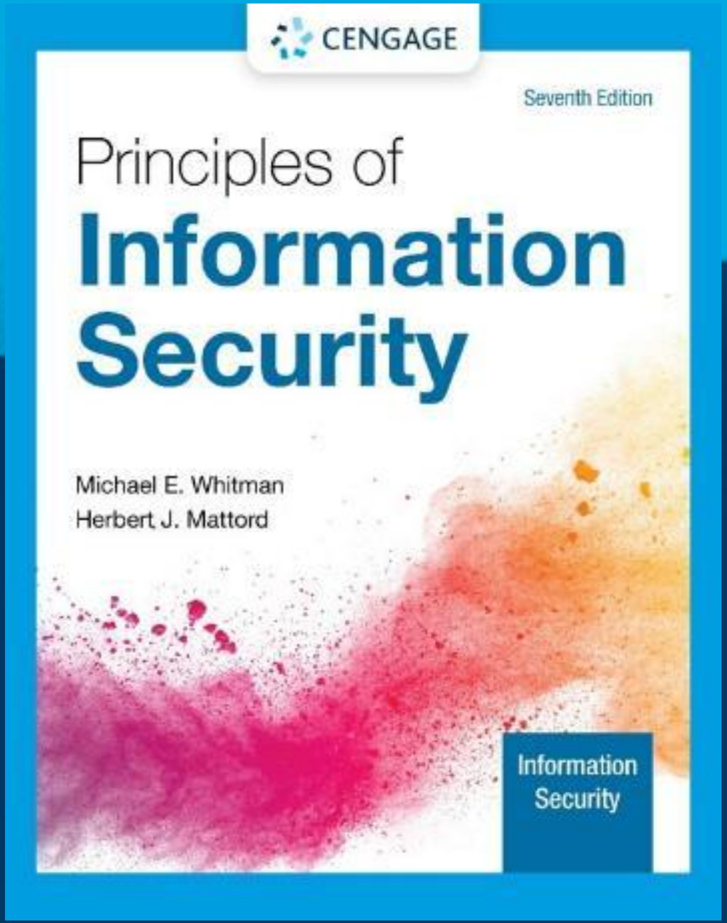


Module 2

The need for InfoSec

Module Objectives

By the end of this module, you should be able to:

2.1 Discuss the need for information security

2.2 Explain why a successful information security program is the shared responsibility of the entire organization

2.3 List and describe the threats posed to information security and common attacks associated with those threats

2.4 List the common information security issues that result from poor software development efforts

Introduction to the Need for Information Security (1 of 2)

- The primary mission of an information security program is to ensure that **information assets**—information and the systems that house them—remain safe and useful.
- If threats didn’t exist, resources could be used exclusively to improve systems that contain, use, and transmit information.
- The threat of attacks on information systems is a constant concern.
- Organizations must understand the environment in which information assets reside so their information security programs can address actual and potential problems.

Introduction to the Need for Information Security (2 of 2)

- 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**

Business Needs First

- When **security** needs **and business** needs collide, **business wins**.
- Without the underlying business to generate revenue and use the information, the information may lose value, and there would be no need for it.
- If the **business cannot function**, **information security becomes less important**.
- The key is to **balance** the **business needs** of the organization with the need to protect information assets, realizing that **business needs come first.**

Protecting Functionality

- All three communities of interest (InfoSec Manag, IT Manag, Organization Manag) are responsible for facilitating security programs.
- Implementing information security has **more to do with management than technical.**
- Communities of interest should address information security in terms of business impact and cost of business interruption, rather than isolating security as a technical problem.

Protecting Data That Organizations Collect and Use

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

Enabling the Safe Operation of Applications

- Today’s organizations are under immense pressure to create and operate integrated, efficient, and capable applications (software).
- Organizations needs environment that safeguard applications using IT systems.
- Management must continue to oversee infrastructure once in place—not relegate (transfer) it to the 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.
- IT continues to add new capabilities and methods that allow organizations to solve business information management challenges.

Information Security Threats and Attacks

- **Threat:** A *potential risk* to an asset's loss of value. (a virus)
- **Attack:** An intentional or unintentional *act* that can damage or otherwise compromise information and the systems that support it. (backdoor virus attack)
- **Vulnerability:** A potential *weakness* in an asset or its defensive control system(s). (virus scan not up to date)
- **Exploit:** A *technique* used to compromise a system. (attacker exploits virus scan not update to download files remotely from your computer using FinSpy)
- Management must be informed about the various threats to an organization's people, applications, data, and information systems.
- Overall security is improving, but the number of potential hackers is growing.

Knowledge Check Activity 1

Match the terms on the left with the definitions on the right.

Term
Threat
Attack
Exploit
Vulnerability

Definition
An intentional or unintentional act that can damage or otherwise compromise information and the systems that support it.
A potential weakness in an asset or its defensive control system(s).
A potential risk to an asset’s loss of value.
A technique used to compromise a system.

Knowledge Check Activity 1: Answer

Match the terms with the definitions.

Answer:

Term	Definition
Threat	A potential risk to an asset's loss of value.
Attack	An intentional or unintentional act that can damage or otherwise compromise information and the systems that support it.
Exploit	A technique used to compromise a system.
Vulnerability	A potential weakness in an asset or its defensive control system(s).

World Internet Usage

World Regions	Population (2020 Est.)	Population % of World	Internet Users (6/30/2020)	Penetration Rate (% Pop.)	Growth 2000–2020	Internet World %
Africa	1,340,598,447	17.2%	566,138,772	42.2%	12,441%	11.7%
Asia	4,294,516,659	55.1%	2,525,033,874	58.8%	2,109%	52.2%
Europe	834,995,197	10.7%	727,848,547	87.2%	592%	15.1%
Latin America/ Caribbean	654,287,232	8.4%	467,817,332	71.5%	2,489%	9.7%
Middle East	260,991,690	3.3%	184,856,813	70.8%	5,527%	3.8%
North America	368,869,647	4.7%	332,908,868	90.3%	208%	6.9%
Oceania/ Australia	42,690,838	0.5%	28,917,600	67.7%	279%	0.6%
WORLD TOTAL	7,796,949,710	100.0%	4,833,521,806	62.0%	1,239%	100.0%

Rated Threats from Internal Sources in 2015 SEC/CISE Survey of Threats to Information Protection (1 of 2)

From Employees or Internal Stakeholders	Not a Threat 1	2	3	4	A Severe Threat 5
Inability/unwillingness to follow established policy	6.6%	17.2%	33.6%	26.2%	16.4%
Disclosure due to insufficient training	8.1%	23.6%	29.3%	25.2%	13.8%
Unauthorized access or escalation of privileges	4.8%	24.0%	31.2%	31.2%	8.8%
Unauthorized information collection/data sniffing	6.4%	26.4%	40.0%	17.6%	9.6%
Theft of on-site organizational information assets	10.6%	32.5%	34.1%	12.2%	10.6%
Theft of mobile/laptop/tablet and related/ connected information assets	15.4%	29.3%	28.5%	17.9%	8.9%

Rated Threats from Internal Sources in 2015 SEC/CISE Survey of Threats to Information Protection (2 of 2)

From Employees or Internal Stakeholders	Not a Threat 1	2	3	4	A Severe Threat 5
Intentional damage or destruction of information assets	22.3%	43.0%	18.2%	13.2%	3.3%
Theft or misuse of organizationally leased, purchased, or developed software	29.6%	33.6%	21.6%	10.4%	4.8%
Web site defacement	43.4%	33.6%	16.4%	4.9%	1.6%
Blackmail of information release or sales	43.5%	37.1%	10.5%	6.5%	2.4%

Rated Threats from External Sources in 2015 SEC/CISE Survey of Threats to Information Protection (1 of 2)

From Outsiders or External Stakeholders	Not a Threat 1	2	3	4	A Severe Threat 5
Unauthorized information collection/data sniffing	6.4%	14.4%	21.6%	32.8%	24.8%
Unauthorized access or escalation of privileges	7.4%	14.0%	26.4%	31.4%	20.7%
Web site defacement	8.9%	23.6%	22.8%	26.8%	17.9%
Intentional damage or destruction of information assets	14.0%	32.2%	18.2%	24.8%	10.7%
Theft of mobile/laptop/tablet and related/ connected information assets	20.5%	25.4%	26.2%	15.6%	12.3%
Theft of on-site organizational information assets	21.1%	24.4%	25.2%	17.9%	11.4%

Rated Threats from External Sources in 2015 SEC/CISE Survey of Threats to Information Protection (2 of 2)

