Chapter 10: Securing Information Systems

Having thorough plans and approaches for dealing with IS security attacks and natural disasters is critical for effectively managing IS resources within organizations and your personal life

Chapter 10 Learning Objectives

Computer Crime

- Define computer crime and describe several types of computer crime.

Cyberwar and Cyberterrorism

- Describe and explain the differences between cyberwar and cyberterrorism.

Managing Information Systems Security

- Discuss the process of managing IS security and describe various IS controls that can help in ensuring IS security.

Computer Crime

Computer Crime

- Define computer crime and describe several types of computer crime.

Cyberwar and Cyberterrorism

Describe and explain the differences between cyberwar and cyberterrorism.

Managing Information Systems Security

Discuss the process of managing IS security and describe various IS controls that can help in ensuring IS security.

What Is Computer Crime?

"Using a computer to commit an illegal act"

- Targeting a computer while committing an offense
  - Unauthorized access of a server to destroy data
- Using a computer to commit an offense
  - Using a computer to embezzle funds
- Using computers to support criminal activity
  - Maintaining books for illegal gambling on a computer

Hacking and Cracking

- Hackers
  - Anyone who can gain unauthorized access to computers
  - White hat hackers don't intend to do harm
- Crackers
  - Individuals who break into computer systems with the intent to commit crime or do damage
  - Also called black hat hackers
  - Hacktivists: Crackers who are motivated by political or ideological goals and who use cracking to promote their interests

Malicious hackers are referred to as black hats and those not motivated to do harm are referred to as white hats

Who Commits Computer Crimes?

- Computer criminals come in all shapes and sizes, in order of infractions they are:
  1. Current or former employees; most organizations report insider abuses as their most common crime (CSI, 2011)
  2. People with technical knowledge who commit business or information sabotage for personal gain
  3. Career criminals who use computers to assist in crimes
  4. Outside crackers—commit millions of intrusions per year
- Studies show that only 10% of cracker attacks cause damage

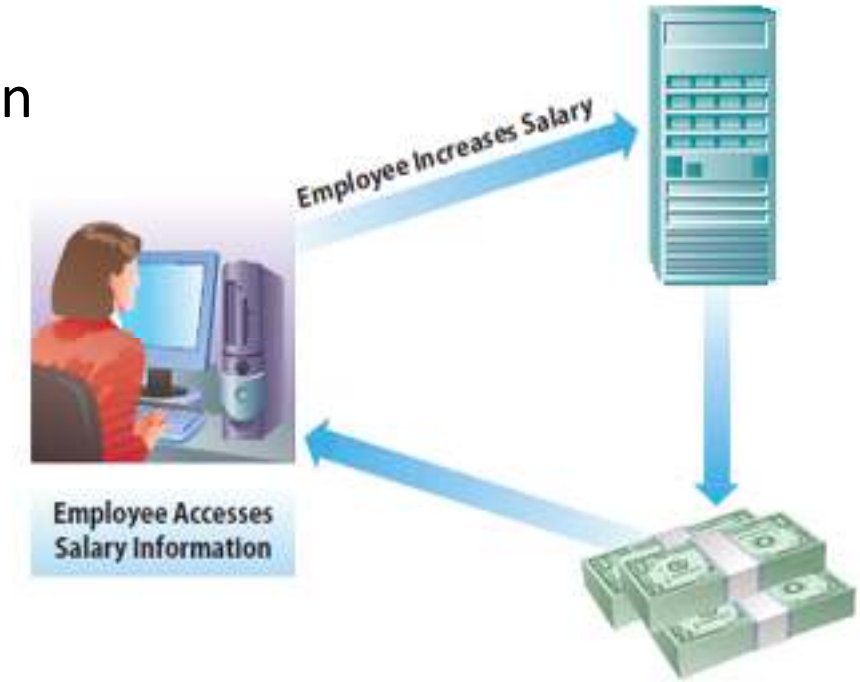
How Do They Do It?

- Technology
  - Vulnerability scanners
  - Packet sniffers
  - Keyloggers
  - Brute force
- Exploiting human weaknesses
  - Phishing
  - Social engineering
  - Shoulder surfing
  - Dumpster diving

Types of Computer Crimes

- Unauthorized Access
  - Stealing information
  - Stealing use of computer resources
  - Accessing systems with the intent to commit information modification
- Information Modification
  - Changing data for financial gain (e.g., embezzlement)
  - Defacing a Web site (e.g., hacktivists making a statement)

An information modification attack.



Insider Threats

- Unauthorized access can occur in many ways
- Some are based on insider threats
  - Disgruntled employees, former employees, contractors
- Edward Snowden is a recent example

Other Threats

Often institutions and individuals fail to exercise proper care and implement effective controls
Passwords and access codes written down on paper, in plain sight or unsecured
Antivirus software isn't installed or isn't maintained
Systems left with default manufacturer passwords in place after being deployed
Information carelessly shared over the phone, or by letting unauthorized individuals see monitor screens
Company files and resources without proper access controls
Failure to install and maintain firewalls and intrusion prevention/detection systems
Poor background checks on new hires
Employees with unmonitored access to data and resources
Fired employees left unmonitored and have access to damage the system before they leave the company

