

Principles of Information Security, Fifth Edition

Chapter 2 *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 material, you should be able to:
 - Discuss the organizational business need for information security
 - Explain why a successful information security program is the shared responsibility of an organization's general management and IT management
 - List and describe the threats posed to information security and common attacks associated with those threats
 - Describe the relationship between threats and attacks against information within systems

Introduction

- The primary mission of an information security program is to ensure information assets—information and the systems that house them—remain safe and useful.
- If no threats existed, resources could be used exclusively to improve systems that contain, use, and transmit information.
- Threat of attacks on information systems is a constant concern.

Business Needs First

- Information security performs four important functions for an organization:
 - Protecting the organization's ability to function
 - Protecting the data and information the organization collects and uses
 - Enabling the safe operation of applications running on the organization's IT systems
 - Safeguarding the organization's technology assets

Protecting the Functionality of an Organization

- Management (general and IT) is responsible for facilitating security program.
- Implementing information security has more to do with management than technology.
- Communities of interest should address information security in terms of business impact and cost of business interruption.

Protecting Data That Organizations Collect and Use

- Without data, an organization loses its record of transactions and ability to deliver value to customers.
- Protecting data in transmission, in processing, and at rest (storage) is a critical aspect of information security.

Enabling the Safe Operation of Applications

- Organization needs environments that safeguard applications using IT systems.
- Management must continue to oversee infrastructure once in place—not relegate to IT department.

Safeguarding Technology Assets in Organizations

- Organizations must employ secure infrastructure hardware appropriate to the size and scope of the enterprise.
- Additional security services may be needed as the organization grows.
- More robust solutions should replace security programs the organization has outgrown.

Threats

- Threat: a potential risk to an asset's loss of value
- Management must be informed about the various threats to an organization's people, applications, data, and information systems.
- Overall security is improving, so is the number of potential hackers.
- The 2010–2011 CSI/FBI survey found
 - 67.1 percent of organizations had malware infections.
 - 11 percent indicated system penetration by an outsider.

Type of attack or misuse	2010/11	2008	2006	2004	2002	2000
Malware infection (revised after 2008)	67%	50%	65%	78%	85%	85%
Being fraudulently represented as sender of phishing message	39%	31%	(new category)			
Laptop/mobile hardware theft/loss	34%	42%	47%	49%	55%	60%
Bots/zombies in organization	29%	20%	(new category)			
Insider abuse of Internet access or e-mail	25%	44%	42%	59%	78%	79%
Denial of service	17%	21%	25%	39%	40%	27%
Unauthorized access or privilege escalation by insider	13%	15%	(revised category)			
Password sniffing	11%	9%	(new category)			
System penetration by outsider	11%	(revised category)				
Exploit of client Web browser	10%	(new category)				
Attack/misuse categories with less than 10% responses (listed in decreasing order):						
Financial fraud						
Web site defacement						
Exploit of wireless network						
Other exploit of public-facing Web site						
Theft of or unauthorized access to PII or PHI due to all other causes						
Instant Messaging misuse						
Theft of or unauthorized access to IP due to all other causes						
Exploit of user's social network profile						
Theft of or unauthorized access to IP due to mobile device theft/loss						
Theft of or unauthorized access to PII or PHI due to mobile device theft/loss						
Exploit of DNS server						
Extortion or blackmail associated with threat of attack or release of stolen data						

Table 2-1 CSI Survey Results for Types of Attack or Misuse (2000–2011)⁵

© Cengage Learning 2015

Category of threat	Attack examples
Compromises to intellectual property	Piracy, copyright infringement
Deviations in quality of service	Internet service provider (ISP), power, or WAN service problems
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, floods, earthquakes, lightning
Human error or failure	Accidents, employee mistakes
Information extortion	Blackmail, information disclosure
Sabotage or vandalism	Destruction of systems or information
Software attacks	Viruses, worms, macros, denial-of-service
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of equipment or information