From Outsiders or External Stakeholders	Not a Threat 1	2	3	4	A Severe Threat 5
Blackmail of information release or sales	31.1%	30.3%	14.8%	14.8%	9.0%
Disclosure due to insufficient training	34.5%	21.8%	22.7%	13.4%	7.6%
Inability/unwillingness to follow established policy	33.6%	29.4%	18.5%	6.7%	11.8%
Theft or misuse of organizationally leased, purchased, or developed software	31.7%	30.1%	22.8%	9.8%	5.7%

Perceived Threats to Information Assets in 2015 SEC/ CISE Survey of Threats to Information Protection (1 of 5)

General Threats to Information Assets	Not a Threat 1	2	3	4	A Severe Threat 5
Electronic phishing/spoofing attacks	0.8%	13.1%	16.4%	32.0%	37.7%
Malware attacks	1.7%	12.4%	27.3%	36.4%	22.3%
Unintentional employee/insider mistakes	2.4%	17.1%	26.8%	35.8%	17.9%
Loss of trust due to information loss	4.1%	18.9%	27.0%	22.1%	27.9%
Software failures or errors due to unknown vulnerabilities in externally acquired software	5.6%	18.5%	28.2%	33.9%	13.7%
Social engineering of employees/insiders based on social media information	8.1%	14.6%	32.5%	34.1%	10.6%
Social engineering of employees/insiders based on other published information	8.9%	19.5%	24.4%	32.5%	14.6%

Perceived Threats to Information Assets in 2015 SEC/ CISE Survey of Threats to Information Protection (2 of 5)

General Threats to Information Assets	Not a Threat 1	2	3	4	A Severe Threat 5
Software failures or errors due to poorly developed, internally created applications	7.2%	21.6%	24.0%	32.0%	15.2%
SQL injections	7.6%	17.6%	31.9%	29.4%	13.4%
Social engineering of employees/insiders based on organization's Web sites	11.4%	19.5%	23.6%	31.7%	13.8%
Denial of service (and distributed DoS) attacks	8.2%	23.0%	27.9%	32.8%	8.2%
Software failures or errors due to known vulnerabilities in externally acquired software	8.9%	23.6%	26.8%	35.8%	4.9%
Outdated organizational software	8.1%	28.2%	26.6%	26.6%	10.5%

Perceived Threats to Information Assets in 2015 SEC/ CISE Survey of Threats to Information Protection (3 of 5)

General Threats to Information Assets	Not a Threat 1	2	3	4	A Severe Threat 5
Loss of trust due to representation as source of phishing/spoofing attack	9.8%	23.8%	30.3%	23.0%	13.1%
Loss of trust due to Web defacement	12.4%	30.6%	31.4%	19.8%	5.8%
Outdated organizational hardware	17.2%	34.4%	32.8%	12.3%	3.3%
Outdated organization data format	18.7%	35.8%	26.8%	13.8%	4.9%
Inability/unwillingness to establish effective policy by management	30.4%	26.4%	24.0%	13.6%	5.6%
Hardware failures or errors due to aging equipment	19.5%	39.8%	24.4%	14.6%	1.6%

Perceived Threats to Information Assets in 2015 SEC/ CISE Survey of Threats to Information Protection (4 of 5)

General Threats to Information Assets	Not a Threat 1	2	3	4	A Severe Threat 5
Hardware failures or errors due to defective equipment	17.9%	48.0%	24.4%	8.1%	1.6%
Deviations in quality of service from other provider	25.2%	38.7%	25.2%	7.6%	3.4%
Deviations in quality of service from data communications provider/ISP	26.4%	39.7%	23.1%	7.4%	3.3%
Deviations in quality of service from telecommunications provider/ISP (if different from data provider)	29.9%	38.5%	18.8%	9.4%	3.4%
Loss due to other natural disaster	31.0%	37.9%	23.3%	6.9%	0.9%

Perceived Threats to Information Assets in 2015 SEC/ CISE Survey of Threats to Information Protection (5 of 5)

General Threats to Information Assets	Not a Threat 1	2	3	4	A Severe Threat 5
Loss due to fire	26.2%	49.2%	21.3%	3.3%	0.0%
Deviations in quality of service from power provider	36.1%	43.4%	12.3%	5.7%	2.5%
Loss due to flood	33.9%	43.8%	19.8%	1.7%	0.8%
Loss due to earthquake	41.7%	35.8%	15.0%	6.7%	0.8%

Common Attack Pattern Enumeration and Classification (CAPEC)

- A tool that security professionals can use to understand attacks is the Common Attack Pattern Enumeration and Classification (CAPEC) Web site hosted by Mitre—a nonprofit research and development organization sponsored by the U.S. government.
- This online repository can be searched for characteristics of a particular attack or simply browsed by professionals who want additional knowledge of how attacks occur procedurally.

The 12 Categories of Threats

The 12 Categories of Threats to Information Security

Category of Threat	Attack Examples
Compromises to intellectual property	Piracy, copyright infringement (violation)
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

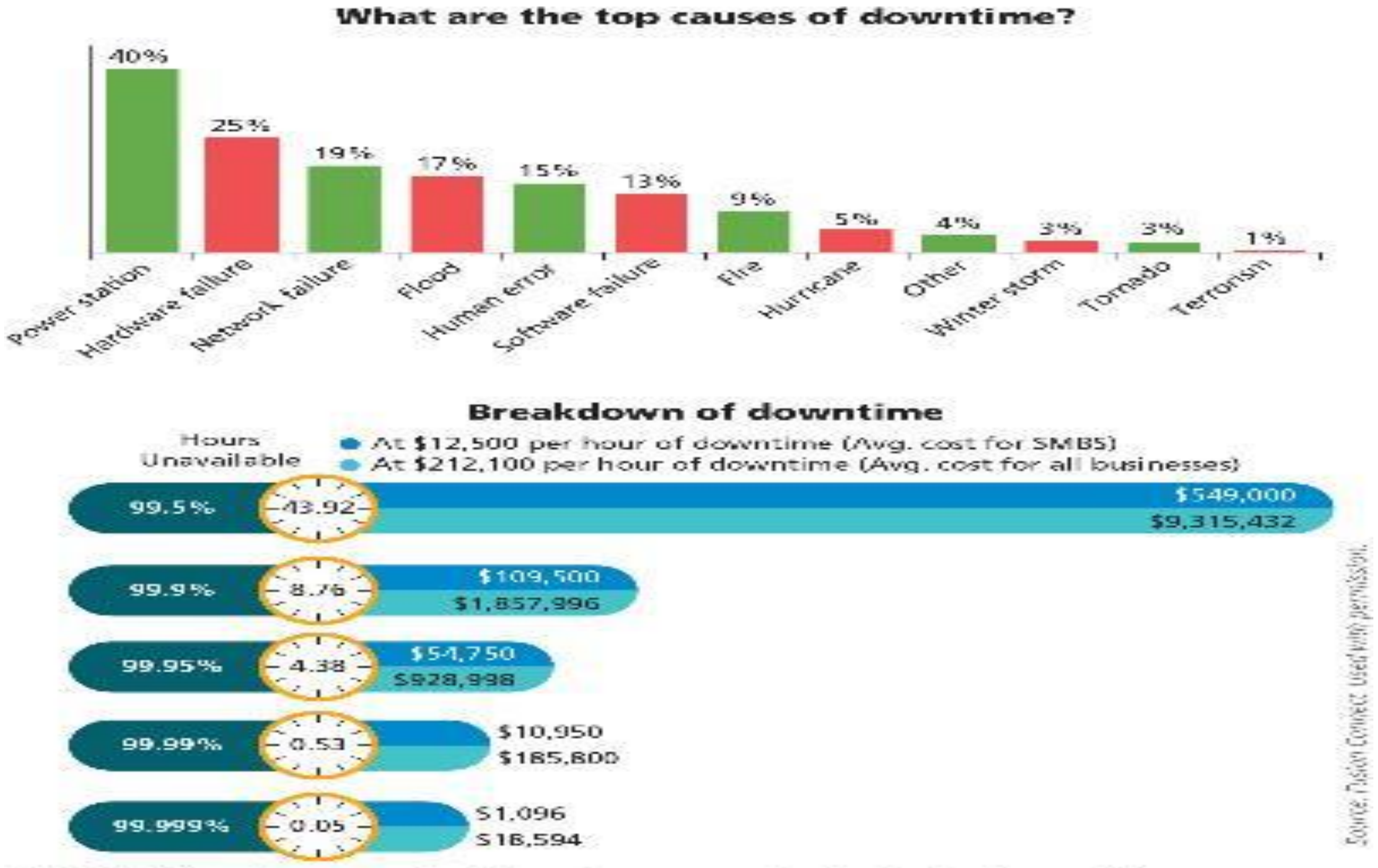
Compromises to Intellectual Property

- **Intellectual property (IP)**: creation, ownership, and control of original ideas as well as the tangible or virtual representation of those ideas,
- IP includes trade secrets, copyrights, trademarks, and patents.
- The most common IP breaches involve the unlawful use or duplication of software (software piracy).
- Two watchdog organizations investigate software abuse:
    - Software and Information Industry Association (SIIA)
    - Business Software Alliance (BSA)
- According to the BSA, in 2018, approximately 37 percent of software installed on personal computers globally was not properly licensed.