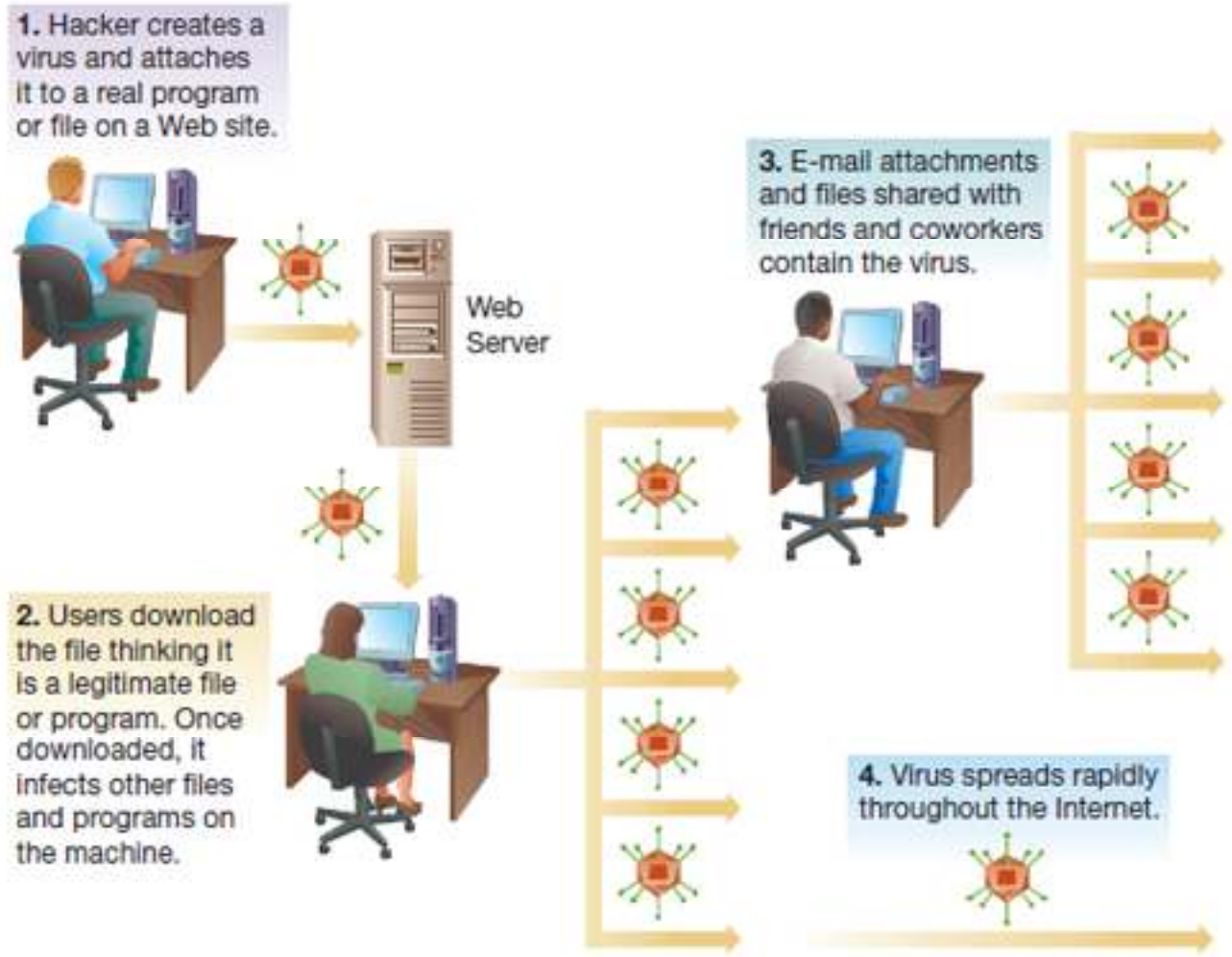
Mobile Threats

With the popularity of mobile devices like smartphones and tablets, many additional security threats have emerged
Individuals lose their mobile devices and don't have capabilities to remotely wipe data from the device
Individuals keep sensitive data on mobile devices and do not use passcodes
Individuals "jailbreaking" their mobile phones
Individuals use poorly designed mobile applications that can have security vulnerabilities
Individuals use unsecure wireless networks, leaving their devices vulnerable to different types of attacks