Table 2-2 The 12 Categories of Threats to Information Security⁷

© Cengage Learning 2015

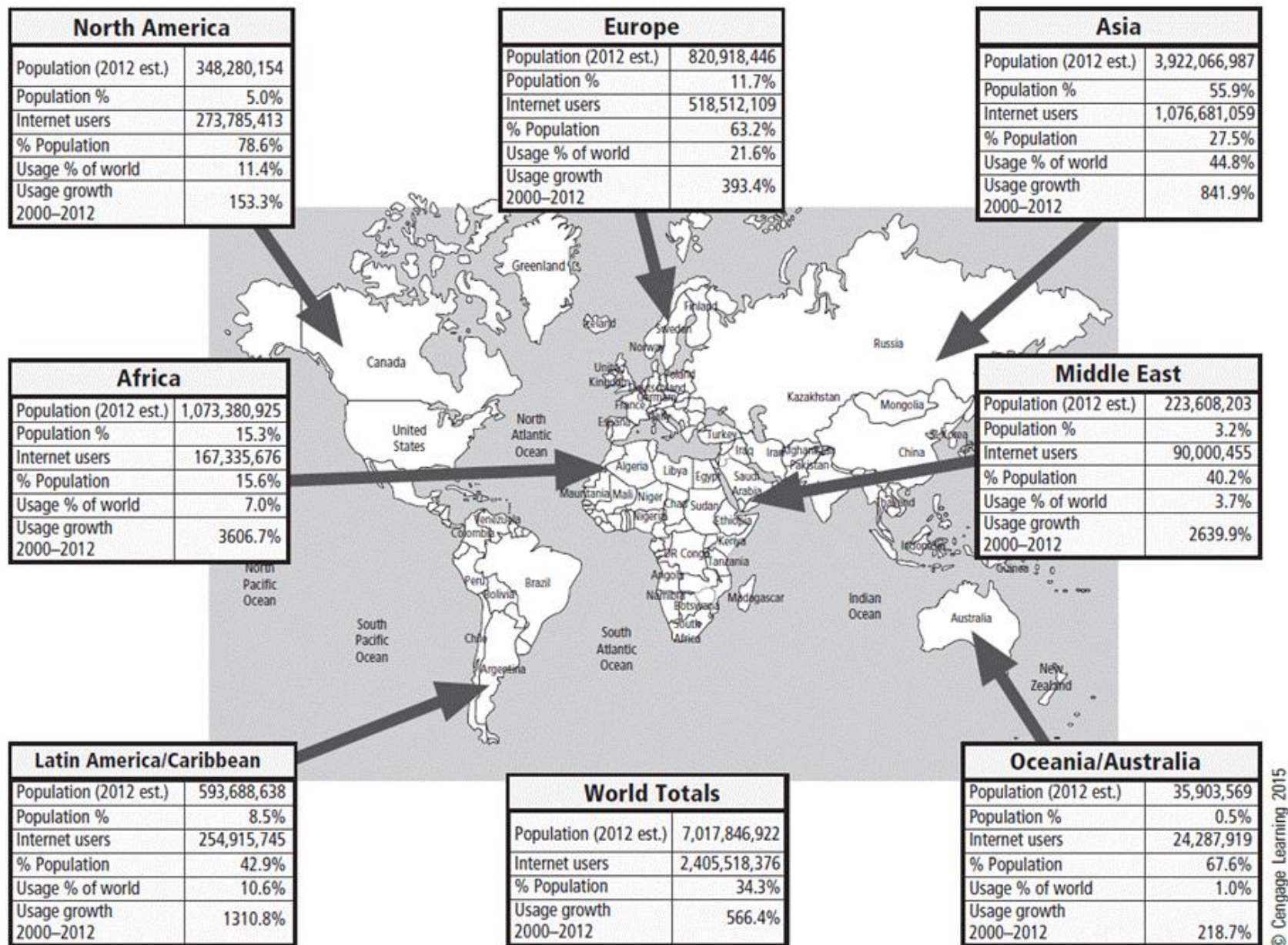


Figure 2-1 World Internet usage³

Compromises to Intellectual Property

- Intellectual property (IP): creation, ownership, and control of original ideas as well as the representation of those ideas
- The most common IP breaches involve software piracy.
- Two watchdog organizations investigate software abuse:
 - Software & Information Industry Association (SIIA)
 - Business Software Alliance (BSA)
- Enforcement of copyright law has been attempted with technical security mechanisms.

Deviations in Quality of Service

- Information system depends on the successful operation of many interdependent support systems.
- Internet service, communications, and power irregularities dramatically affect the availability of information and systems.

Deviations in Quality of Service (cont'd)

- Internet service issues
 - Internet service provider (ISP) failures can considerably undermine the availability of information.
 - Outsourced Web hosting provider assumes responsibility for all Internet services as well as for the hardware and Web site operating system software.
- Communications and other service provider issues
 - Other utility services affect organizations: telephone, water, wastewater, trash pickup.
 - Loss of these services can affect organization's ability to function.