Deviations in Quality of Service (1 of 3)

- This category represents situations in which a product or services are not delivered to the organization as expected.
- An information system depends on the successful operation of many interdependent support systems, including power grids, telecom networks, parts suppliers, service vendors, and even the janitorial staff and garbage haulers.
- Internet service, communications, and power irregularities dramatically affect the availability of information and systems.
- Services are usually arranged with a service level agreement (SLA).

Average Cost of Downtime According to Fusion Connect



Source: Fusion Connect. Used with permission.

Figure 2-4 Average cost of downtime according to Fusion Connect[12]

Deviations in Quality of Service (2 of 3)

- Internet service issues
  - Internet Service Provider (ISP) failures can considerably undermine the availability of information.
  - An 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 an organization’s ability to function.

Deviations in Quality of Service (3 of 3)

- Power irregularities
  - Commonplace
  - Lead to fluctuations such as power excesses, power shortages, and power losses (blackout, brownout, fault, noise, sag, spike, or surge)
  - Sensitive electronic equipment vulnerable to and easily damaged/destroyed by fluctuations
  - Controls can be applied to manage power quality.

Espionage or Trespass

- This threat represents a well-known and broad category of electronic and human activities that breach the confidentiality of information.
- Access of protected information by unauthorized individuals
- When information gatherers employ techniques that cross the threshold of what is legal and/or ethical, they enter the world of industrial espionage.
- **Competitive intelligence** techniques are legal, whereas **industrial espionage** techniques are not.
- Acts of **trespass** can lead to unauthorized real or virtual actions that enable information gatherers to enter premises or systems without permission.

Espionage or Trespass

- Controls are sometimes implemented to mark the boundaries of an organization’s virtual territory.
- These boundaries give notice to trespassers that they are intruding on the organization’s cyberspace.
- The classic perpetrator (criminal) of deliberate acts of espionage or trespass is the hacker.
- A hacker uses skill, guile (cleverness), or fraud to attempt to bypass the controls placed around information that is the property of someone else.
- The hacker frequently spends long hours examining the types and structures of the targeted systems.

Shoulder Surfing

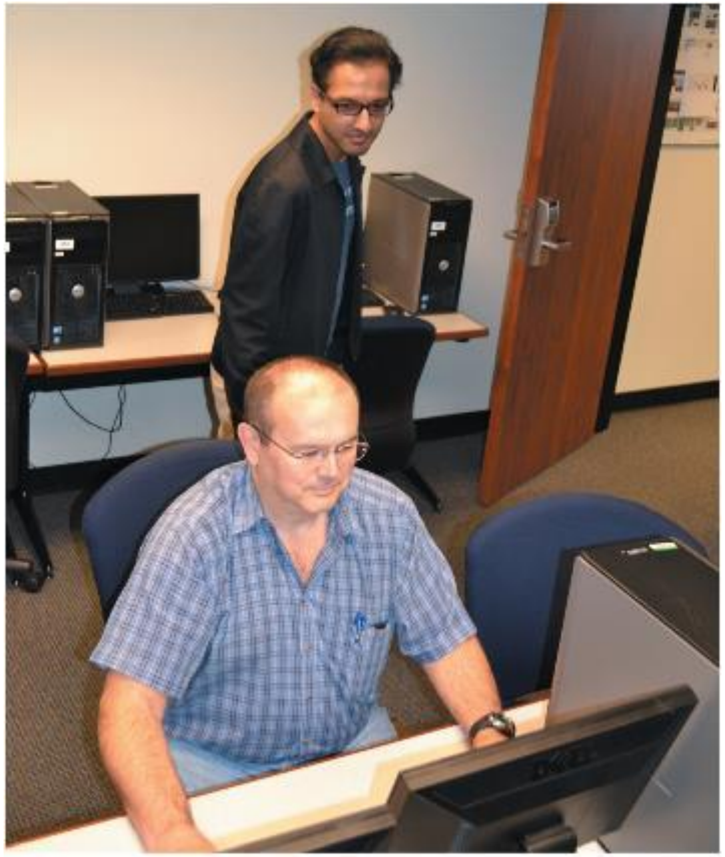


Figure 2-5 Shoulder surfing

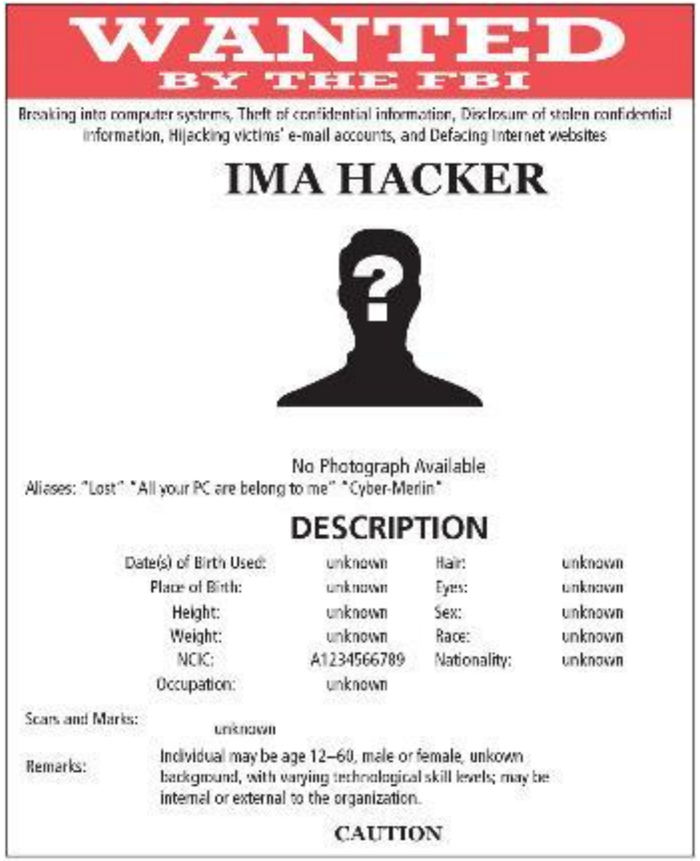
Shoulder surfing can occur anywhere a person accesses confidential information.

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

Espionage or Trespass

- Expert hacker
  - Develops software scripts and program exploits
  - Usually a master of many skills (programming languages, networking protocols, and operating systems and also exhibits a mastery of the technical environment of the chosen targeted system.)
  - Will often create attack software and share with others
- Unskilled hackers
  - Many more unskilled hackers than expert hackers
  - Use expertly written software to exploit a system
  - Do not usually fully understand the systems they hack
  - Also known as **script kiddies** or **packet monkeys**

Hacker Profile



WANTED
BY THE FBI

Breaking into computer systems, Theft of confidential information, Disclosure of stolen confidential information, Hijacking victims' e-mail accounts, and Defacing Internet websites

IMA HACKER

No Photograph Available

Aliases: "Lost" "All your PC are belong to me" "Cyber-Merlin"

DESCRIPTION

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, unkown background, with varying technological skill levels; may be internal or external to the organization.