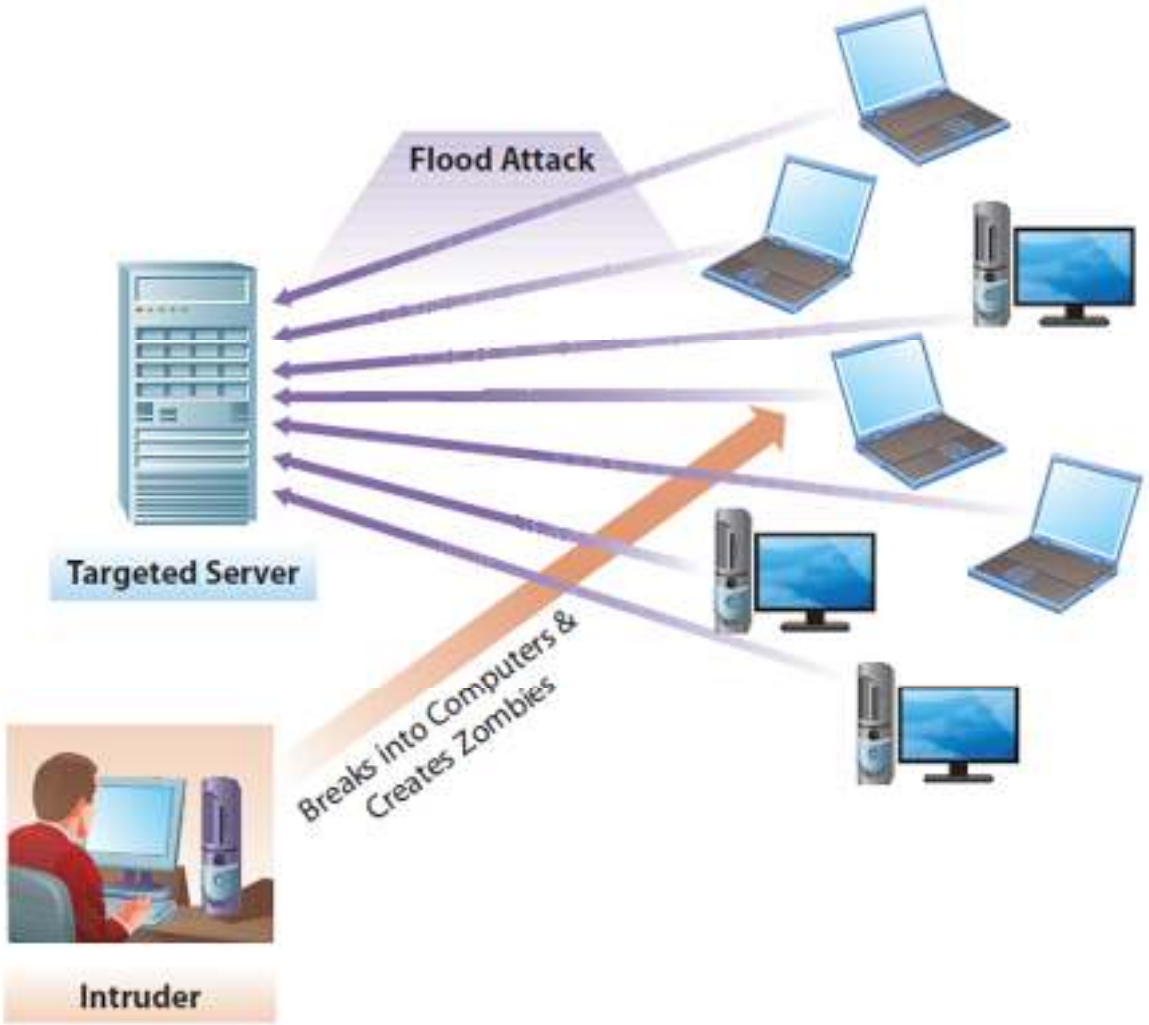
Computer Viruses and Other Destructive Code

- Computer viruses
- Worms, Trojan horses, and other sinister programs
- Denial of service
- Spyware, spam, and cookies
  - *Spyware*
  - *Spam*
  - *Cookies*
- The rise of botnets and the cyberattack supply chain
- Identity theft

Computer Viruses and Other Destructive Code: Viruses



Computer Viruses and Other Destructive Code: Denial-of-Service



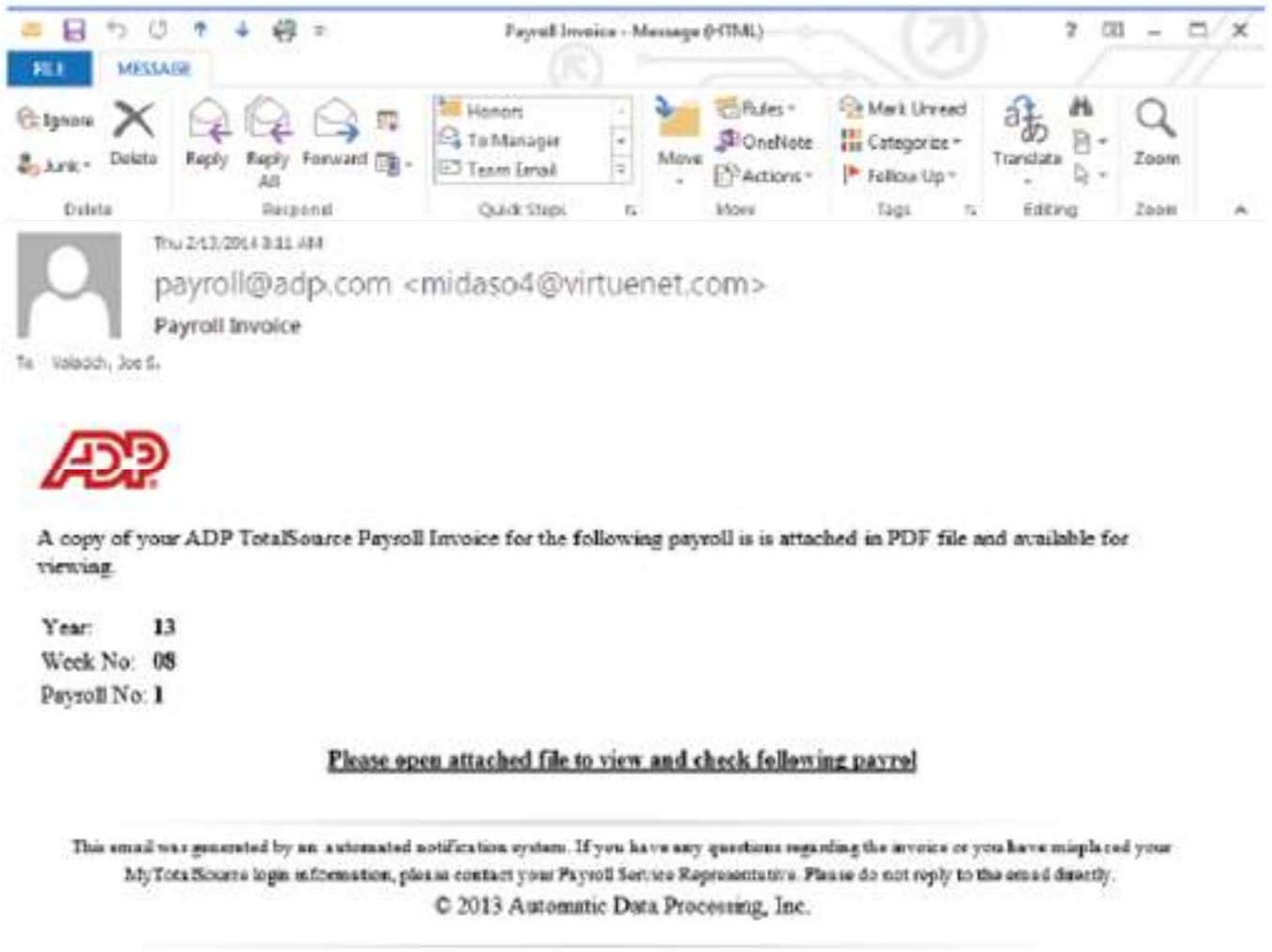
Computer Viruses and Other Destructive Code: Spyware, Spam, and Cookies

