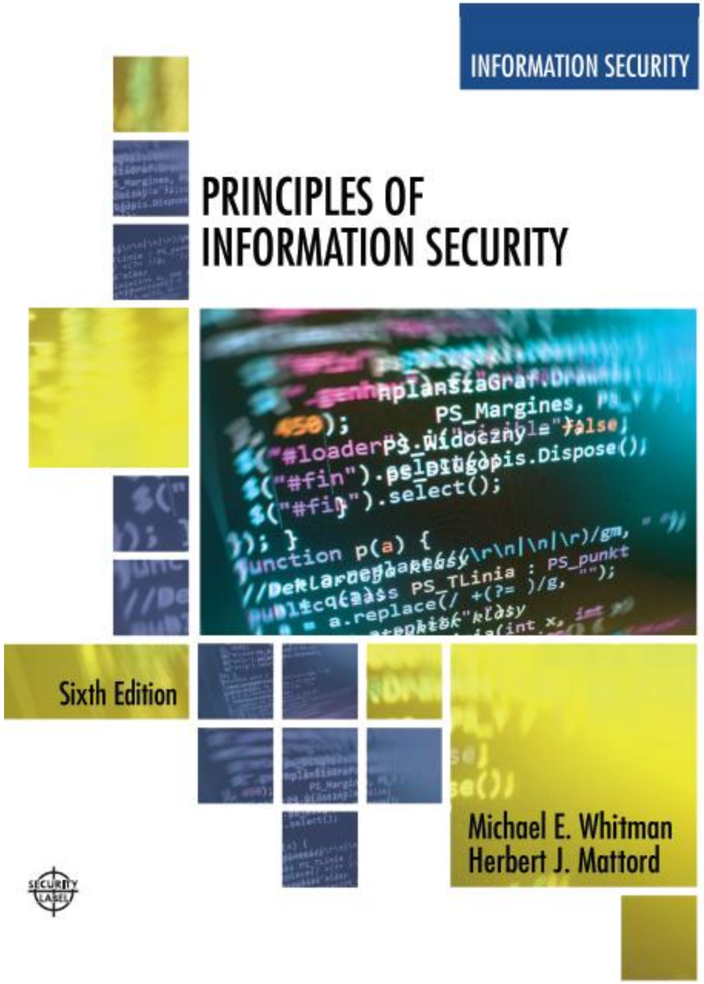
Principles of Information Security

Sixth Edition



Chapter 2

The Need for Security

Learning Objectives

- Upon completion of this material, you should be able to:
  - Discuss the organizational need for information security
  - Explain why a successful information security program is the shared responsibility of an organization’s three communities of interest
  - List and describe the threats posed to information security and common attacks associated with those threats
  - List the common development failures and errors that result from poor software security efforts

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.

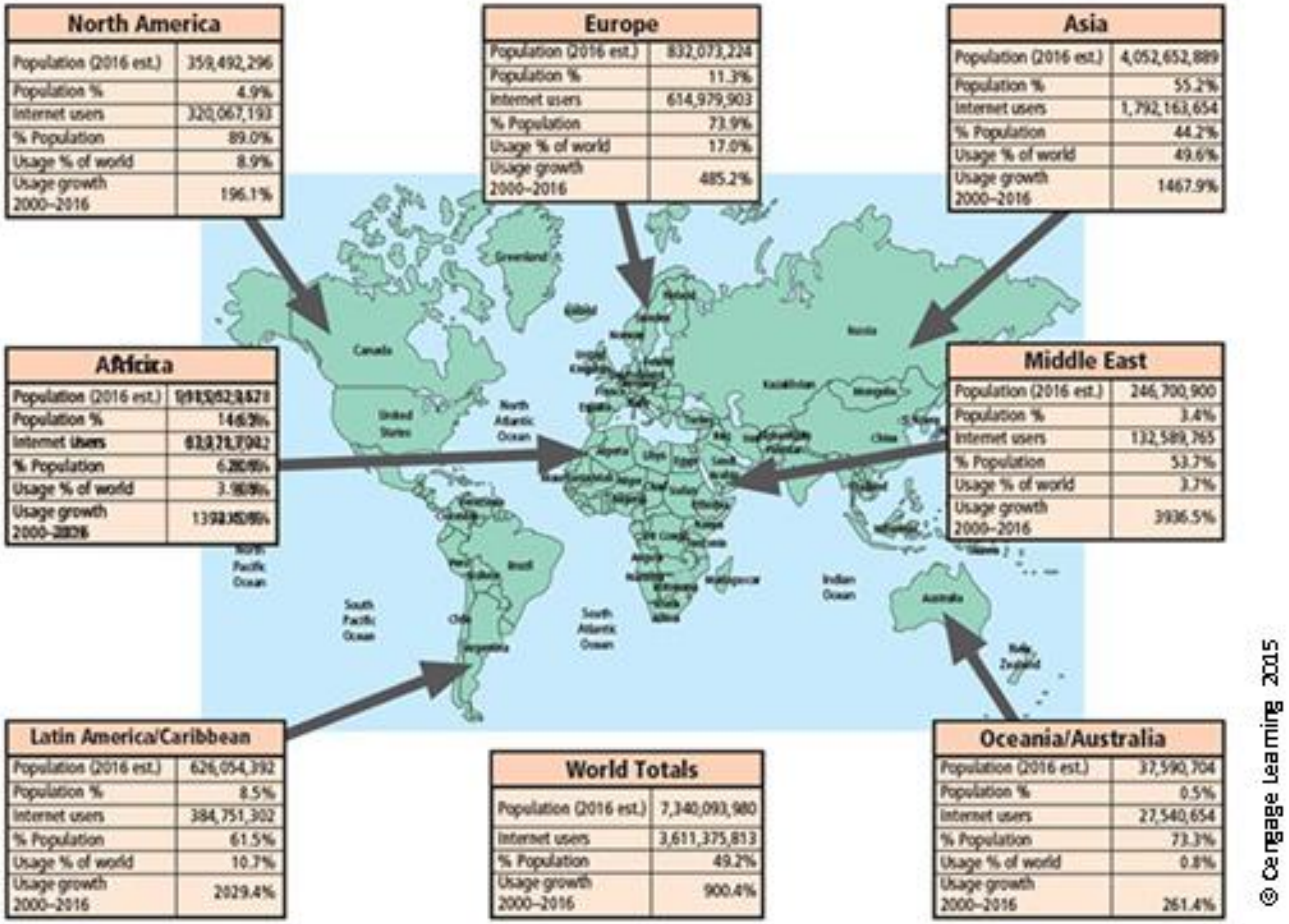
Safeguarding Technology Assets in Organizations

- 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 and Attacks

- 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).
- Management must be informed about the various threats to an organization's people, applications, data, and information systems.
- Overall security is improving, but so is the number of potential hackers.