CAUTION

Figure 2-6 Contemporary hacker profile

Espionage or Trespass

- 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

Password Strength (1 of 2)

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	0.36 seconds
9	5,429,503,678,976	9.27 seconds
10	141,167,095,653,376	4.02 minutes
11	3,670,344,486,987,780	1.74 hours
12	95,428,956,661,682,200	1.89 days
13	2,481,152,873,203,740,000	49.05 days
14	64,509,974,703,297,200,000	3.5 years
15	1,677,259,342,285,730,000,000	90.9 years
16	43,608,742,899,428,900,000,000	2,362.1 years

Password Strength (2 of 2)

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	1.0 hours
9	167,619,550,409,708,000	3.3 days
10	13,744,803,133,596,100,000	271.7 days
11	1,127,073,856,954,880,000,000	61.0 years
12	92,420,056,270,299,900,000,000	5,006.0 years
13	7,578,444,614,164,590,000,000,000	410,493.2 years
14	621,432,458,361,496,000,000,000,000	33,660,438.6 years
15	50,957,461,585,642,700,000,000,000,000	2,760,155,968.2 years
16	4,178,511,850,022,700,000,000,000,000,000	226,332,789,392.1 years

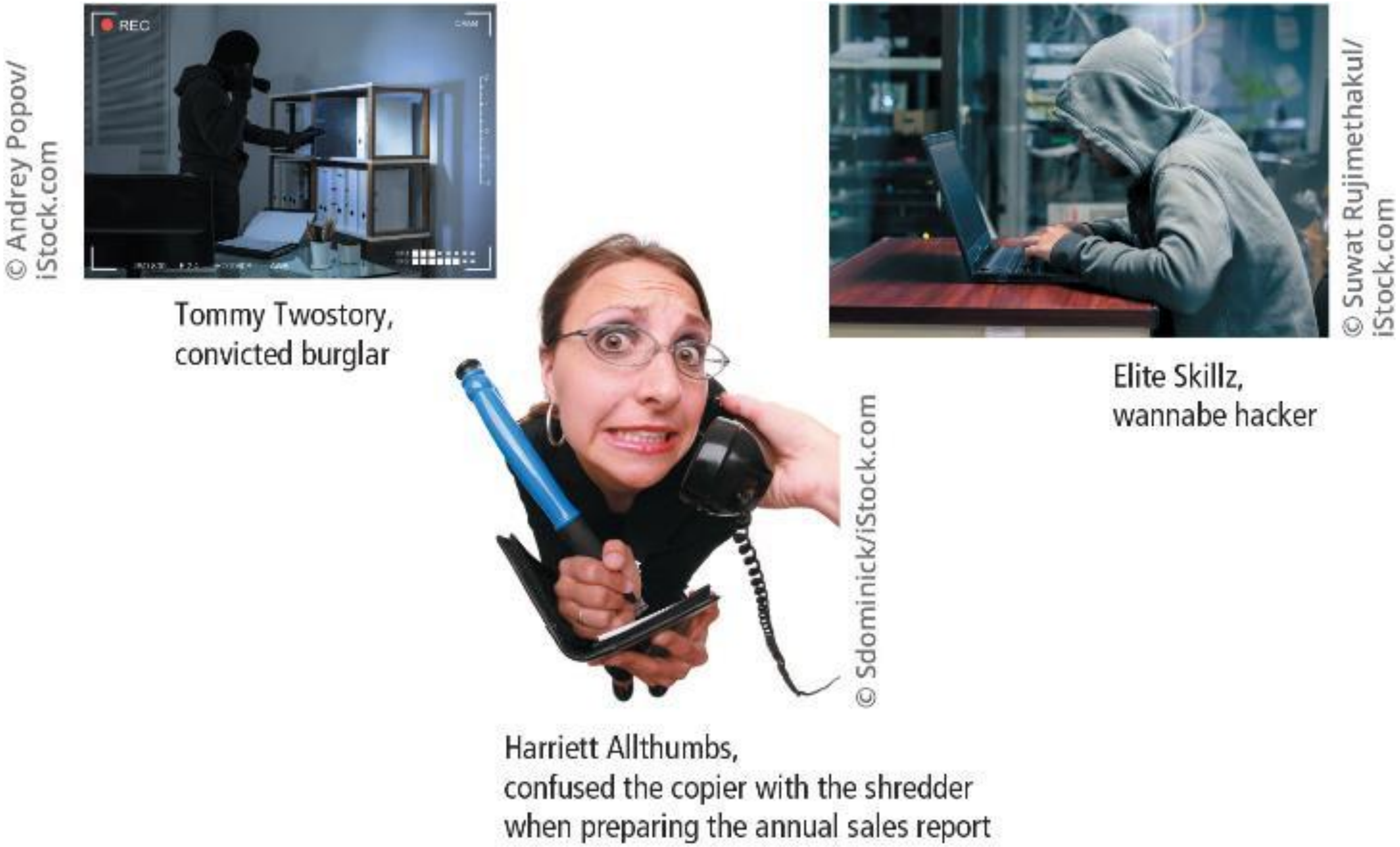
Forces of Nature

- 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.
- Threats include fires, floods, earthquakes, lightning, landslides, tornados, hurricanes, tsunamis, ESD, dust contamination, solar activity, civil unrest, and acts of war.
- Organizations must implement controls to limit damage and prepare contingency (emergency) plans for continued operations.

Human Error or Failure (1 of 2)

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

The Biggest Threat—Acts of Human Error or Failure



© Andrey Popov/iStock.com

© Suwat Rujimethakul/iStock.com

© Sdominick/iStock.com

Figure 2-8 The biggest threat—acts of human error or failure

Human Error or Failure (2 of 2)

- 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.

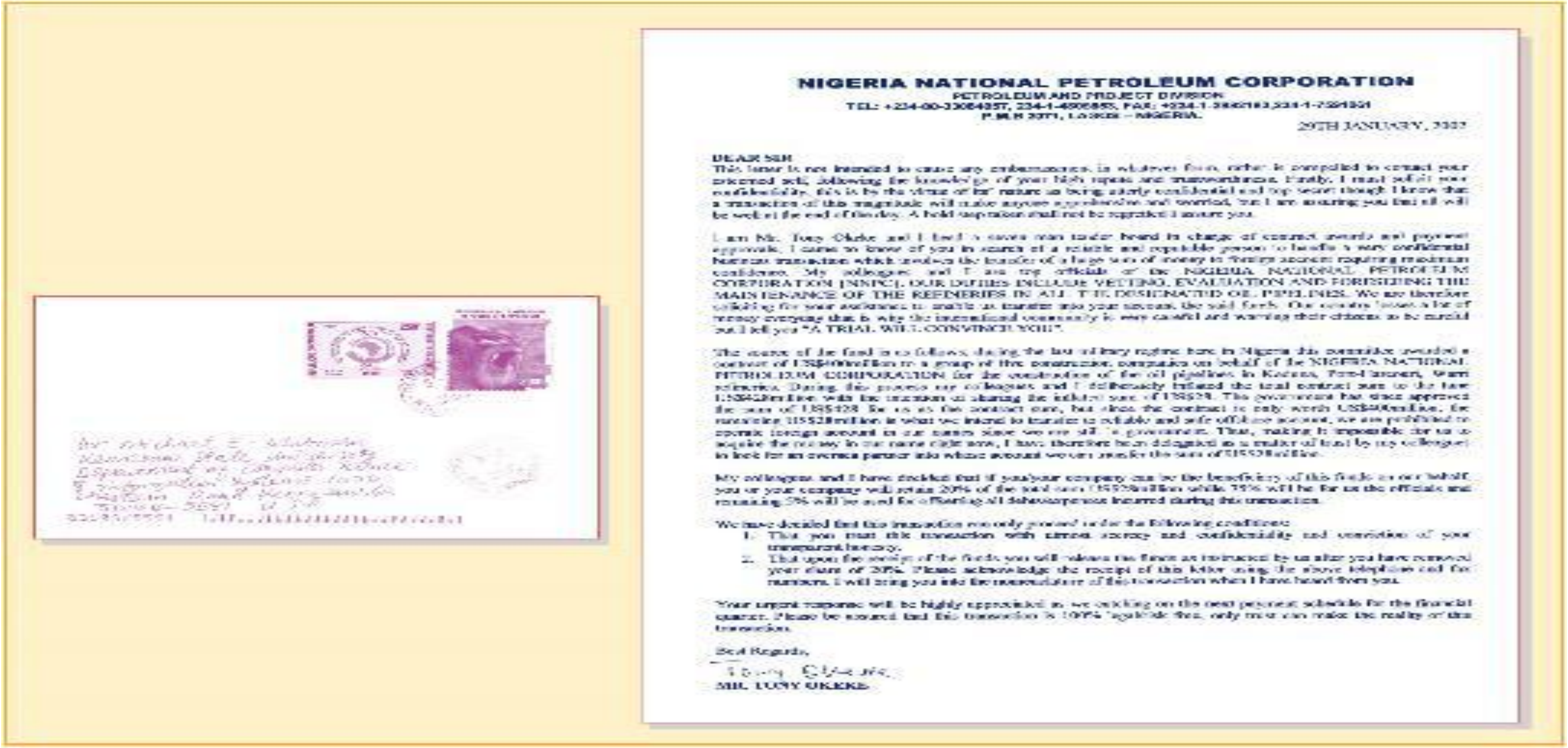
Social Engineering

- **Social engineering** uses social skills to convince people to reveal access credentials or other valuable information to an attacker.
- “People are the weakest link. You can have the best technology; firewalls, intrusion-detection systems, biometric devices ... and somebody can call an unsuspecting employee. That's all she wrote, baby. They got everything.” —Kevin Mitnick