- Spyware, Spam, and Cookies
  - *Spyware:* software that monitors the activity on a computer, such as the Web sites visible or even the keystrokes of the user
  - *Spam:* Bulk unsolicited e-mail sent to millions of users at extremely low cost, typically seeking to sell a product, distribute malware, or conduct a phishing attack
  - *Cookies:* A small file Web sites place on a user's computer; can be legitimate (to capture items in a shopping cart) but can be abused (to track individuals' browsing habits) and can contain sensitive information (like credit card numbers) and pose a security risk

Computer Viruses and Other Destructive Code: The Rise of Botnets and the Cyberattack Supply Chain

- Botnets are software robots working together with zombie computers
- 85% of all e-mail spam is sent by only six botnets
- Example phishing attack:
  - A programmer writes a phishing attack template and sells it
  - A phisher purchases the template and designs the attack
  - The phisher contracts with a cracker to host the phishing Web site
  - The phisher contacts a bot herder to sent the botnets
  - The phisher sends the information attained to a collector
  - The collector works with a mule herder to withdraw funds from banks

A Typical Phishing E-mail



Payroll Invoice - Message (HTML)

payroll@adp.com <midaso4@virtuenet.com>

Payroll Invoice

A copy of your ADP TotalSource Payroll Invoice for the following payroll is is attached in PDF file and available for viewing.

Year: 13
Week No: 08
Payroll No: 1

Please open attached file to view and check following payrol

This email was generated by an automated notification system. If you have any questions regarding the invoice or you have misplaced your MyTotalSource login information, please contact your Payroll Service Representative. Please do not reply to the email directly.

© 2013 Automatic Data Processing, Inc.

Identity Theft

- Identity theft is one of the fastest growing information crimes
- Stealing Social Security, credit card, bank account numbers and information
- Possible solutions
  - Government and private sector working together to change practices
  - Use of biometrics and encryption

Source: HenrikS000/Getty Images

Cyberharassment, Cyberstalking, and Cyberbullying

- Cyberharassment
  - Use of a computer to communicate obscene, vulgar, or threatening content that causes a reasonable person to endure distress
- Cyberstalking
  - Tracking an individual, performing harassing acts not otherwise covered by cyberharassment, or inciting others to perform harassing acts
- Cyberbullying
  - Deliberately causing emotional distress
- All three are closely related, a cyberstalker may be committing cyberharassment and cyberbullying

Software Piracy

Region	Piracy Level	Dollar Loss (in US$ millions)
North America Western	19%	10,958
Europe	32%	13,749
Asia/Pacific	60%	20,998
Latin America	61%	7,459
Middle East/Africa	58%	4,159
Eastern Europe	62%	6,133
Worldwide	42%	63,456

Source: Based on Business Software Alliance. (2012). Extracted from unnumbered tables on pages 8–9 from http://portal.bsa.org/globalpiracy2011/downloads/study_pdf/2011_BSA_Piracy_Study-Standard.pdf.

Internet Hoaxes and Cybersquatting

- Internet Hoaxes
  - False messages circulated about topics of interest
  - Users should verify the content of e-mails before forwarding
  - May be used to harvest e-mails for spam mailings
- Cybersquatting
  - Buying and holding a domain name with the intent to sell
  - The 1999 Anti-Cybersquatting Consumer Protection Act makes it a crime if the intent is to profit from the goodwill of a trademark belonging to someone else

Federal Laws

- Federal Laws
  - The Computer Fraud and Abuse Act of 1986
    - A crime to access government computers or communications
    - A crime to extort money by damaging computer systems
    - A crime to threaten the president, vice president, members of Congress, administration officials
  - Electronic Communications Privacy Act of 1986
    - A crime to break into any electronic communications service, including telephone services
    - Prohibits the interception of any type of electronic communications

Cyberwar and Cyberterrorism

Computer Crime

Define computer crime and describe several types of computer crime.

Cyberwar and Cyberterrorism

- Describe and explain the differences between cyberwar and cyberterrorism.

Managing Information Systems Security

Discuss the process of managing IS security and describe various IS controls that can help in ensuring IS security.