Average Cost of Downtime According to MegaPath

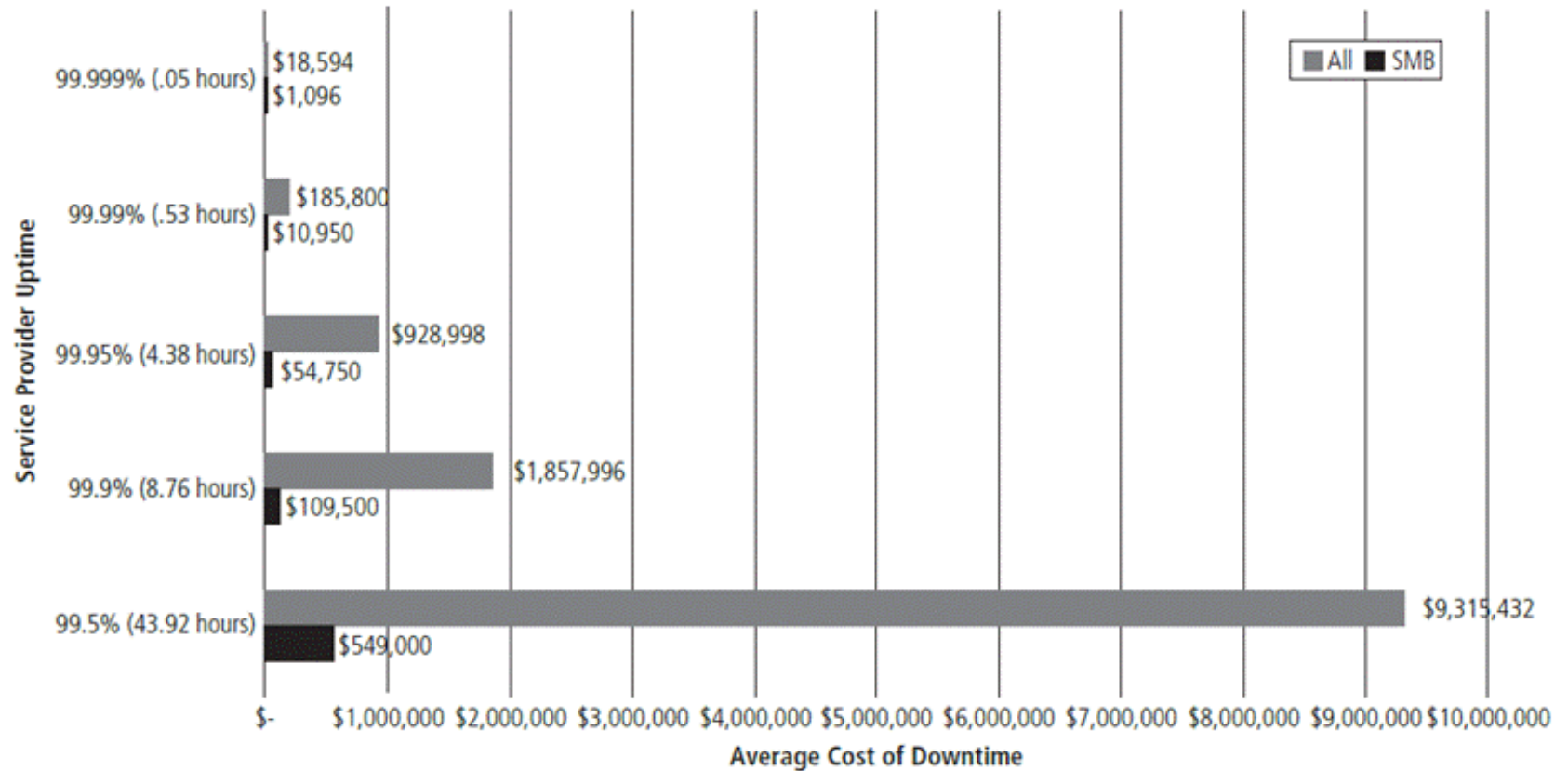


Figure 2-5 Cost of online service provider downtime¹⁰

Source: MegaPath. Used with permission.

Deviations in Quality of Service (cont'd)

- Power irregularities
 - Commonplace
 - Lead to fluctuations such as power excesses, power shortages, and power losses
 - Sensitive electronic equipment vulnerable to and easily damaged/destroyed by fluctuations
 - Controls can be applied to manage power quality.

Espionage or Trespass

- Access of protected information by unauthorized individuals
- Competitive intelligence (legal) versus industrial espionage (illegal)
- Shoulder surfing can occur anywhere a person accesses confidential information.
- Controls let trespassers know they are encroaching on organization's cyberspace.
- Hackers use skill, guile, or fraud to bypass controls protecting others' information.




© Cengage Learning 2015

Figure 2-6 Shoulder surfing

Espionage or Trespass (cont'd)

- Expert hacker
 - Develops software scripts and program exploits
 - Usually a master of many skills
 - Will often create attack software and share with others
- Unskilled hacker
 - Many more unskilled hackers than expert hackers
 - Use expertly written software to exploit a system
 - Do not usually fully understand the systems they hack

<h1>WANTED</h1> <h2>BY THE FBI</h2>			
Breaking into computer systems, Theft of confidential information, Disclosure of stolen confidential information, Hijacking victims' e-mail accounts, and Defacing Internet websites			
<h3>IMA HACKER</h3>			
			
No Photograph Available			
Aliases: "Lost" "All your PC are belong to me" "Cyber-Merlin"			
<h3>DESCRIPTION</h3>			
Date(s) of Birth Used:	unknown	Hair:	unknown
Place of Birth:	unknown	Eyes:	unknown
Height:	unknown	Sex:	unknown
Weight:	unknown	Race:	unknown
NCIC:	A1234566789	Nationality:	unknown
Occupation:	unknown		
Scars and Marks:	unknown		
Remarks:	Individual may be age 12–60, male or female, unknown background, with varying technological skill levels; may be internal or external to the organization.		
<h3>CAUTION</h3>			

© Cengage Learning 2015

Figure 2-7 Contemporary hacker profile

Espionage or Trespass (cont'd)

- Other terms for system rule breakers:
 - Cracker: “cracks” or removes software protection designed to prevent unauthorized duplication
 - Phreaker: hacks the public telephone system to make free calls or disrupt services
- Password attacks
 - Cracking
 - Brute force
 - Dictionary
 - Rainbow tables
 - Social engineering

Case-Insensitive Passwords Using a Standard Alphabet Set (No Numbers or Special Characters)		
Password length	Odds of cracking: 1 in (based on number of characters ^ password length):	Estimated time to crack*
8	208,827,064,576	1.9 seconds
9	5,429,503,678,976	50.8 seconds
10	141,167,095,653,376	22.0 minutes
11	3,670,344,486,987,780	11.1 hours
12	95,428,956,661,682,200	10.3 days
13	2,481,152,873,203,740,000	268.6 days
14	64,509,974,703,297,200,000	19.1 years
15	1,677,259,342,285,730,000,000	497.4 years
16	43,608,742,899,428,900,000,000	12,932.8 years
Case-Sensitive Passwords Using a Standard Alphabet Set with Numbers and 20 Special Characters		
Password length	Odds of cracking: 1 in (based on number of characters ^ password length):	Estimated time to crack*
8	2,044,140,858,654,980	5.2 hours
9	167,619,550,409,708,000	18.14 days
10	13,744,803,133,596,100,000	4.1 years
11	1,127,073,856,954,880,000,000	334.3 years
12	92,420,056,270,299,900,000,000	27,408.5 years
13	7,578,444,614,164,590,000,000,000	2,247,492.6 years
14	621,432,458,361,496,000,000,000,000	184,294,395.9 years
15	50,957,461,585,642,700,000,000,000,000	15,112,140,463.3 years
16	4,178,511,850,022,700,000,000,000,000,000	1,239,195,517,993.3 years

Table 2-3 Password Power

*Estimated Time to Crack is based on an average 2013-era Intel i7 PC (3770K) chip performing 109,924 Dhrystone MIPS (million instructions per second) at 3.9 GHz.