Advance-fee fraud

- indicates recipient is due money and small advance fee or personal banking information required to facilitate transfer
- Business e-mail compromise: exploiting business e-mail systems and users

Example of a Nigerian 4-1-9 Fraud Letter



Mr Michael E. Whitman
Kennesaw State University
Department of Computer Science
& Information Systems 1000
Chastain Road Kennesaw
30144-5591 USA

NIGERIA NATIONAL PETROLEUM CORPORATION
PETROLEUM AND PROJECT DIVISION
TEL: +234-80-3308435T, 234-1-4806855, FAX: +234-1-3860183,234-1-7591821
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 large 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 losses 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 are working 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

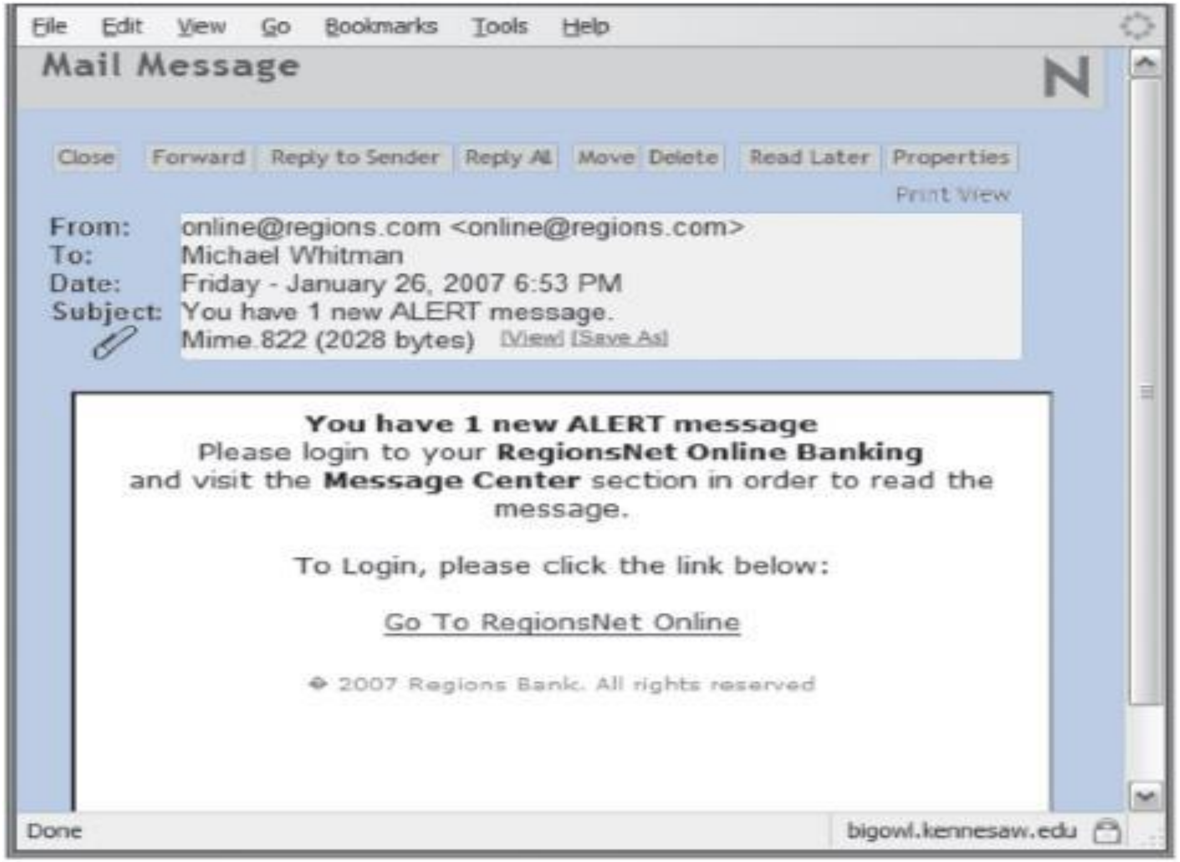
Figure 2-9 Example of a Nigerian 4-1-9 fraud letter

Phishing

- Phishing: attempt to gain personal/confidential information; apparent legitimate communication hides embedded code that redirects user to third-party site
- Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.
- It occurs when an attacker, masquerading as a trusted entity, fools a victim into opening an email, instant message, or text message.
- The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

Phishing Example: Lure

Phishing is an email sent from an Internet criminal disguised as an email from a legitimate, trustworthy source. The message is meant to lure (trap) you into revealing sensitive or confidential information.



From: online@regions.com <online@regions.com>
To: Michael Whitman
Date: Friday - January 26, 2007 6:53 PM
Subject: You have 1 new ALERT message.
Mime.822 (2028 bytes) [View] [Save As]

You have 1 new ALERT message
Please login to your **RegionsNet Online Banking**
and visit the **Message Center** section in order to read the message.

To Login, please click the link below:

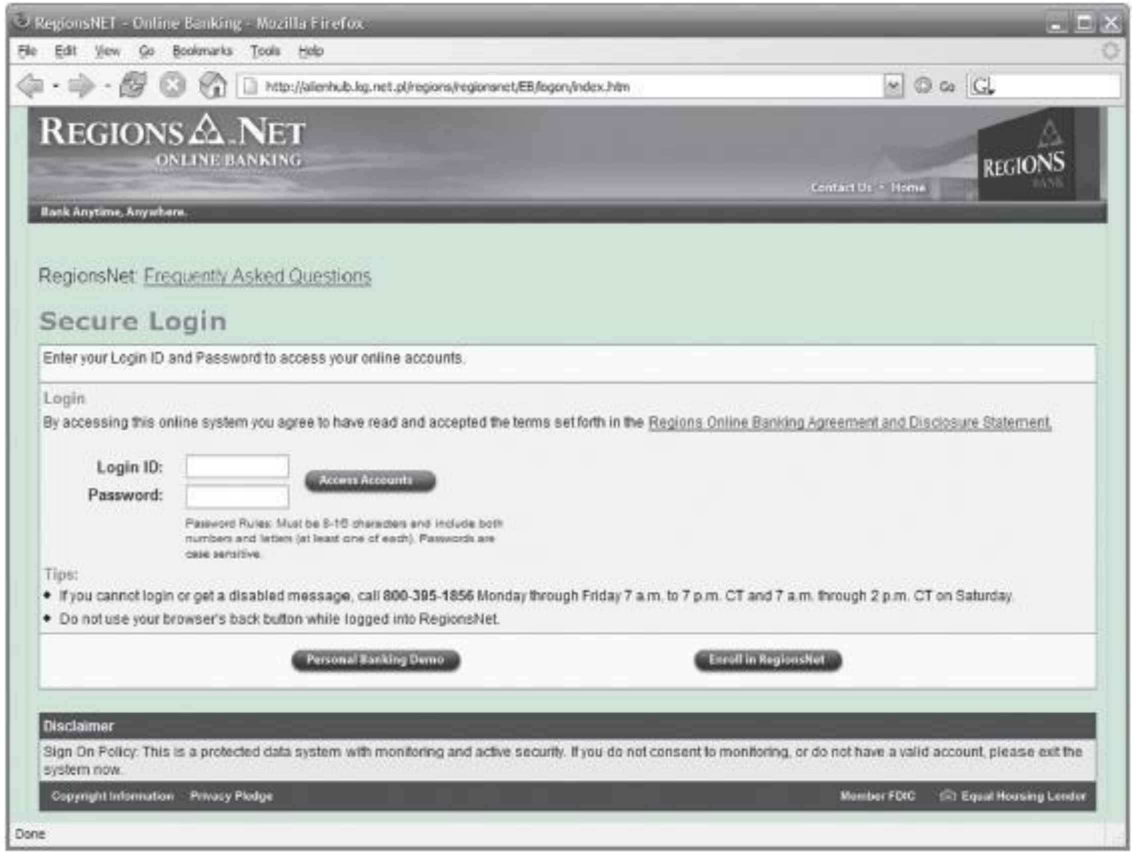
Go To RegionsNet Online

© 2007 Regions Bank. All rights reserved

Figure 2-10 Phishing example: lure

Pharming Example: Fake Website

Pharming is a malicious website that resembles a legitimate website, used to gather usernames and passwords.