Cyberwar

- Cyberwar Vulnerabilities
  - Command-and-control systems
  - Intelligence collection, processing, and distribution systems
  - Tactical communication systems and methods
  - Troop and weapon positioning systems
  - Friend-or-foe identification systems
  - Smart weapons systems

Cyberwar (continued)

- Cyberwar strategy includes controlling Internet-based propaganda
  - Web vandalism
- "Patriot hackers"—governments sometimes blame independent citizens or groups for cyberwar attacks
- Stuxnet—malware against an Iranian system
  - Originally blamed on patriot hackers, then revealed to be developed by the U.S. and Israel

Cyberterrorism

- What kinds of attacks are considered cyberterrorism?
  - Attacks by individuals and organized groups
  - Political, religious, or ideological goals
- How the Internet is changing the business processes of terrorists
  - Terrorists are leveraging the Internet to coordinate their activities, recruit, and perform fundraising

Cyberterrorism (continued)

- Assessing the cyberterrorism threat
  - The Internet is generally open and accessible from anywhere in the world
  - There have been many attacks, and although not significantly damaging, the will and potential exist
- The globalization of terrorism
  - Terrorism is now a global business
  - Attacks can be launched from anywhere in the world

Cyberterrorism (continued)

Types of Cyberterrorism

- Coordinated bomb attacks
- Manipulation of financial and banking information
- Manipulation of the pharmaceutical industry
- Manipulation of transportation control systems
- Manipulation of civilian infrastructures
- Manipulation of nuclear power plants

Terrorist Use of the Internet

- Information dissemination
- Data mining
- Fundraising
- Recruiting and mobilization
- Networking
- Information sharing
- Training
- Planning and coordinating
- Information gathering
- Location monitoring

Managing Information Systems Security

Computer Crime

Define computer crime and describe several types of computer crime.

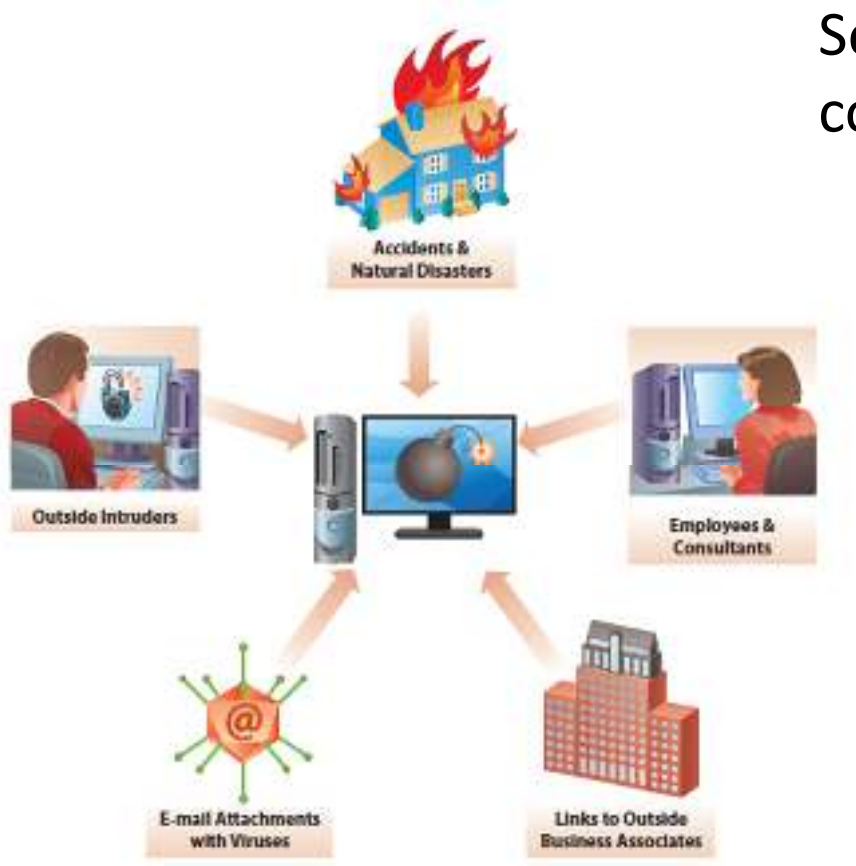
Cyberwar and Cyberterrorism

Describe and explain the differences between cyberwar and cyberterrorism.

Managing Information Systems Security

- Discuss the process of managing IS security and describe various IS controls that can help in ensuring IS security.

Threats to IS Security



Securing against these threats must consider these primary goals:

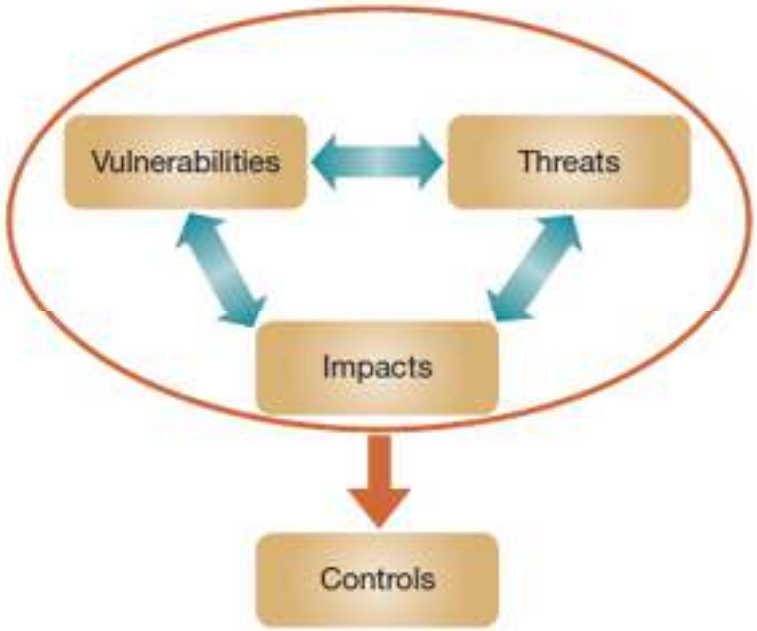
- Availability:
  - Ensuring that legitimate users can access the system
- Integrity
  - Preventing unauthorized manipulations of data and systems
- Confidentiality
  - Protecting data from unauthorized access
- Accountability
  - Ensuring that actions can be traced

The Process of Information Security

Information systems security is an ongoing process.