Forces of Nature

- Forces of nature can present some of the most dangerous threats.
- They disrupt not only individual lives, but also storage, transmission, and use of information.
- Organizations must implement controls to limit damage and prepare contingency plans for continued operations.

Human Error or Failure

- Includes acts performed without malicious intent or in ignorance
- Causes include:
 - Inexperience
 - Improper training
 - Incorrect assumptions
- Employees are among the greatest threats to an organization's data.



Tommy Twostory,
convicted burglar



Elite Skillz,
wannabe hacker



Harriett Allthumbs,
confused the copier with the shredder
when preparing the annual sales report

Figure 2-9 The biggest threat—acts of human error or failure

Source: © iStockphoto/BartCo, © iStockphoto/sdominick, © iStockphoto/mikkelwilliam.

Human Error or Failure (cont'd)

- Employee mistakes can easily lead to:
 - Revelation of classified data
 - Entry of erroneous data
 - Accidental data deletion or modification
 - Data storage in unprotected areas
 - Failure to protect information
- Many of these threats can be prevented with training, ongoing awareness activities, and controls.
- Social engineering uses social skills to convince people to reveal access credentials or other valuable information to an attacker.

Social Engineering

- “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.”—Kevin Mitnick
- Advance-fee fraud: indicates recipient is due money and small advance fee/personal banking information required to facilitate transfer
- Phishing: attempt to gain personal/confidential information; apparent legitimate communication hides embedded code that redirects user to third-party site



NIGERIA NATIONAL PETROLEUM CORPORATION

PETROLEUM AND PROJECT DIVISION

TEL: +234-80-33084057, 234-1-4806653, FAX: +234-1-2882183, 234-1-7591061

P.M.B 2071, LAGOS - NIGERIA.

29TH JANUARY, 2002

DEAR SIR

This letter is not intended to cause any embarrassment in whatever form, rather is compelled to contact your esteemed self, following the knowledge of your high repute and trustworthiness. Firstly, I must solicit your confidentiality, this is by the virtue of its' nature as being utterly confidential and top secret though I know that a transaction of this magnitude will make anyone apprehensive and worried, but I am assuring you that all will be well at the end of the day. A bold step taken shall not be regretted I assure you.

I am Mr. Tony Okeke and I head a seven man tender board in charge of contract awards and payment approvals, I came to know of you in search of a reliable and reputable person to handle a very confidential business transaction which involves the transfer of a huge sum of money to foreign account requiring maximum confidence. My colleagues and I are top officials of the NIGERIA NATIONAL PETROLEUM CORPORATION (NNPC). OUR DUTIES INCLUDE VETTING, EVALUATION AND FORESEEING THE MAINTENANCE OF THE REFINERIES IN ALL THE DESIGNATED OIL PIPELINES. We are therefore soliciting for your assistance to enable us transfer into your account the said funds. Our country loses a lot of money everyday that is why the international community is very careful and warning their citizens to be careful but I tell you "A TRIAL WILL CONVINCE YOU".

The source of the fund is as follows; during the last military regime here in Nigeria this committee awarded a contract of US\$400million to a group of five construction companies on behalf of the NIGERIA NATIONAL PETROLEUM CORPORATION for the construction of the oil pipelines in Kaduna, Port-Harcourt, Warri refineries. During this process my colleagues and I deliberately inflated the total contract sum to the tune US\$428million with the intention of sharing the inflated sum of US\$28. The government has since approved the sum of US\$428 for us as the contract sum, but since the contract is only worth US\$400million, the remaining US\$28million is what we intend to transfer to reliable and safe offshore account, we are prohibited to operate foreign account in our names since we are still in government. Thus, making it impossible for us to acquire the money in our name right now, I have therefore been delegated as a matter of trust by my colleagues to look for an overseas partner into whose account we can transfer the sum of US\$28million.

My colleagues and I have decided that if you/your company can be the beneficiary of this funds on our behalf, you or your company will retain 20% of the total sum US\$28million while 75% will be for us the officials and remaining 5% will be used for offsetting all debts/expenses incurred during this transaction.

We have decided that this transaction can only proceed under the following conditions:

1. That you treat this transaction with utmost secrecy and confidentiality and conviction of your transparent honesty.
2. That upon the receipt of the funds you will release the funds as instructed by us after you have removed your share of 20%. Please acknowledge the receipt of this letter using the above telephone and fax numbers. I will bring you into the nomenclature of this transaction when I have heard from you.

Your urgent response will be highly appreciated as we catching on the next payment schedule for the financial quarter. Please be assured that this transaction is 100% legal/risk free, only trust can make the reality of this transaction.

Best Regards,

Tony Okeke
MR. TONY OKEKE

Figure 2-10 Example of a Nigerian 4-1-9 fraud letter

Information Extortion

- Attacker steals information from a computer system and demands compensation for its return or nondisclosure. Also known as cyberextortion.
- Commonly done in credit card number theft

Sabotage or Vandalism

- Threats can range from petty vandalism to organized sabotage.
- Web site defacing can erode consumer confidence, diminishing organization's sales, net worth, and reputation.
- Threat of hacktivist or cyberactivist operations is rising.
- Cyberterrorism/Cyberwarfare: a much more sinister form of hacking

Cyber Activists Wanted - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://archive.greenpeace.org/~climate/messages.html> Go

Cyber Activists Wanted

If you are tired of watching what is going on in the world and want to help us make tomorrow better - then join us.