RegionsNet: Frequently Asked Questions

Secure Login

Enter your Login ID and Password to access your online accounts.

Login

By accessing this online system you agree to have read and accepted the terms set forth in the Regions Online Banking Agreement and Disclosure Statement.

Login ID:

Password:

Password Rules: Must be 8-16 characters and include both numbers and letters (at least one of each). Passwords are case sensitive.

Tips:

- If you cannot login or get a disabled message, call **800-395-1856** Monday through Friday 7 a.m. to 7 p.m. CT and 7 a.m. through 2 p.m. CT on Saturday.
- Do not use your browser's back button while logged into RegionsNet.

Disclaimer

Sign On Policy: This is a protected data system with monitoring and active security. If you do not consent to monitoring, or do not have a valid account, please exit the system now.

Figure 2-11 Phishing example: fake Web site

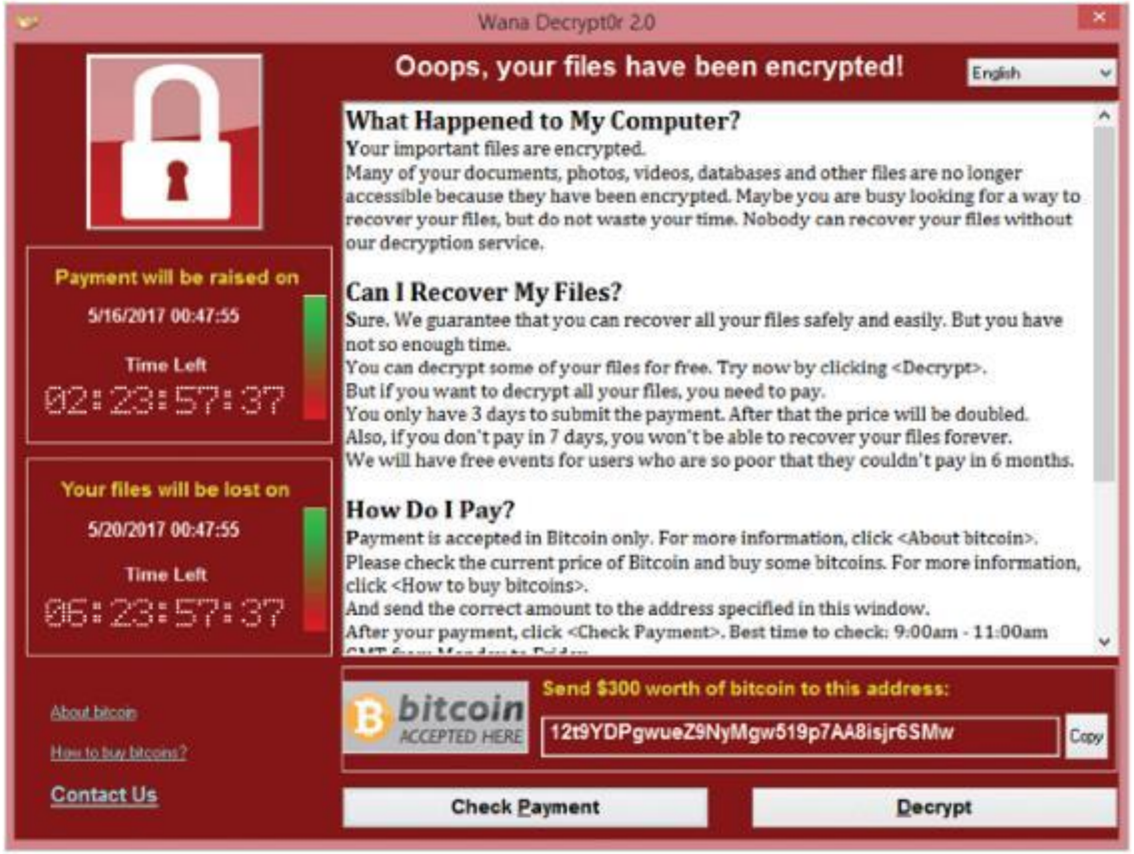
Information Extortion

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

Ransomware

- Ransomware is a malware attack on the host system that **denies access** to the user and then offers to provide a key to allow access back to the user's system and data for a fee.
- There are two types of ransomware: **lockscreen** and **encryption**.
- Common phishing mechanisms to get a user to download ransomware include pop-ups indicating that illegal information or malware was detected on the user's system, threatening to notify law enforcement, or offering to delete the offending material if the user clicks a link or button.

Ransomware Notification Screen



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Figure 2-13 Ransomware notification screen

Sabotage or Vandalism

- Threats can range from petty (minor) vandalism to organized sabotage.
- Web site damaging can erode (wear away) consumer confidence, diminishing an organization’s sales, net worth, and reputation.
- Threat of **hacktivist** or **cyberactivist** operations is rising.
- **Cyberterrorism/cyberwarfare**: a much more sinister form of hacking

Software Attacks (1 of 5)

- **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.
- When an attack makes use of malware that is not yet known by the antimalware software companies, it is said to be a **zero-day attack**.

Software Attacks (2 of 5)

- 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
    - Polymorphic threat: actually evolves to elude (escape) detection
    - Virus and worm hoaxes (tricks): ***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 (3 of 5)

- 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 a 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.

The Most Dangerous Malware Attacks to Date (1 of 2)

Malware	Type	Year	Estimated Number of Systems Infected	Estimated Financial Damage
CIH, a.k.a. Chernobyl	Memory-resident virus	1998	Unknown	$250 million
Melissa	Macro virus	1999	Unknown	$300 million to $600 million
ILOVEYOU	Virus	2000	10% of Internet	$5.5 billion
Klez (and variants)	Virus	2001	7.2% of Internet	$19.8 billion
Code Red (and CR II)	Worm	2001	400,000 servers	$2.6 billion
Nimda	Multivector worm	2001	Unknown	Unknown
Sobig F	Worm	2003	1 million	$3 billion
SOL Slammer, a.k.a. Sapphire	Worm	2003	75,000	$950 million to $1.2 billion

The Most Dangerous Malware Attacks to Date (2 of 2)

Malware	Type	Year	Estimated Number of Systems Infected	Estimated Financial Damage
MyDoom	Worm	2004	2 million	$38 billion
Sasser	Worm	2004	500,000 to 700,000	Unknown
Nesky	Virus	2004	Less than 100,000	Unknown
Storm Worm	Trojan horse virus	2006	10 million	Unknown
Leap-A/Oompa-A	Virus	2006	Unknown (Apple)	Unknown
Conficker	Worm	2009	15 million	Unknown
Stutznet	Worm	2009	~200,000	Unknown