Figure 2-1 World Internet usage



North America	
Population (2016 est.)	359,492,296
Population %	4.9%
Internet users	320,067,193
% Population	89.0%
Usage % of world	8.9%
Usage growth 2000–2016	196.1%

Europe	
Population (2016 est.)	832,073,224
Population %	11.3%
Internet users	614,979,903
% Population	73.9%
Usage % of world	17.0%
Usage growth 2000–2016	485.2%

Asia	
Population (2016 est.)	4,052,652,889
Population %	55.2%
Internet users	1,792,163,654
% Population	44.2%
Usage % of world	49.6%
Usage growth 2000–2016	1467.9%

Afficica	
Population (2016 est.)	[illegible]
Population %	[illegible]
Internet users	[illegible]
% Population	[illegible]
Usage % of world	[illegible]
Usage growth 2000–2016	[illegible]

Middle East	
Population (2016 est.)	246,700,900
Population %	3.4%
Internet users	132,589,765
% Population	53.7%
Usage % of world	3.7%
Usage growth 2000–2016	3936.5%

Latin America/Caribbean	
Population (2016 est.)	626,054,392
Population %	8.5%
Internet users	384,751,302
% Population	61.5%
Usage % of world	10.7%
Usage growth 2000–2016	2029.4%

World Totals	
Population (2016 est.)	7,340,093,980
Internet users	3,611,375,813
% Population	49.2%
Usage growth 2000–2016	900.4%

Oceania/Australia	
Population (2016 est.)	37,590,704
Population %	0.5%
Internet users	27,540,654
% Population	73.3%
Usage % of world	0.8%
Usage growth 2000–2016	261.4%

© Cengage Learning 2015

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

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)	(new category)		
Laptop/ mobile hardware theft/loss	34%	42%	47%	49%	55%	60%
Bots/zombies in organization	29%	20%	(new category)	(new category)		
Inside abuse of internet access or e-mail	25%	44%	42%	59%	78%	79%
Denial of service	17%	21%	25%	39%	40%	27%

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

Type of Attack or Misuse	**2010/11**	**2008**	**2006**	**2004**	**2002**	**2000**
Unauthorized access or privilege escalation by insider	13%	15%	(revised category)	(revised category)		
Password sniffing	11%	9%	(new category)	(new category)		
System penetration by outsider	11%		(revised category)	(revised category)		
Exploit of client web browser	10%		(new category)	(new category)		

Source: Whitman and Mattord, 2015 SEC/CISE Threats to Information Protection Report.

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

From Employees or Internal Stakeholders	Not a Threat 1	2	3	4	A Severe Threat 5	Comp. Rank
Inability/unwillingness to follow established policy	6.6%	17.2%	33.6%	26.2%	16.4%	66%
Disclosure due to insufficient training	8.1%	23.6%	29.3%	25.2%	13.8%	63%
Unauthorized access or escalation of privileges	4.8%	24.0%	31.2%	31.2%	8.8%	63%
Unauthorized information collection/data sniffing	6.4%	26.4%	40.0%	17.6%	9.6%	60%
Theft of on-site organizational information assets	10.6%	32.5%	34.1%	12.2%	10.6%	56%
Theft of mobile/laptop/tablet and related/connected information assets	15.4%	29.3%	28.5%	17.9%	8.9%	55%
Intentional damage or destruction of information assets	22.3%	43.0%	18.2%	13.2%	3.3%	46%

CENGAGE Learning

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

From Employees or Internal Stakeholders	Not a Threat 1	2	3	4	A Severe Threat 5	Comp. Rank
Theft or misuse of organizationally leased, purchased, or developed software	29.6%	33.6%	21.6%	10.4%	4.8%	45%
Web site defacement	43.4%	33.6%	16.4%	4.9%	1.6%	38%
Blackmail of information release or sales	43.5%	37.1%	10.5%	6.5%	2.4%	37%

Table 2-3 Rated Threats from External Sources in 2015 SEC/CISE Survey of Threads to Information Protection (1 of 2)

From Employees or Internal Stakeholders	Not a Threat 1	2	3	4	A Severe Threat 5	Comp. Rank
Unauthorized information collection/data sniffing	6.4%	14.4%	21.6%	32.8%	24.8%	71%
Unauthorized access or escalation of privileges	7.4%	14.0%	26.4%	31.4%	20.7%	69%
Web site defacement	8.9%	23.6%	22.8%	26.8%	17.9%	64%
Intentional damage or destruction of information assets	14.0%	32.2%	18.2%	24.8%	10.7%	57%
Theft of mobile/laptop/tablet and related/connected information assets	20.5%	25.4%	26.2%	15.6%	12.3%	55%
Theft of on-site organizational informational assets	21.1%	24.4%	25.2%	17.9%	11.4%	55%
Blackmail of information release or sales	31.1%	30.3%	14.8%	14.8%	9.0%	48%
Disclosure due to insufficient training	34.5%	21.8%	22.7%	13.4%	7.6%	48%

Table 2-3 Rated Threats from External Sources in 2015 SEC/CISE Survey of Threads to Information Protection (2 of 2)

From Employees or Internal Stakeholders	Not a Threat 1	2	3	4	A Severe Threat 5	Comp. Rank
Inability/unwillingness to follow established policy	33.6%	29.4%	18.5%	6.7%	11.8%	47%
Theft or misuse of organizationally leased, purchased, or developed software	31.7%	30.1%	22.8%	9.8%	5.7%	46%

Table 2-4 Perceived Threats to Information Assets in 2015 SEC/CISE Survey of Threats to Information Protection (1 of 4)

General Threats to Information Assets	Not a Threat 1	2	3	4	A Severe Threat 5	Comp. Rank
Electronic phishing/spoofing attacks	0.8%	13.1%	16.4%	32.0%	37.7%	79%
Malware attacks	1.7%	12.4%	27.3%	36.4%	22.3%	73%
Unintentional employee/insider mistakes	2.4%	17.1%	26.8%	35.8%	17.9%	70%
Loss of trust due to information loss	4.1%	18.9%	27.0%	22.1%	27.9%	70%
Software failures or errors due to unknown vulnerabilities in externally acquired software	5.6%	18.5%	28.2%	33.9%	13.7%	66%
Social engineering of employees/insiders based on social media information	8.1%	14.6%	32.5%	34.1%	10.6%	65%
Social engineering of employees/insiders based on other published information	8.9%	19.5%	24.4%	32.5%	14.6%	65%
Software failures or errors due to poorly developed, internally created applications	7.2%	21.6%	24.0%	32.0%	15.2%	65%

