintenance
- Need to understand how vulnerability assessment and remediation tie into information security maintenance
- Need to understand how to build readiness and review procedures into information security maintenance