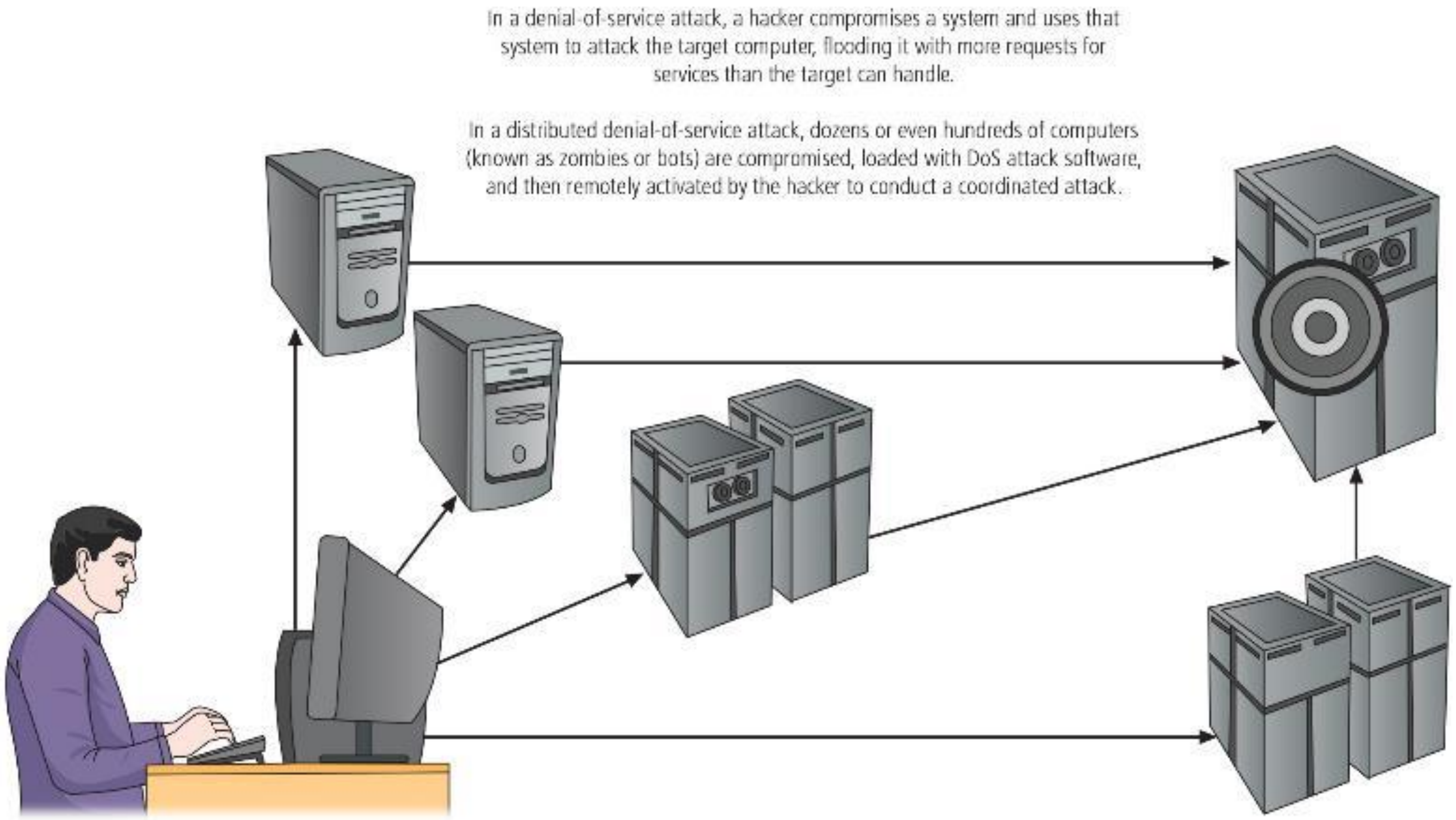
Attack Replication Vectors (1 of 2)

Vector	Description
IP scan and attack	The infected system scans a range of IP addresses and service ports and targets 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 infectious, including .html, .asp, .cgi, and other files. Users who browse to those pages infect their machines.
Virus	Each affected machine infects common executable or script files on all computers to which it can write, which spreads the virus code to cause further infection.
Unprotected shares	Using vulnerabilities in file systems and in the way many organizations configure them, the infected machine copies the viral component to all locations it can reach.

Attack Replication Vectors (2 of 2)

Vector	Description
Mass mail	By sending e-mail infections to addresses found in the address book, the affected machine infects many other users, whose mail-reading programs automatically run the virus program and infect even more systems.
Simple Network Management Protocol (SNMP)	SNMP is used for remote management of network and computer devices. By using the widely known and common passwords that were employed in early versions of this protocol, the attacking program can gain control of the device. Most vendors have closed these vulnerabilities with software upgrades.

Denial-of-Service Attacks



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 or bots) are compromised, loaded with DoS attack software, and then remotely activated by the hacker to conduct a coordinated attack.

Figure 2-16 Denial-of-service attacks

Software Attacks (4 of 5)

- Types of attacks (cont’d)
  - Mail bombing (also a DoS): An attacker routes large quantities of e-mail to a target to overwhelm the receiver.
  - Spam (unsolicited commercial e-mail): It is considered more a annoyance than an attack, though it is emerging as a vector for some attacks.
  - Packet sniffer: It monitors data traveling over a 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; an intruder assumes a trusted IP address.

Spam, Sniffing, Spoofing

- **Spam** is unsolicited email, instant messages, or social media messages. These messages are fairly easy to spot and can be damaging if you open or respond.
- **Sniffing** takes place when an attacker collects data packets that pass over a network by utilizing packet sniffers and data traffic in the network.
- **Spoofing** describes a criminal who impersonates another individual or organization (by using its IP address), with the intent to gather personal or business information.

IP Spoofing Attack

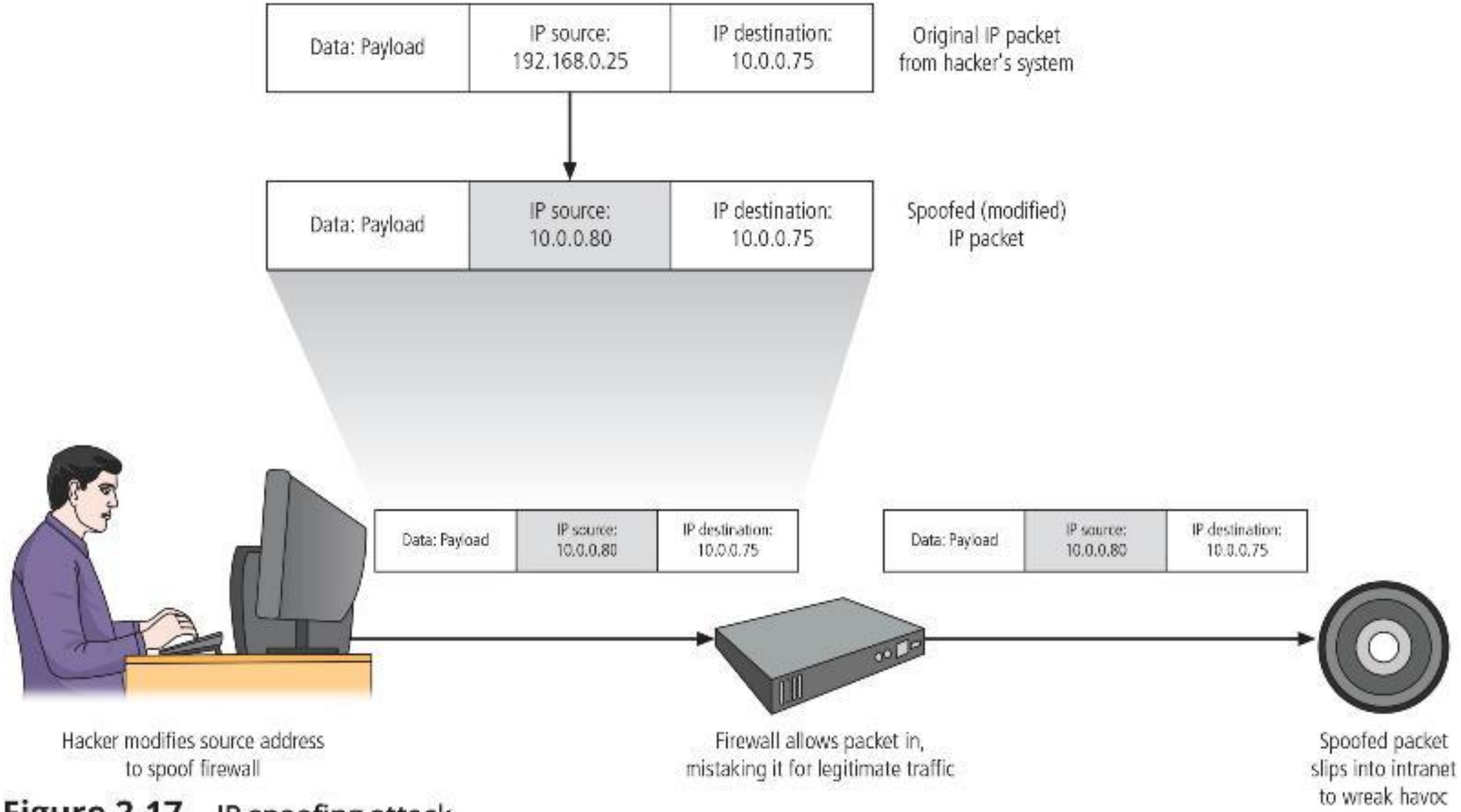
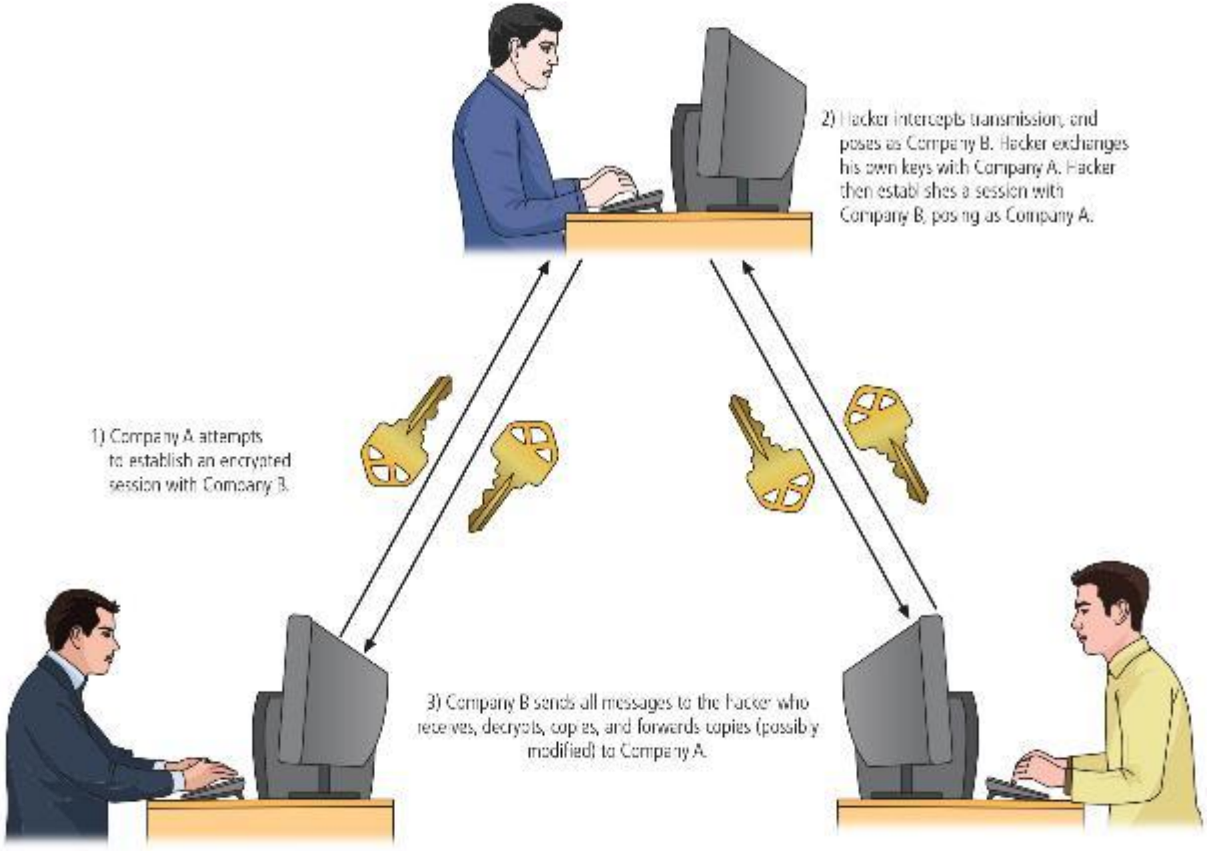