Table 2-4 Perceived Threats to Information Assets in 2015 SEC/CISE Survey of Threats to Information Protection (2 of 4)

General Threats to Information Assets	Not a Threat 1	2	3	4	A Severe Threat 5	Comp. Rank
SQL injections	7.6%	17.6%	31.9%	29.4%	13.4%	65%
Social engineering of employees/insiders based on organization's Web sites	11.4%	19.5%	23.6%	31.7%	13.8%	63%
Denial of service (and distributed DoS) attacks	8.2%	23.0%	27.9%	32.8%	8.2%	62%
Software failures or errors due to known vulnerabilities in externally acquired software	8.9%	23.6%	26.8%	35.8%	4.9%	61%
Outdated organizational software	8.1%	28.2%	26.6%	26.6%	10.5%	61%
Loss of trust due to representation as source of phishing/spoofing attack	9.8%	23.8%	30.3%	23.0%	13.1%	61%
Loss of trust due to Web defacement	12.4%	30.6%	31.4%	19.8%	5.8%	55%
Outdated organizational hardware	17.2%	34.4%	32.8%	12.3%	3.3%	50%

Table 2-4 Perceived Threats to Information Assets in 2015 SEC/CISE Survey of Threats to Information Protection (3 of 4)

General Threats to Information Assets	Not a Threat 1	2	3	4	A Severe Threat 5	Comp. Rank
Outdated organizational data format	18.7%	35.8%	26.8%	13.8%	4.9%	50%
Inability/unwillingness to establish effective policy by management	30.4%	26.4%	24.0%	13.6%	5.6%	48%
Hardware failures or errors due to aging equipment	19.5%	39.8%	24.4%	14.6%	1.6%	48%
Hardware failures or errors due to defective equipment	17.9%	48.0%	24.4%	8.1%	1.6%	46%
Deviations in quality of service from other provider	25.2%	38.7%	25.2%	7.6%	3.4%	45%
Deviations in quality of service from data communications provider/ISP	26.4%	39.7%	23.1%	7.4%	3.3%	44%
Deviations in quality of service from telecommunication provider/ISP (if different from data provider)	29.9%	38.5%	18.8%	9.4%	3.4%	44%

Table 2-4 Perceived Threats to Information Assets in 2015 SEC/CISE Survey of Threats to Information Protection (4 of 4)

General Threats to Information Assets	Not a Threat 1	2	3	4	A Severe Threat 5	Comp. Rank
Loss due to other natural disaster	31.0%	37.9%	23.3%	6.9%	0.9%	42%
Loss due to fire	26.2%	49.2%	21.3%	3.3%	0.0%	40%
Deviations in quality of service from power provider	36.1%	43.4%	12.3%	5.7%	2.5%	39%
Loss due to flood	33.9%	43.8%	19.8%	1.7%	0.8%	38%
Loss due to earthquake	41.7%	35.8%	15.0%	6.7%	0.8%	38%

Table 2-5 The 12 Categories of Threats to Information Security

Category of Threat	Attack Examples
Compromises to intellectual property	Piracy, copyright infringement
Deviations in equality 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 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.

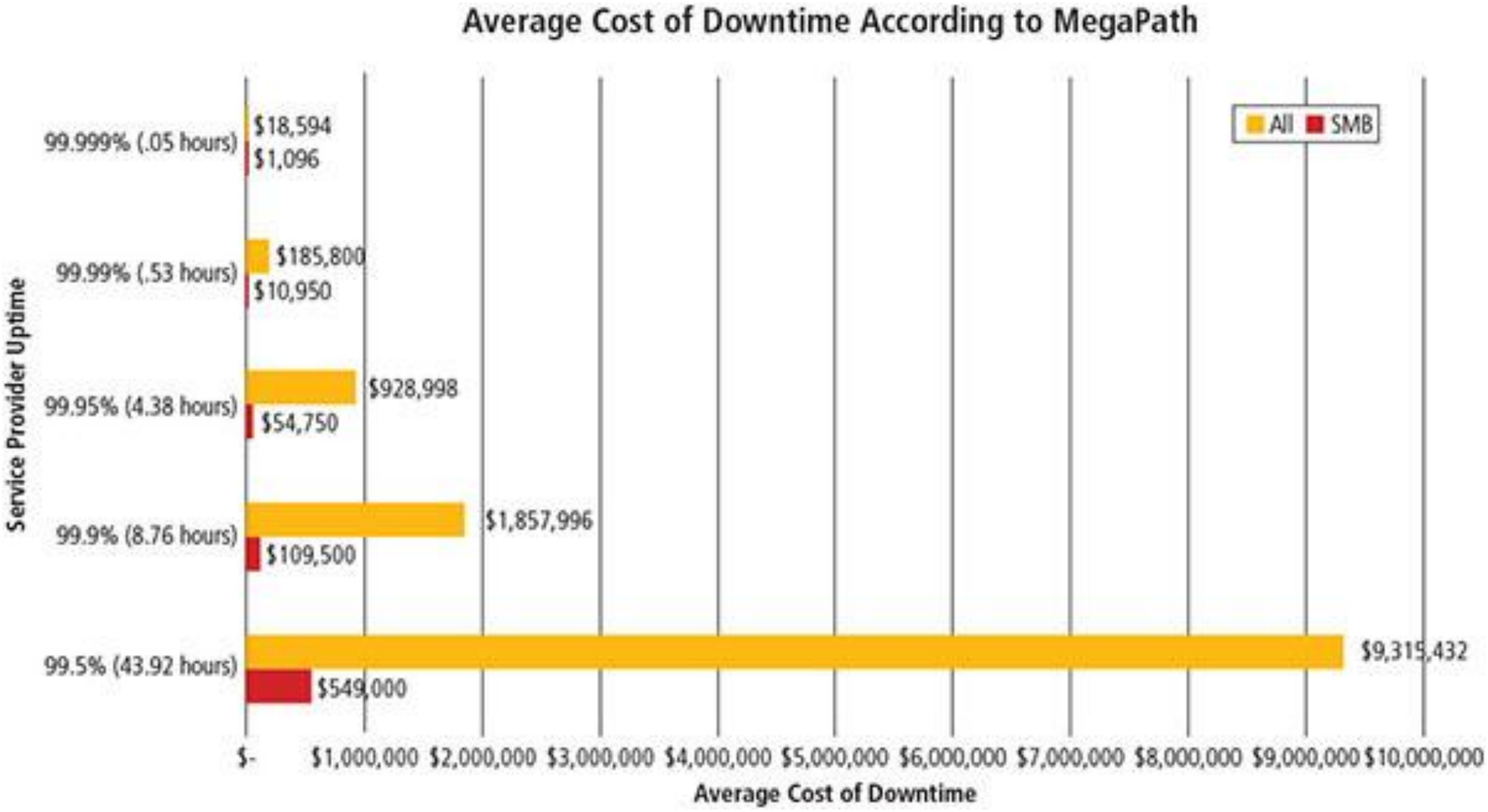
Deviations in Quality of Service (1 of 2)