Assessing IS Risks

- Options for addressing risk
  - Risk Reduction
    - Actively installing countermeasures
  - Risk Acceptance
    - Accepting any losses that occur
  - Risk Transference
    - Have someone else absorb the risk (insurance, outsourcing)
  - Risk Avoidance
    - Using alternative means, avoiding risky tasks



Interplay between threats, vulnerabilities, and impacts

Developing a Security Strategy

- After assessing risk, a strategy is developed detailing the **information security controls**
- Types of controls:
  - Preventive
  - Detective
  - Corrective
- Use the principles of *least permissions* and *least privileges*

Developing a Security Strategy: Policies and Procedures

- Not all security measures are technical in nature. Managerial activities are important
- Policies and procedures include:
  - Information policy
  - Security policy
  - Use policy
  - Backup policy
  - Account management policy
  - Incident handling procedures
  - Disaster recovery plan

Developing a Security Strategy: Disaster Planning

- **Business continuity plan**—how a business continues operating after a disaster
- **Disaster recovery plan**—detailed procedures for recovering from systems-related disasters
- Questions for a disaster recovery plan:
  - What events are considered a disaster?
  - What should be done to prepare the backup site?
  - What is the chain of command; who declares a disaster?
  - What hardware and software are needed?
  - Which personnel are needed?
  - What is the sequence for moving back to the original location?
  - Which providers can be drawn on to aid in disaster recovery?

Developing a Security Strategy: Backups

- Backup sites are critical for business continuity in the event a disaster strikes
- Backup media include CD, external hard drives, and tapes
- Cold backup site—an empty warehouse with all necessary connections for power and communication but nothing else
- Hot backup site—fully equipped backup facility, all needed equipment and one-to-one replication of current data

Developing a Security Strategy: Designing the Recovery Plan

- Recovery time objectives
  - Specify the maximum time allowed to recover from a catastrophic event
  - Minutes, hours, days?
- Recovery point objectives
  - Specify how current the backup data should be
  - Mission-critical transaction data need to be very current
  - Hot backup involves mirrored data

Implementing Controls and Training

- Commonly used controls:
  - Physical access restrictions
  - Firewalls
  - Encryption
  - Virus monitoring and prevention
  - Secure data centers
  - Systems development controls
  - Human controls

Implementing Controls and Training: Physical Access Restrictions

- Physical access controls typically focus on authentication
  - Something you have
    - Keys
    - Smart cards
  - Something you know
    - Password
    - PIN code
  - Something you are
    - Biometrics

A smart card
Source: al62/Fotolia

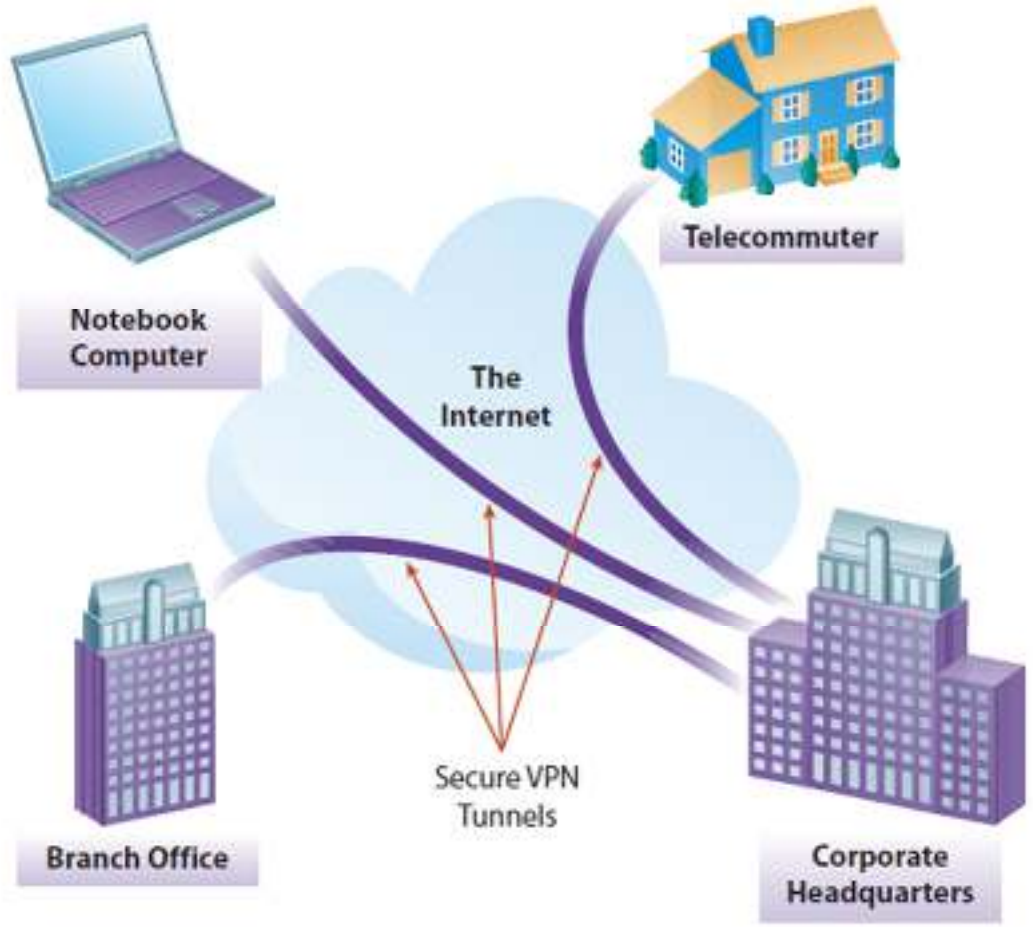
Implementing Controls and Training: Physical Access Restrictions (continued)