We are now recruiting online activists to work with us on Greenpeace actions. If you want to join us, please complete and send the form below. You will be contacted by email in the days leading up to actions around the world and then be asked to be log onto the web at a specified time to take part in coordinated Net actions.

Your name:	<input type="text"/>
Your e-mail:	<input type="text"/>
Your City:	<input type="text"/>
Your Country:	<input type="text"/>
Age:	<input type="text"/>
Member of Greenpeace?	<input type="checkbox"/>
Previous action experiences?	<input type="checkbox"/>
How did you find out about the Greenpeace call for cyber activists?	<input type="text" value="Greenpeace Website"/>
<input type="button" value="Send"/> <input type="button" value="Clear Form"/>	

Done Internet

© Cengage Learning 2015

Figure 2-14 Cyberactivists wanted

Software Attacks

- Malicious software (malware) is used to overwhelm the processing capabilities of online systems or to gain access to protected systems via hidden means.
- Software attacks occur when an individual or a group designs and deploys software to attack a system.

Software Attacks (cont'd)

- Types of attacks include:
 - Malware (malicious code): It includes the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information.
 - Virus: It consists of code segments that attach to existing program and take control of access to the targeted computer.
 - Worms: They replicate themselves until they completely fill available resources such as memory and hard drive space.
 - Trojan horses: malware disguised as helpful, interesting, or necessary pieces of software

Malware	Type	Year	Estimated number of systems infected	Estimated financial damage
MyDoom	Worm	2004	2 million	\$38 billion
Klez (and variants)	Virus	2001	7.2% of Internet	\$19.8 billion
ILOVEYOU	Virus	2000	10% of Internet	\$5.5 billion
Sobig F	Worm	2003	1 million	\$3 billion
Code Red (and CR II)	Worm	2001	400,000 servers	\$2.6 billion
SQL Slammer, a.k.a. Sapphire	Worm	2003	75,000	\$950 million to \$1.2 billion
Melissa	Macro virus	1999	Unknown	\$300 million to \$600 million
CIH, a.k.a. Chernobyl	Memory-resident virus	1998	Unknown	\$250 million
Storm Worm	Trojan horse virus	2006	10 million	Unknown
Conficker	Worm	2009	15 million	Unknown
Nimda	Multivector worm	2001	Unknown	Unknown
Sasser	Worm	2004	500,000 to 700,000	Unknown
Nesky	Virus	2004	Under 100,000	Unknown
Leap-A/Oompa-A	Virus	2006	Unknown (Apple)	Unknown