- 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.
- 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.

Deviations in Quality of Service (2 of 2)

- 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.
- Power irregularities
  - Are 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

Figure 2-5 Cost of online service provider downtime



Source: MegaPath. Used with permission.

Espionage or Trespass (1 of 3)

- 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

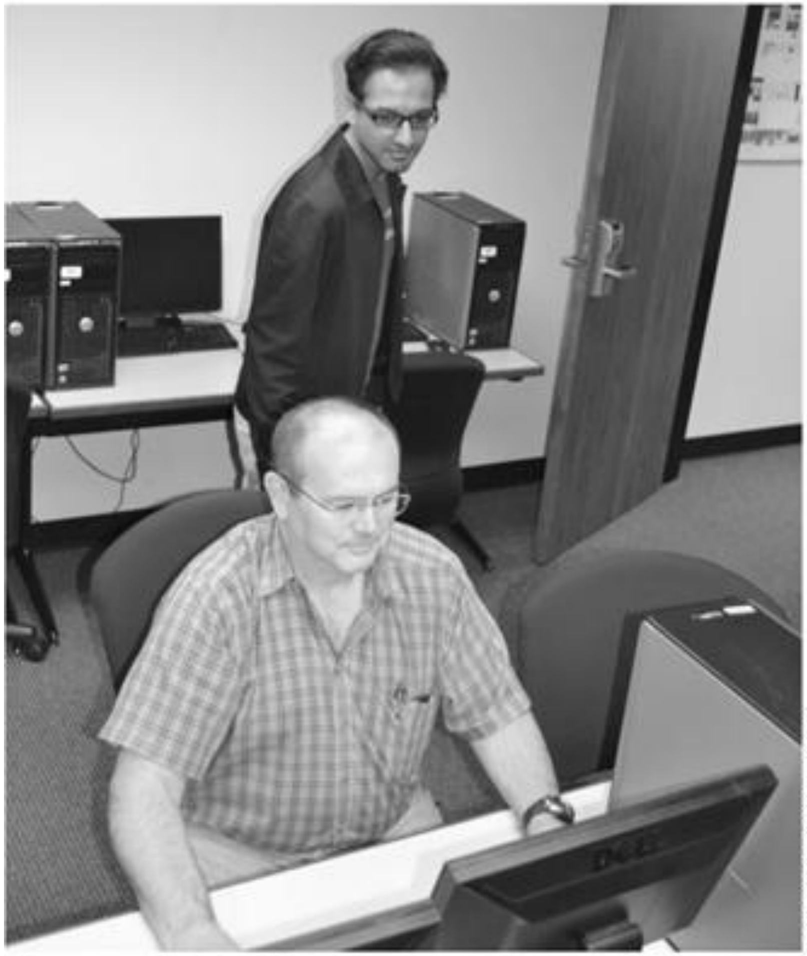
Espionage or Trespass (2 of 3)

- Expert hackers
  - Develop software scripts and program exploits
  - Usually a master of many skills
  - 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

Espionage or Trespass (3 of 3)

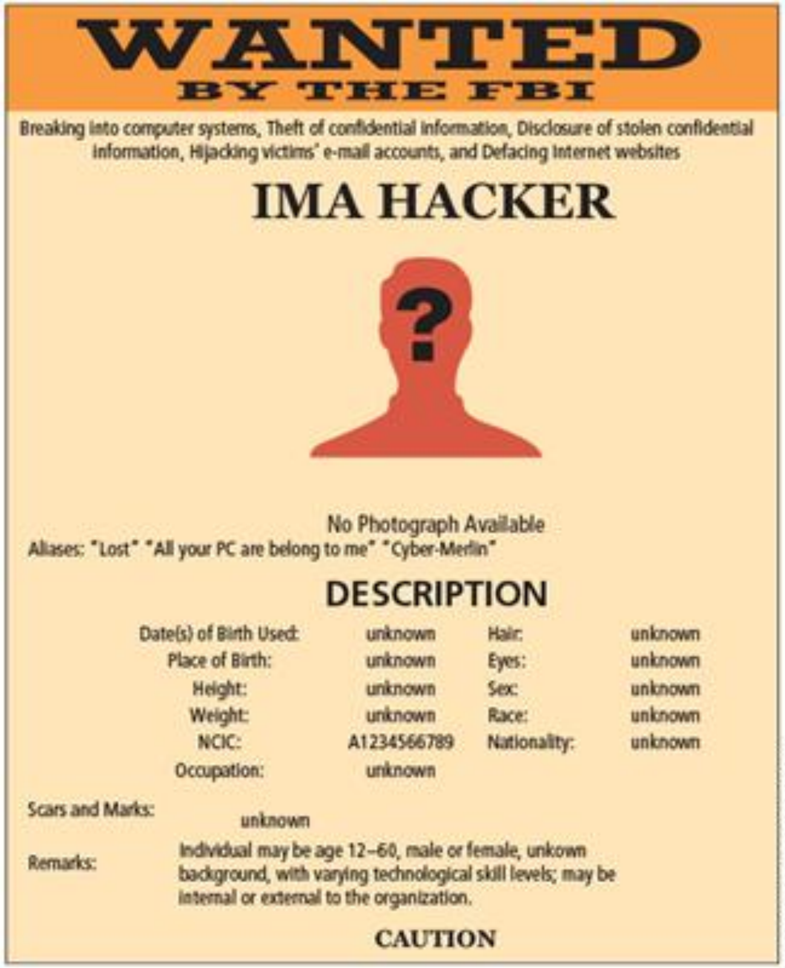
- Other terms for system rule breakers:
  - Cracker: “cracks” or removes software protection designed to prevent unauthorized duplication
  - Phreaker: hacks the public telephone system to make free calls or disrupt services
- Password attacks
  - Cracking
  - Brute force
  - Dictionary
  - Rainbow tables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