- Methods for implementing physical access control
  - Biometrics
    - Identification via fingerprints, retinal patterns in the eye, facial features, or other bodily characteristics
  - Access Control Software
    - Allowing computer users access only to those files related to their work
    - Restricting type of access (read, write, delete, etc.)
  - Wireless LAN (WLAN) Controls
    - Securing wireless networks prevents drive-by hacking
  - Virtual Private Networks(VPN)
    - Also called a secure tunnel

Implementing Controls and Training: Firewalls

- Filter traffic
  - Incoming and/or outgoing traffic
  - Filter based on traffic type
  - Filter based on traffic source
  - Filter based on traffic destination
  - Filter based on combinations of parameters

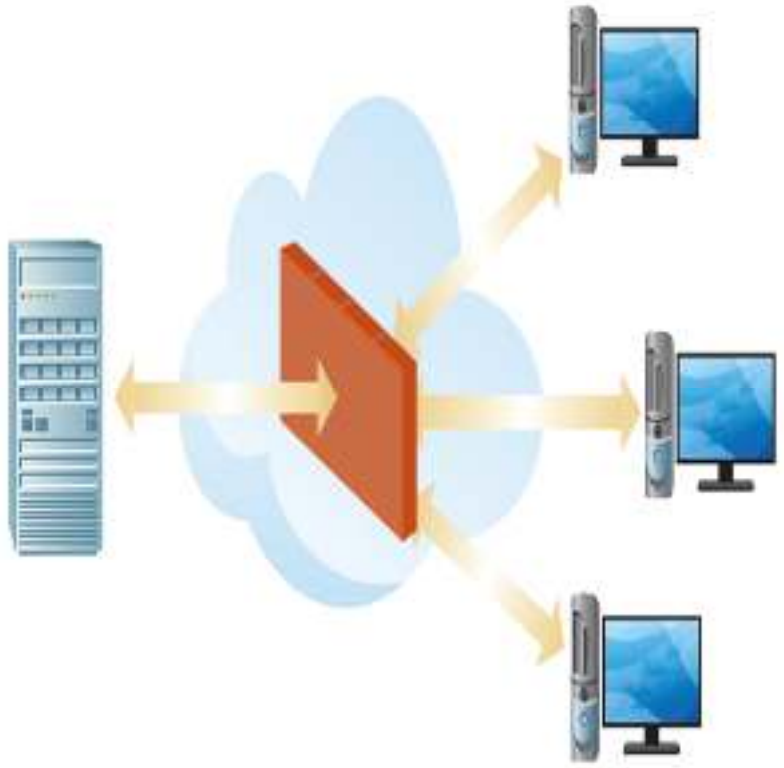
Implementing Controls and Training: Encryption and VPN




```
Ciphertext letters:
JOGPSNBUJPO TZTUFNT UPEBZ
Equivalent plaintext letters:
INFORMATION SYSTEMS TODAY
```

Implementing Controls and Training: Firewalls

- **Firewall**—part of a computer system designed to detect intrusion and prevent unauthorized access to or from a private network
- A “security fence”



Implementing Controls and Training: Virus Monitoring and Prevention

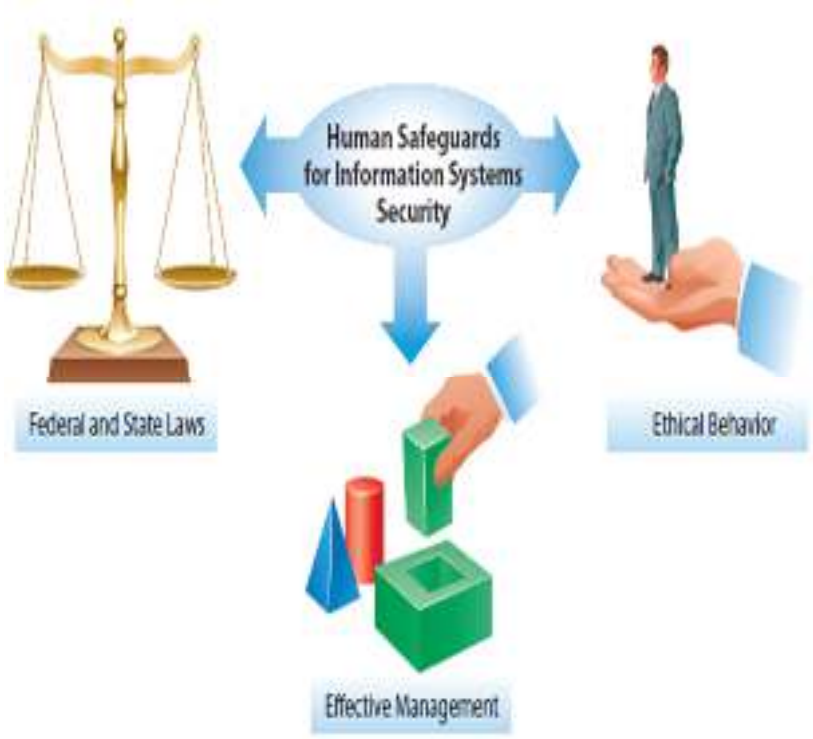
- Standard precautions
  - Purchase, install, and maintain antivirus software
  - Do not use flash drives or shareware from unknown or suspect sources
  - Use reputable sources when downloading material from the Internet
  - Delete without opening any e-mail message received from an unknown source
  - Do not blindly open e-mail attachments, even if they come from a known source
  - If your computer system contracts a virus, report it