Table 2-4 The Most Dangerous Malware Attacks to Date^{36,37}

© Cengage Learning 2015

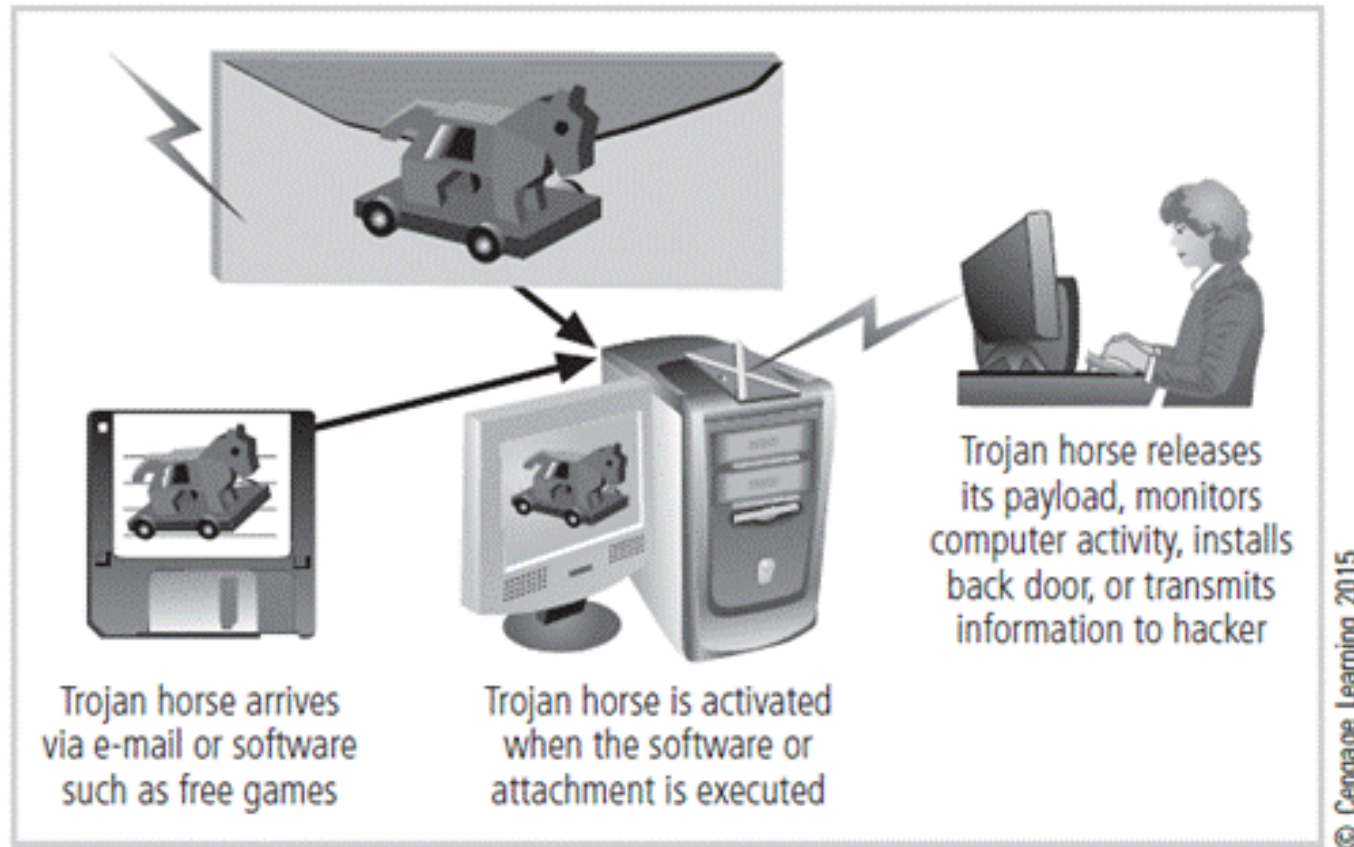


Figure 2-17 Trojan horse attacks

Software Attacks (cont'd)

- Types of attacks (cont'd)
 - Polymorphic threat: actually evolves to elude detection
 - Virus and worm hoaxes: nonexistent malware that employees waste time spreading awareness about
 - Back door: gaining access to system or network using known or previously unknown/newly discovered access mechanism

Software Attacks (cont'd)

- Types of attacks (cont'd)
 - Denial-of-service (DoS): An attacker sends a large number of connection or information requests to a target.
 - The target system becomes overloaded and cannot respond to legitimate requests for service.
 - It may result in system crash or inability to perform ordinary functions.
 - Distributed denial-of-service (DDoS): A coordinated stream of requests is launched against a target from many locations simultaneously.

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.

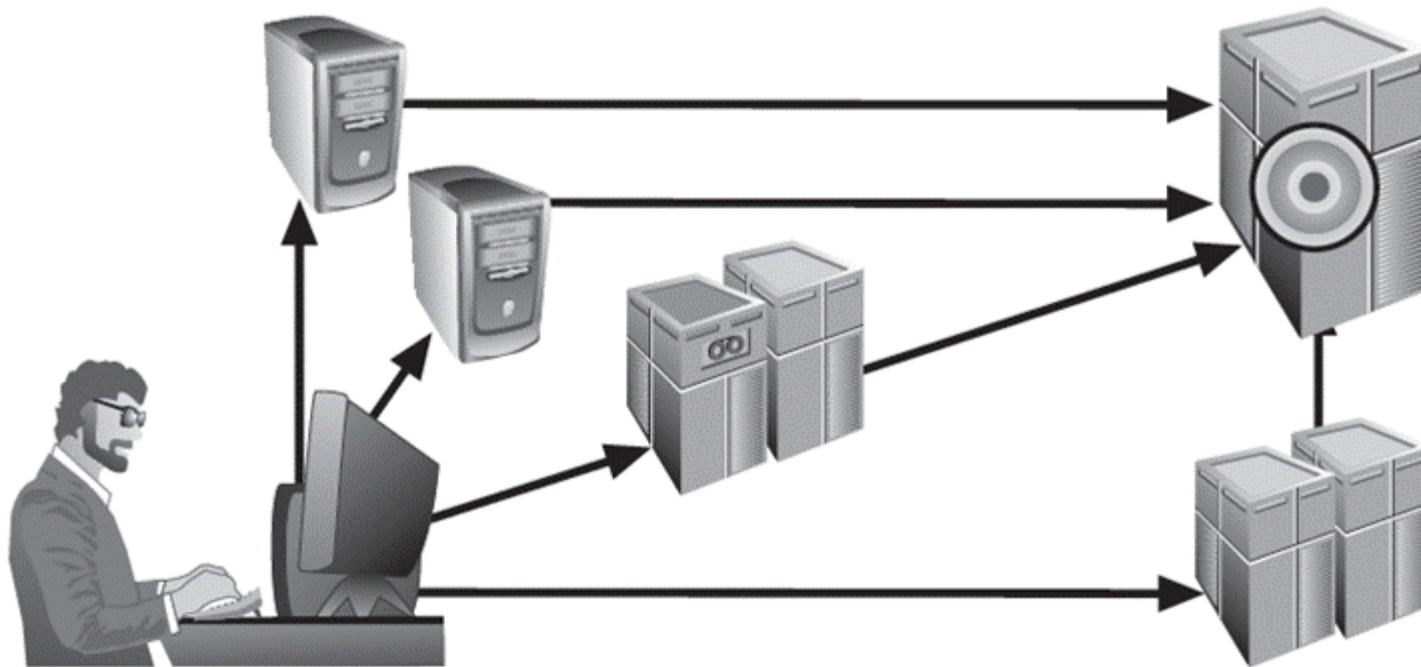


Figure 2-18 Denial-of-service attack

Software Attacks (cont'd)

- Types of attacks (cont'd)
 - Mail bombing (also a DoS): An attacker routes large quantities of e-mail to target to overwhelm the receiver.
 - Spam (unsolicited commercial e-mail): It is considered more a nuisance than an attack, though is emerging as a vector for some attacks.
 - Packet sniffer: It monitors data traveling over network; it can be used both for legitimate management purposes and for stealing information from a network.
 - Spoofing: A technique used to gain unauthorized access; intruder assumes a trusted IP address.