Figure 2-6 Shoulder surfing



© Cengage Learning 2015

Figure 2-7 Contemporary 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

© Cengage Learning 2015

Table 2-6 Password Power (1 of 2)

Case-Insensitive Passwords Using a Standards Alphabet Set (No Numbers or Special Characters)		
Password Length	**Odd of cracking: 1 in (Based on Numbers of Characters ^ Password length):**	**Estimated Time to Crack***
8	208,827,064,576	1.01 seconds
9	5,429,503,678,976	26.2 seconds
10	141,167,095,653,376	11.4 minutes
11	3,670,344,486,987,780	4.9 hours
12	95,428,956,661,682,200	5.3 days
13	2,481,152,873,203,740,000	138.6 days
14	64,509,974,703,297,200,000	9.9years
15	1,677,259,342,285,730,000,000	256.6 years
16	43,608,742,899,428,900,000,000	6,672.9 years

Table 2-6 Password Power (2 of 2)

Case-Sensitive Passwords Using a Standards Alphabet Set (with Numbers and Special Characters)		
Password Length	**Odd of cracking: 1 in (Based on Numbers of Characters ^ Password length):**	**Estimated Time to Crack***
8	2,044,140,858,654,980	2.7 hours
9	167,619,550,409,708,000	9.4 days
10	13,744,803,133,596,100,000	2.1 years
11	1,127,073,856,954,880,000,000	172.5 years
12	92,420,056,270,299,900,000,000	14,141.9 years
13	7,578,444,614,164,590,000,000,000	1,159,633.8 years
14	621,432,458,361,496,000,000,000,000	95,089,967.6 years
15	50,957,461,585,642,700,000,000,000,000	7,797,377,343.5 years
16	4,178,511,850,022,700,000,000,000,000,000	639,384,942,170.1 years

*Estimated Time to crack is based on a 2015-era PC with an intel i7-6700K Quad Core CPU performing 207.23 Dhrystone GIPS (giga/ billion instructions per second) at 4.0 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 (1 of 2)

- 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

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 uses social skills to convince people to reveal access credentials or other valuable information to an attacker

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

Tommy Twostory,
convicted burglar

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

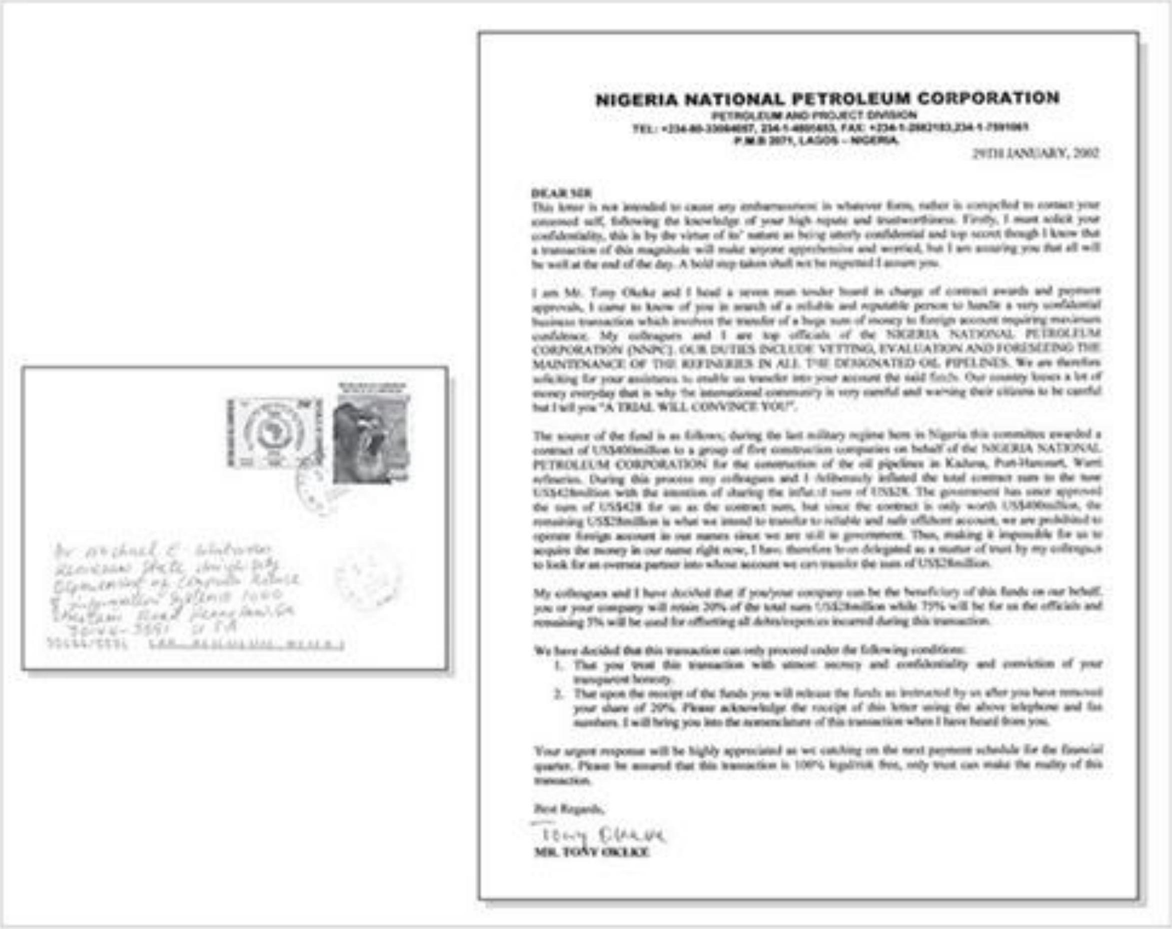
Elite Skillz,
wannabe hacker

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

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

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



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

NIGERIA NATIONAL PETROLEUM CORPORATION
PETROLEUM AND PROJECT DIVISION
TEL: +234-80-33084057, 234-1-4807453, FAX: +234-1-2682183,234-1-7591061
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 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 oversea 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.