Implementing Controls and Training: Secure Data Centers

- Securing the facility's infrastructure
  - Site selection
  - Physical access restrictions
  - Intrusion detection
  - Uninterruptible power supply
  - Protection from environmental threats

Implementing Controls and Training: Other Controls

- System development controls
- Human controls
- Deployment and training



Monitoring Security

- Monitoring external events
  - Information Sharing and Analysis Centers, United States Computer Emergency Readiness Team
- IS Auditing
  - External entity reviews the controls to uncover any potential problems
- Sarbanes-Oxley Act
  - Best practices: Control Objectives for Information and related Technology (COBIT)
- Responding to Security Incidents
- Computer Forensics
  - Examining the computers of crime victims for evidence
  - Auditing computer activity logs

The Sarbanes-Oxley Act

- The Sarbanes-Oxley (S-OX) Act addresses financial controls
  - Companies must demonstrate that controls are in place
  - Companies must preserve evidence documenting compliance
  - Information systems typically used to meet compliance requirements
  - Growing need for IS auditors

The State of IS Security Management

- Information security is a huge management challenge
  - In 2013, malware introduced into Target's point-of-sale system captured the credit card data of 40 million shoppers
- 2013 U.S. State of Cybercrime Security Survey
  - 38 percent of executives indicate lack of good security assessment methodology
  - Greatest security threats from crackers, insiders, and foreign nation-states
  - Insider attacks more costly than external threats
  - Executives use free Internet sites for security information; not necessarily reliable

END OF CHAPTER CONTENT

Managing in the Digital World: Not So "Anonymous"—Activists, Hacktivists, or Just Plain Criminals?

- Anonymous
  - A loose collection of hacktivists
  - Practice civil disobedience by taking part in cyberattacks on Web sites (e.g., WikiLeaks)
  - Politically active: launching attacks on Israeli government for Gaza Strip military actions
  - Well known for Internet vigilantism
  - Claiming to have good intentions, but activities are illegal
  - Dilemma between pursuing ideological goals and crossing the bounds of legality

Ethical Dilemma: Industrial Espionage

- Industrial espionage is widespread, and critical information is always vulnerable to attacks
  - Most commonly associated with industries where research and development (R&D) is a significant expense
  - May be conducted by governments as well as competitors
  - Employees who can be bribed, coerced, or blackmailed often targeted
  - Ex-employees also an opportunistic target
  - Mobile technology provides additional avenues for industrial espionage

When Things Go Wrong: The Bug That Almost Killed the Internet

- OpenSSL is a popular encryption framework used to secure many Internet-based transactions
- Its **heartbleed** bug is a flaw that was created in 2011 and wasn't fixed until 2014
- Attackers can compromise encryption keys, user names and passwords, and sensitive data
- The vulnerability potentially affects thousands of companies and millions of users

Who's Going Mobile: Mobile Security

- With hundreds of thousands of apps in app stores, the potential for mobile malware is significant
- Malware could:
  - Steal user's contacts and photos, turn on the device's camera or send premium-rate text messages
- In 2013, security firm Kaspersky reported that mobile malware poses significant security threats
  - Mobile banking fraud, mobile botnets, and even access to connected PCs
- Android is most vulnerable, because of open marketplace
- Apple iOS is not immune

Brief Case:
3D Crime Scenes

- 3D technology is now widely used for re-creating crime scenes
  - Crime scenes can be scanned and captured in minute detail
  - They can then be viewed from any possible angle and vantage point
  - 3D maps of cities and buildings are also being stored to help foil future terrorist attacks
  - CSI effect: jurors demand more forensic evidence because they see it on popular TV shows

Coming Attractions: Speeding Security Screening

- Airport and customs screening is time consuming and expensive
  - University of Arizona researchers have constructed an embodied conversational agent called AVATAR that can interview travelers
  - Multiple sensor technologies detect the traveler's emotional state and likely deceptiveness
  - As more tests are run, researchers learn more and enhance its capabilities
  - One day it may take the lead in conducting travel interviews

Key Players:
White Knights of the Internet Age

- Every computer is vulnerable to attack
- Security software is big business with many players
  - $19.9 billion in 2013
  - Specialized security companies
    - Symantec, McAfee, TrendMicro, IBM, AVG, etc.
  - Offer full suites of security software, including virus and malware detection, e-mail protection, and other safeguards.
- Yet, a Microsoft survey showed that in 2013, 24 percent of PCs were not protected by up-to-date antivirus software

Industry Analysis: Cybercops Track Cybercriminals

- Police departments have been playing catch-up with technology, but are now making great strides
  - Computer Crime and Intellectual Property Section of DOD is dedicated to tackling cybercrime
  - FBI has dedicated cybercrime resources in 56 field offices
  - Every state has a computer crime investigation unit
  - Lots of municipal computer crime investigation departments
  - Software tools for law enforcement have improved significantly Examples:
    - Software Forensic Tool Kit
    - Statewide Network of Agency Photos (SNAP) database
- While criminals may now be using technology to commit crimes, law enforcement is using technology to catch them