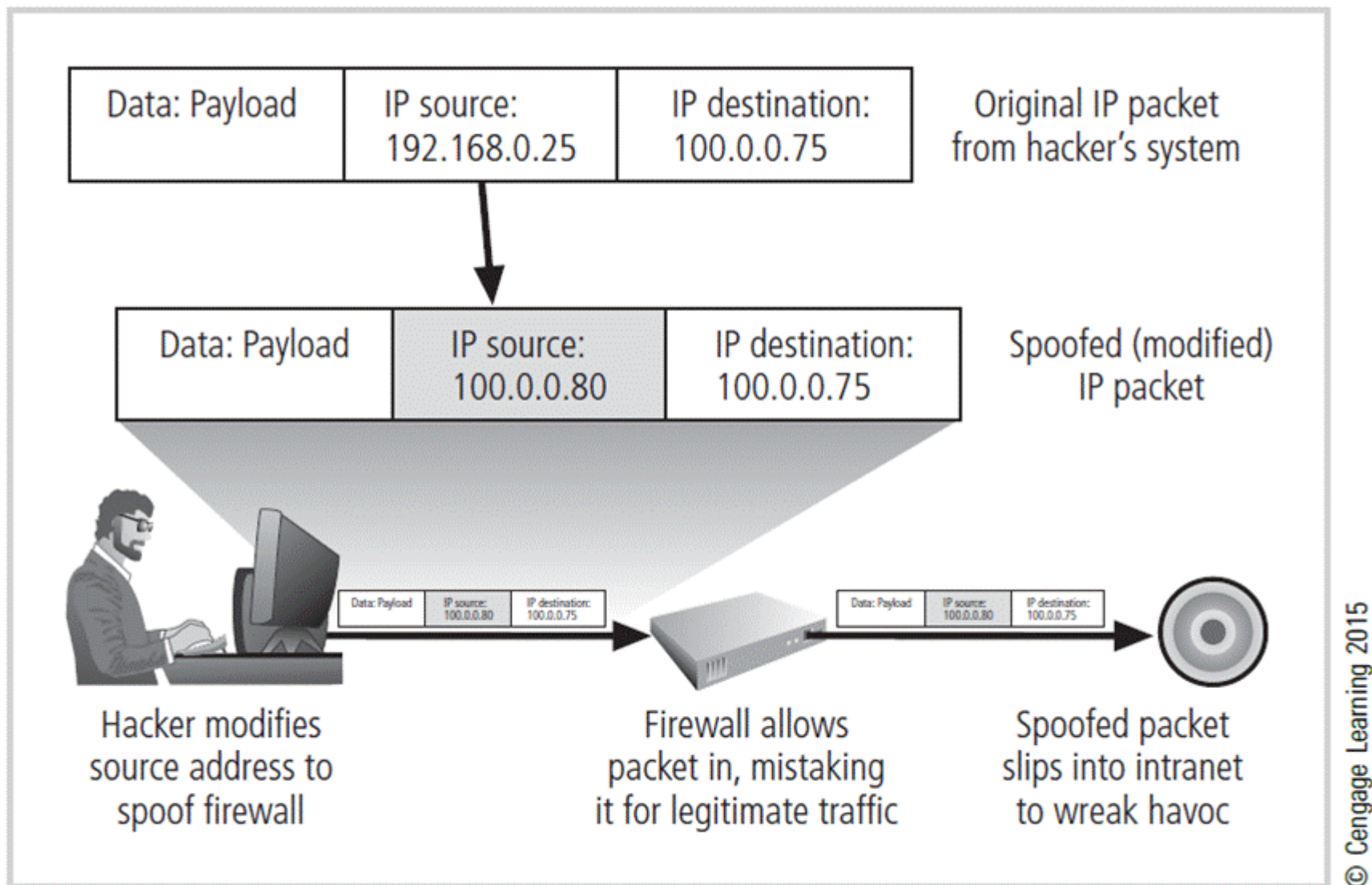
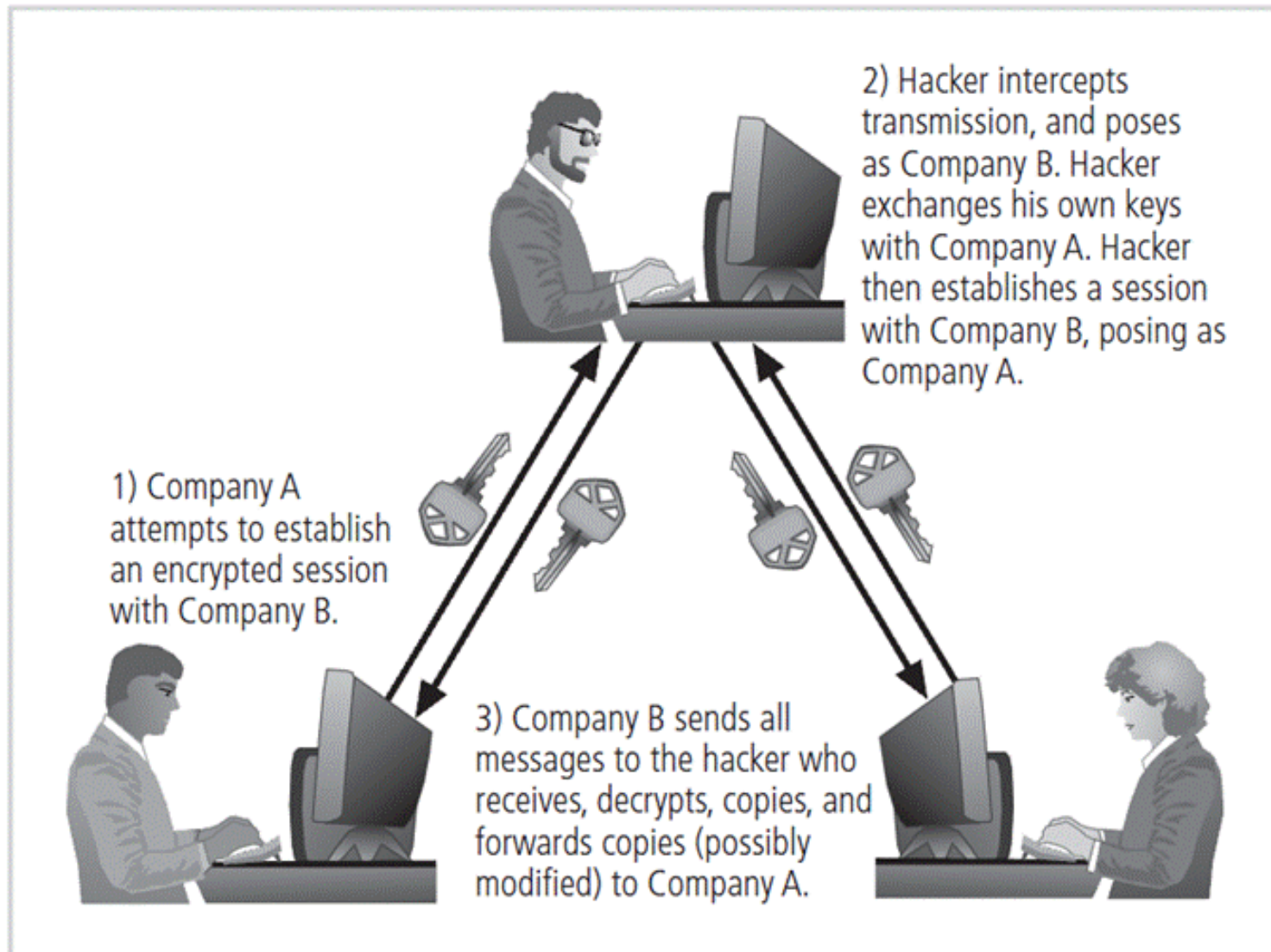