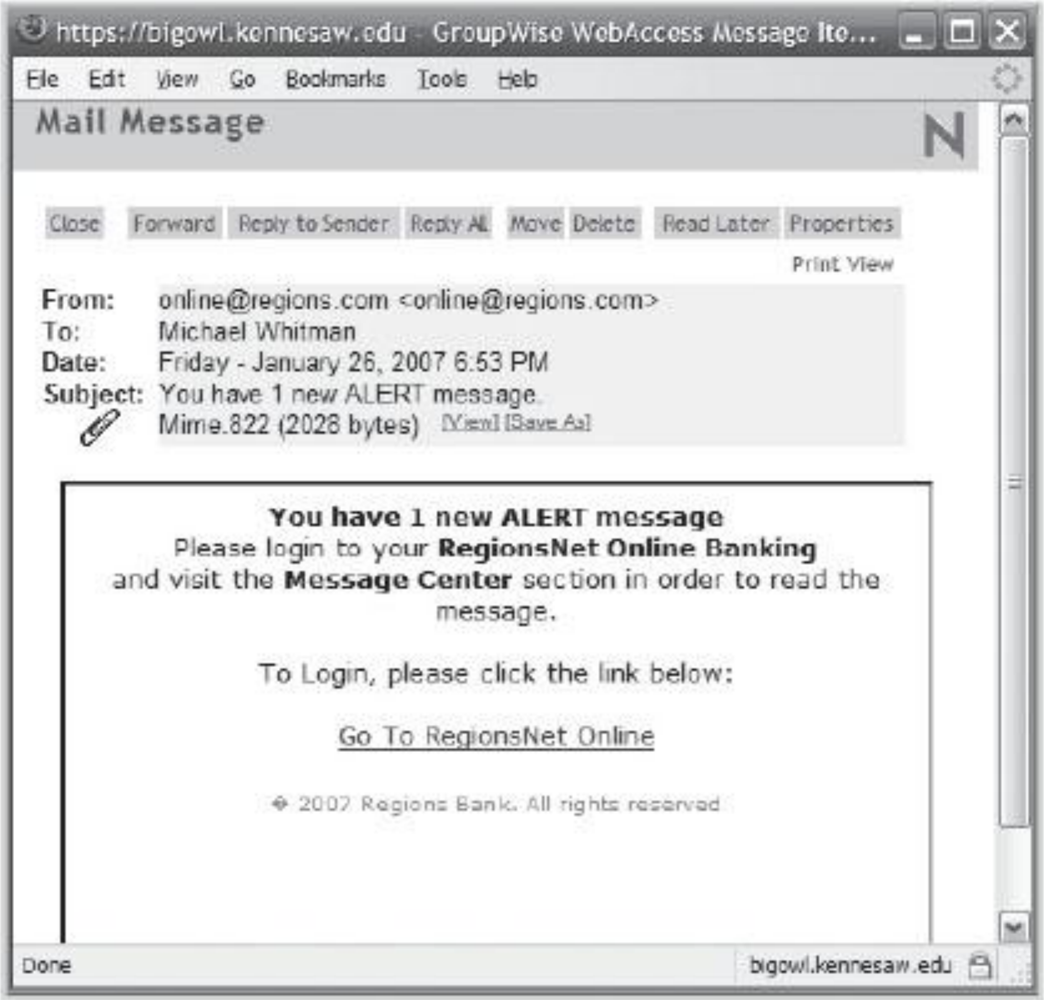
Best Regards,

Tony Okeke
MR. TONY OKEKE

© Cengage Learning 2015

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

Figure 2-11 Phishing example: lure



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)

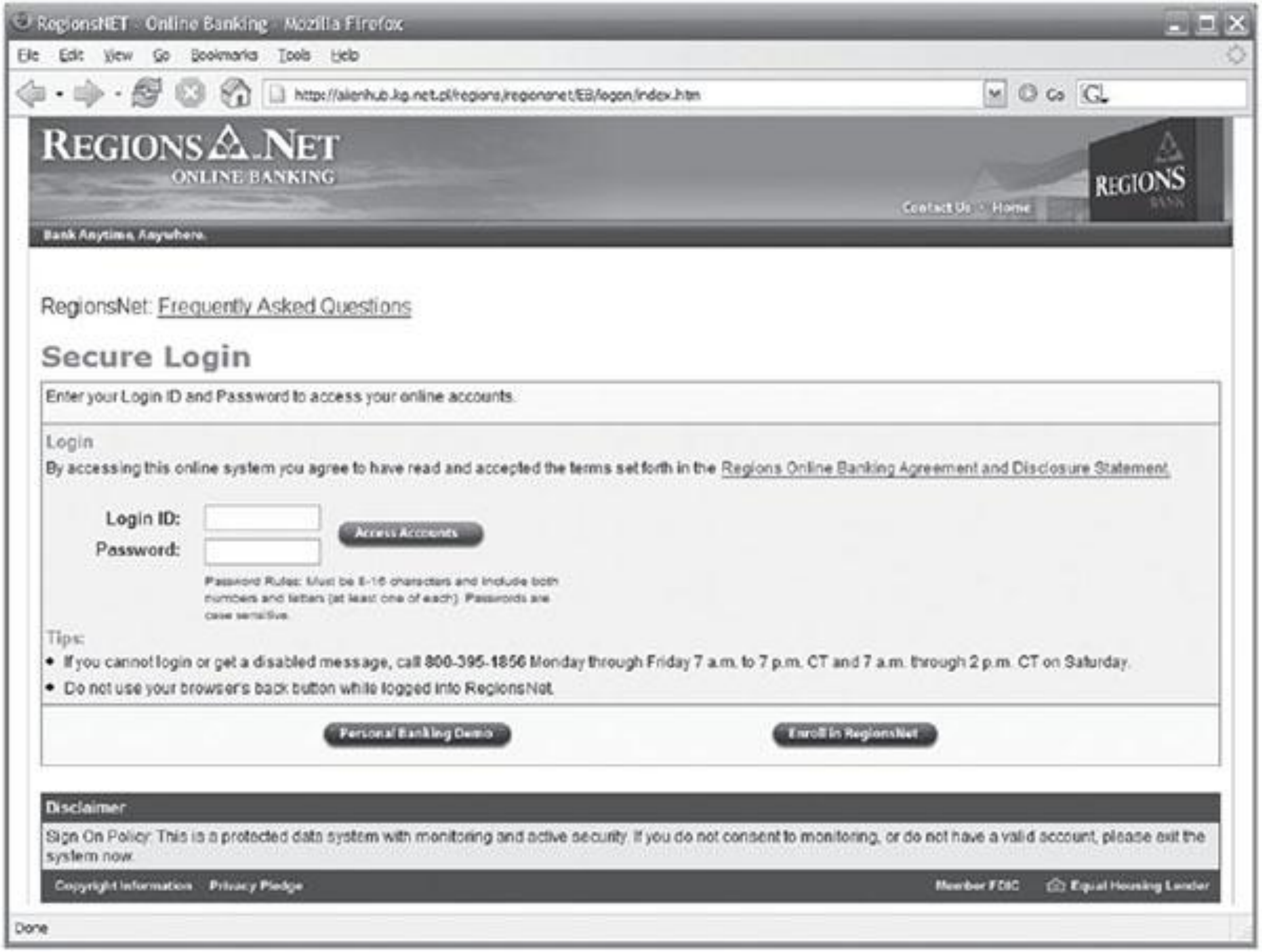
You have 1 new ALERT message
Please login to your **RegionsNet Online Banking**
and visit the **Message Center** section in order to read the message.