Data: Payload
IP source: 192.168.0.25
IP destination: 10.0.0.75
Original IP packet from hacker's system
Data: Payload
IP source: 10.0.0.80
IP destination: 10.0.0.75
Spoofed (modified) IP packet
Data: Payload
IP source: 10.0.0.80
IP destination: 10.0.0.75
Data: Payload
IP source: 10.0.0.80
IP destination: 10.0.0.75
Hacker modifies source address to spoof firewall
Firewall allows packet in, mistaking it for legitimate traffic
Spoofed packet slips into intranet to wreak havoc

Figure 2-17 IP spoofing attack

Software Attacks (5 of 5)

- 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.
  - Pharming: The redirection of legitimate Web traffic (e.g., browser requests) 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.
  - Phishing: An attempt to gain personal or financial information from an individual, usually by posing as a legitimate entity.

Man-in-the-Middle Attack



1) Company A attempts to establish an encrypted session with Company B.

2) Hacker intercepts transmission, and poses as Company B. Hacker exchanges his own keys with Company A. Hacker then establishes a session with Company B, posing as Company A.

3) Company B sends all messages to the hacker who receives, decrypts, copies, and forwards copies (possibly modified) to Company A.

Figure 2-18 Man-in-the-middle attack

Knowledge Check Activity 3

Communications interception attacks include all of the following EXCEPT _____.

a. sniffers

b. spoofing

c. pharming

d. ransomware

e. man-in-the-middle

Knowledge Check Activity 3: Answer

Communications interception attacks include all of the following EXCEPT _____.

Answer: c. ransomware

Each of the others involves using the communication network or procedures as a means of attack. Ransomware uses encryption of the victim’s data as a means to extort payment.

Technical Hardware Failures or Errors (1 of 2)

- 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, while others are intermittent.
- Intel Pentium CPU failure is a notable example.
- **Mean time between failure** and **annualized failure rates** measure hardware failure rates.

Technical Hardware Failures or Errors (2 of 2)

- 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 (1 of 3)

- Common failures in software development:
  - SQL injection
  - Web server-related vulnerabilities (XSS, XSRF, and response splitting)
  - Web client-related vulnerability (XSS)
  - Use of magic URLs and hidden forms
  - Buffer overrun
  - Format string problems
  - Integer bugs (overflows/underflows)
  - C++ catastrophes

The Deadly Sins in Software Security (2 of 3)

- Common failures in software development:
  - Catching exceptions
  - Command injection
  - Failure to handle errors
  - Information leakage
  - Race conditions
  - Poor usability
  - Not updating easily
  - Executing code with too much privilege

The Deadly Sins in Software Security (3 of 3)

- Common failures in software development:
  - Failure to protect stored data
  - Sins of mobile code
  - Use of weak password-based systems
  - Weak random numbers
  - Using cryptography incorrectly
  - Failure to protect network traffic
  - Improper use of PKI, especially SSL
  - Trusting network name resolution
  - Neglecting change control

Technological Obsolescence

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

Theft

- It is the 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.

Summary (1 of 4)

- Information security performs four important functions:
  - Information security performs four important functions to ensure that information assets remain safe and useful: protecting the organization’s ability to function, enabling the safe operation of applications implemented on the organization’s IT systems, protecting the data an organization collects and uses, and safeguarding the organization’s technology assets.
  - To make sound decisions about information security, management must be informed about threats to its people, applications, data, and information systems, and the attacks they face.
  - Threats are any events or circumstances that have the potential to adversely affect operations and assets. An attack is an intentional or unintentional act that can damage or otherwise compromise information and the systems that support it. A vulnerability is a potential weakness in an asset or its defensive controls.

Summary (2 of 4)

- Threats or dangers facing an organization’s people, information, and systems fall into the following categories:
  - Compromises to intellectual property—Intellectual property, such as trade secrets, copyrights, trademarks, or patents, are intangible assets that may be attacked via software piracy or the exploitation of asset protection controls.
  - Deviations in quality of service—Organizations rely on services provided by others. Losses can come from interruptions to those services.
  - Espionage or trespass—Asset losses may result when electronic and human activities breach the confidentiality of information.
  - Forces of nature—A wide range of natural events can overwhelm control systems and preparations to cause losses to data and availability.
  - Human error or failure—Losses to assets may come from intentional or accidental actions by people inside and outside the organization.

Summary (3 of 4)

- Threats or dangers facing an organization’s people, information, and systems fall into the following categories:
  - Information extortion—Stolen or inactivated assets may be held hostage to extract payment of ransom.
  - Sabotage or vandalism—Losses may result from the deliberate sabotage of a computer system or business, or from acts of vandalism. These acts can either destroy an asset or damage the image of an organization.
  - Software attacks—Losses may result when attackers use software to gain unauthorized access to systems or cause disruptions in systems availability.
  - Technical hardware failures or errors—Technical defects in hardware systems can cause unexpected results, including unreliable service or lack of availability.

Summary (4 of 4)

- Threats or dangers facing an organization’s people, information, and systems fall into the following categories:
  - Technical software failures or errors—Software used by systems may have purposeful or unintentional errors that result in failures, which can lead to loss of availability or unauthorized access to information.
  - Technological obsolescence—Antiquated or outdated infrastructure can lead to unreliable and untrustworthy systems that may result in loss of availability or unauthorized access to information.
  - Theft—Theft of information can result from a wide variety of attacks.

Self-Assessment

- Consider this statement:
  - “When security needs and business needs collide, business needs win out.”
- Do you think there are times and circumstances when this is not completely true? When might that be?
- If you are working in the area of information security, what does this statement indicate about how you should work with other units in the organization?