Figure 2-19 IP spoofing attack

Software Attacks (cont'd)

- Types of attacks (cont'd)
 - Pharming: It attacks a browser's address bar to redirect users to an illegitimate site for the purpose of obtaining private information.
 - Man-in-the-middle: An attacker monitors the network packets, modifies them, and inserts them back into the network.



© Cengage Learning 2015

Figure 2-20 Man-in-the-middle attack

Technical Hardware Failures or Errors

- They occur when a manufacturer distributes equipment containing a known or unknown flaw.
- They can cause the system to perform outside of expected parameters, resulting in unreliable service or lack of availability.
- Some errors are terminal and some are intermittent.
- Intel Pentium CPU failure
- Mean time between failure measures the amount of time between hardware failures.

Technical Software Failures or Errors (cont'd)

- Large quantities of computer code are written, debugged, published, and sold before all bugs are detected and resolved.
- Combinations of certain software and hardware can reveal new software bugs.
- Entire Web sites are dedicated to documenting bugs.
- Open Web Application Security Project (OWASP) is dedicated to helping organizations create/operate trustworthy software and publishes a list of top security risks.

The Deadly Sins in Software Security

- Common failures in software development:
 - Buffer overruns
 - Command injection
 - Cross-site scripting (XSS)
 - Failure to handle errors
 - Failure to protect network traffic
 - Failure to store and protect data securely
 - Failure to use cryptographically strong random numbers

The Deadly Sins in Software Security (cont'd)

- Common failures in software development (cont'd):
 - Format string problems
 - Neglecting change control
 - Improper file access
 - Improper use of SSL
 - Information leakage
 - Integer bugs (overflows/underflows)
 - Race conditions
 - SQL injection

The Deadly Sins in Software Security (cont'd)

- Problem areas in software development:
 - Trusting network address resolution
 - Unauthenticated key exchange
 - Use of magic URLs and hidden forms
 - Use of weak password-based systems
 - Poor usability

Technological Obsolescence

- Antiquated/outdated infrastructure can lead to unreliable, untrustworthy systems.
- Proper managerial planning should prevent technology obsolescence.
- IT plays a large role.

Theft

- Illegal taking of another's physical, electronic, or intellectual property
- Physical theft is controlled relatively easily.
- Electronic theft is a more complex problem; the evidence of crime is not readily apparent.

Secure Software Development

- Many information security issues discussed here are caused by software elements of the system.
- Development of software and systems is often accomplished using methodology such as systems development life cycle (SDLC).
- Many organizations recognize the need for security objectives in SDLC and have included procedures to create more secure software.
- This software development approach is known as Software Assurance (SA).

Software Assurance and the SA Common Body of Knowledge

- A national effort is underway to create a common body of knowledge focused on secure software development.
- U.S. Department of Defense and Department of Homeland Security supported the Software Assurance Initiative, which resulted in the publication of Secure Software Assurance (SwA) Common Body of Knowledge (CBK).
- SwA CBK serves as a strongly recommended guide to developing more secure applications.

Software Design Principles

- Good software development results in secure products that meet all design specifications.
- Some commonplace security principles:
 - Keep design simple and small
 - Access decisions by permission not exclusion
 - Every access to every object checked for authority
 - Design depends on possession of keys/passwords
 - Protection mechanisms require two keys to unlock
 - Programs/users utilize only necessary privileges

Software Design Principles (cont'd)

- Some commonplace security principles:
 - Minimize mechanisms common to multiple users
 - Human interface must be easy to use so users routinely/automatically use protection mechanisms.

Summary

- Unlike any other aspect of IT, information security's primary mission is 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 (cont'd)

- 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
- Secure systems require secure software.