To Login, please click the link below:

Go To RegionsNet Online

© 2007 Regions Bank. All rights reserved

Figure 2-12 Phishing example: fake Website



http://alienhub.kg.net.pl/regions/regionsnet/EB/logon/index.htm

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.

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.

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.

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.

Software Attacks (3 of 5)

    - 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
  - 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.

Software Attacks (4 of 5)

- Distributed denial-of-service (DDoS): A coordinated stream of requests is launched against a target from many locations simultaneously.
- 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.

Software Attacks (5 of 5)

- Spoofing: A technique used to gain unauthorized access; intruder assumes a trusted IP address.
- 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.

Table 2-7 The Most Dangerous Malware Attacks to Date (1 of 2)

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

Table 2-7 The Most Dangerous Malware Attacks to Date (2 of 2)

Malware	Type	Year	Estimated Number of Systems Infected	Estimated Financial Damage
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

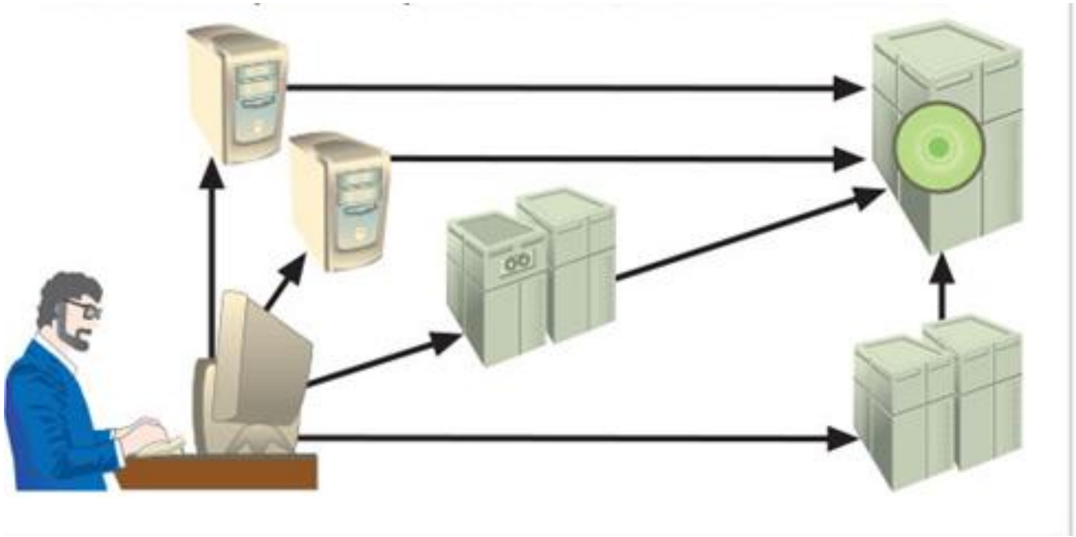
Table 2-8 Attack Replication Vectors

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.
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.

Figure 2-18 Denial-of-service attack

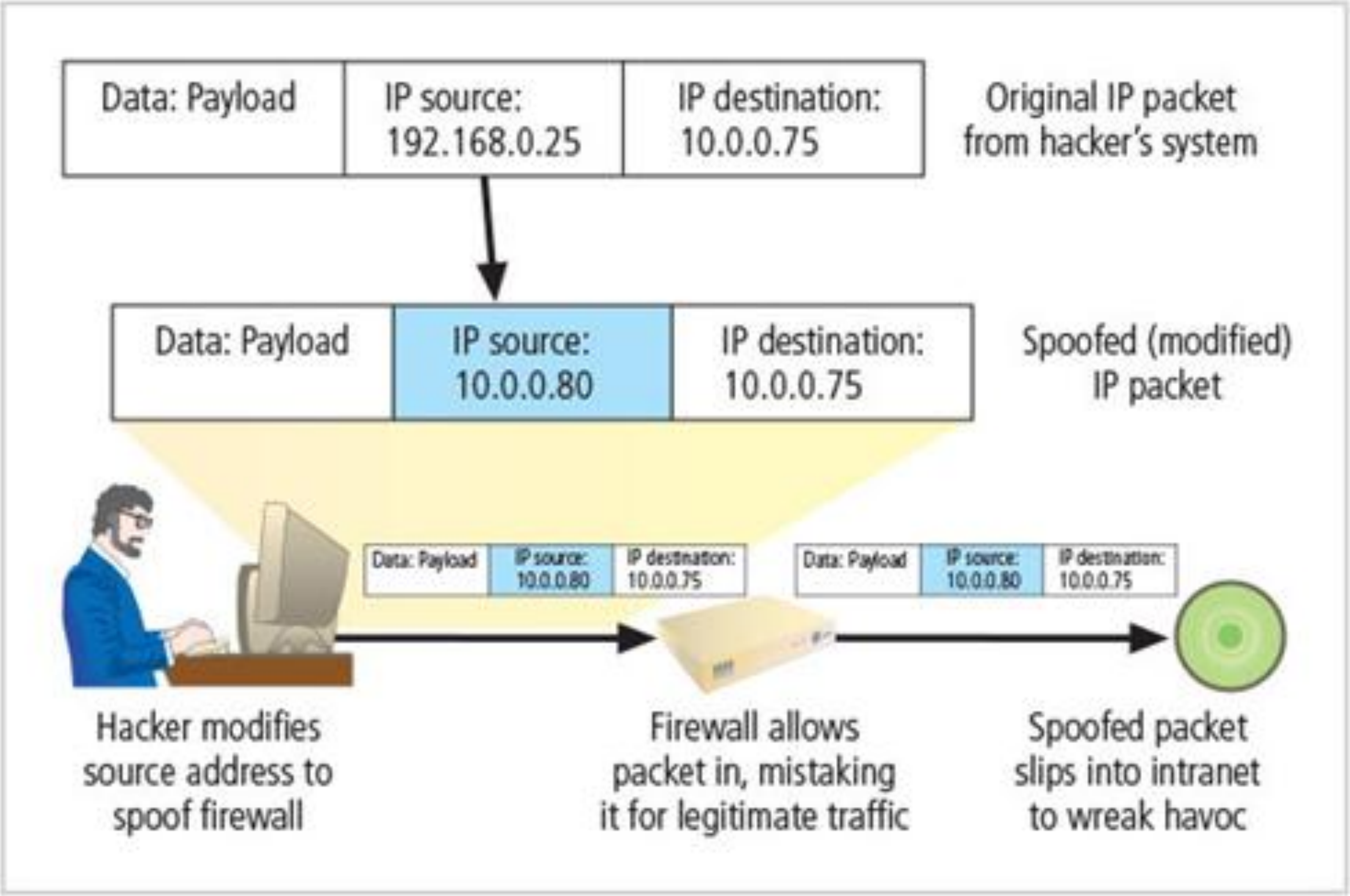
In a denial-of-service attack, a hacker compromises a system and uses that system to attack the target computer, flooding it with more requests for services than the target can handle.

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.



© Cengage Learning 2015

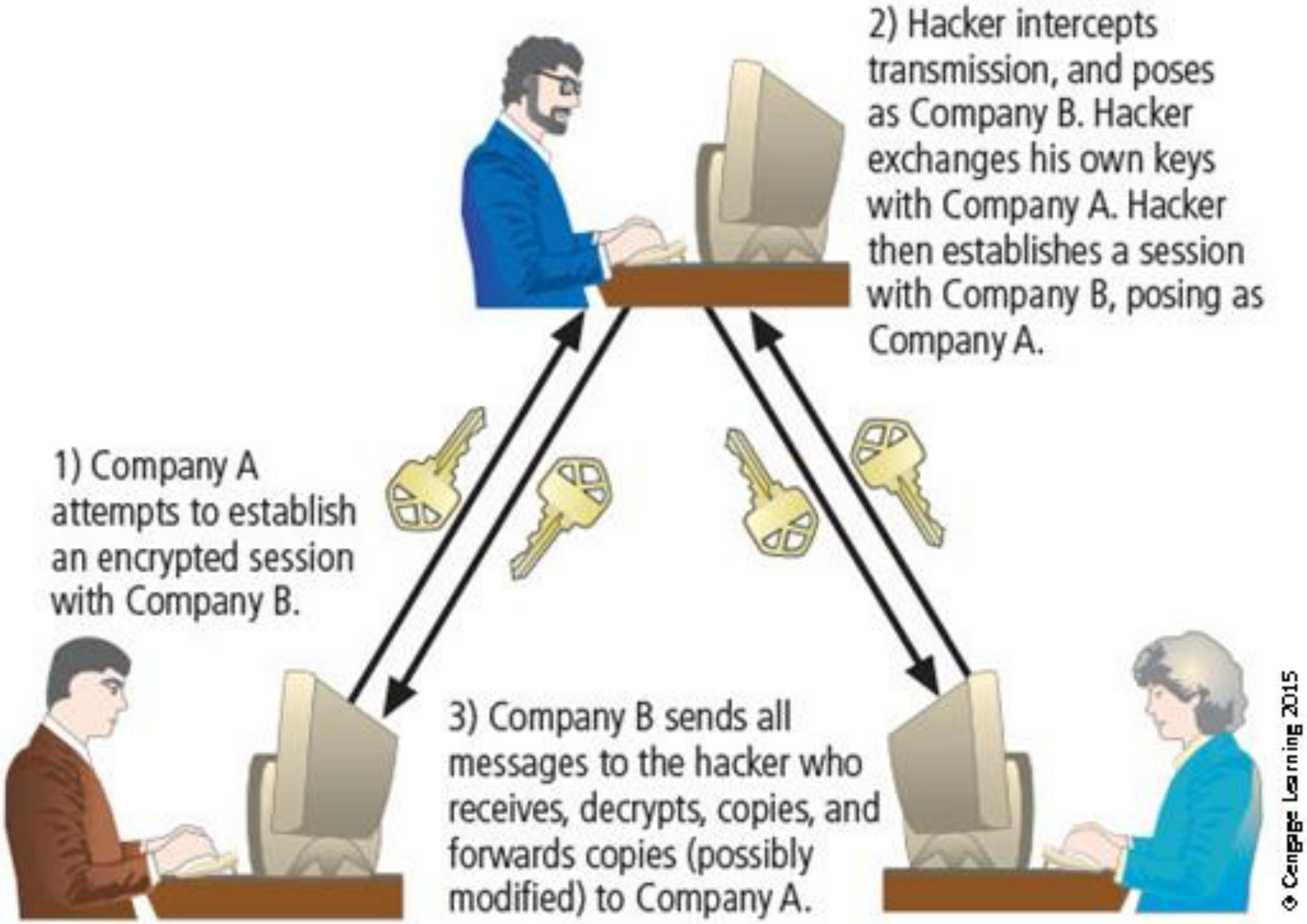
Figure 2-19 IP Spoofing attack



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

© Cengage Learning 2015

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



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.

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

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

© Cengage Learning 2015

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 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 (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:
  - Buffer overruns
  - Catching exceptions
  - 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
  - Format string problems
  - Neglecting change control

The Deadly Sins in Software Security (2 of 3)

- – Improper file access
- – Improper use of Secure Sockets Layer (SSL)
- – Information leakage
- – Integer bugs (overflows/underflows)
- – Race conditions
- – SQL injection

The Deadly Sins in Software Security (3 of 3)

- 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.

Summary (1 of 4)

- Information security performs four important functions:
  - Protecting organization’s ability to function
  - Enabling safe operation of applications implemented on organization’s IT systems
  - Protecting data an organization collects and uses
  - Safeguarding the technology assets in use at the organization
- 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.

Summary (2 of 4)

- 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.
- Information extortion: Stolen or inactivated assets may be held hostage to extract payment of ransom.

Summary (3 of 4)

- 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.
- 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.

Summary (4 of 4)

- 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.