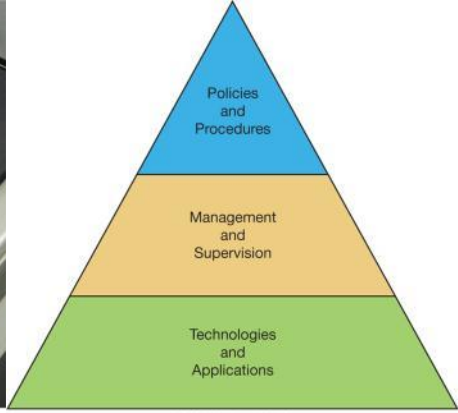
Source: dny3d/Shutterstock

Source: Getty Images - iStock Exclusive RF

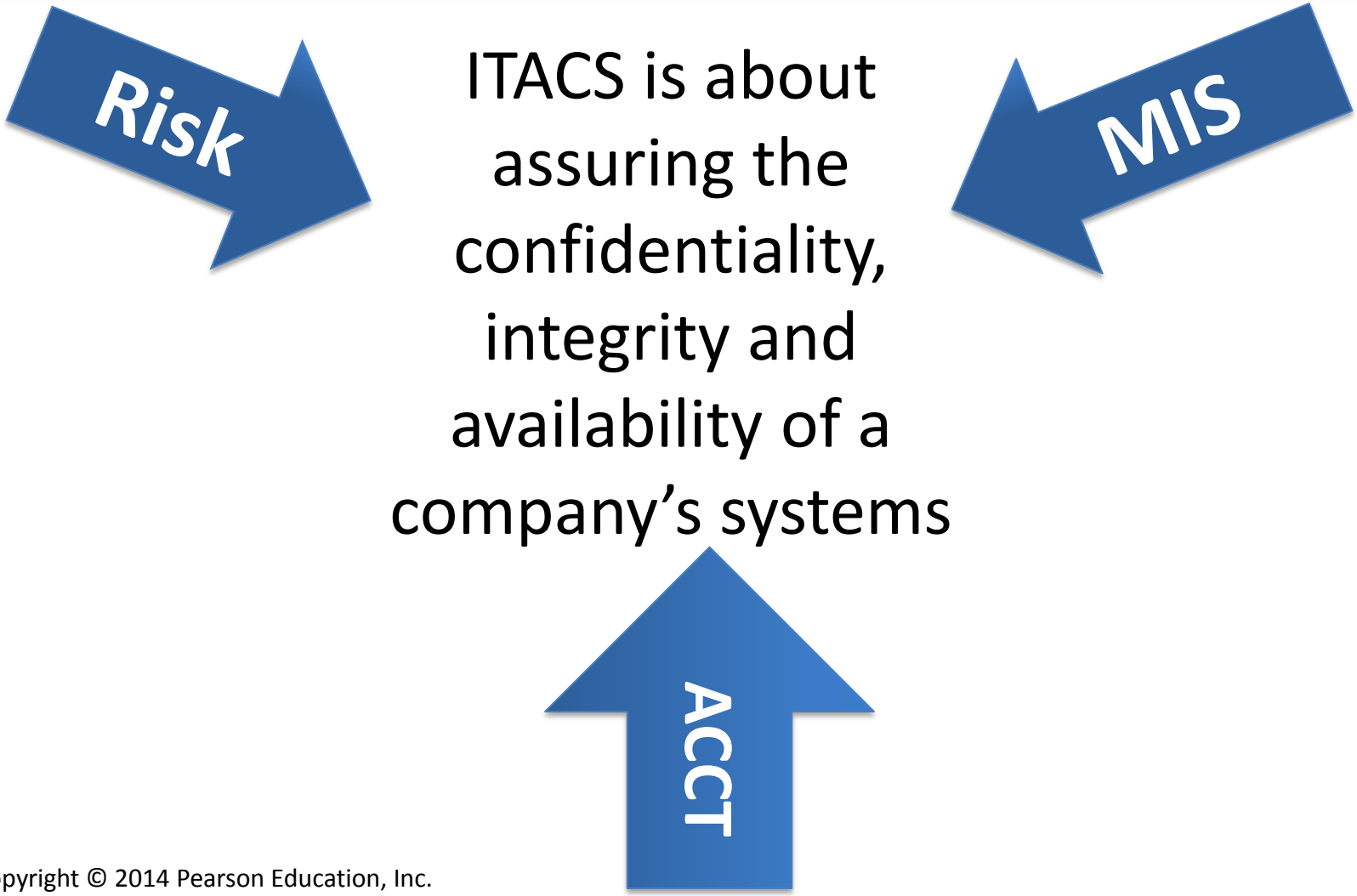
Source: Kilukilu/Dreamstime



Chapter 10 - Securing Information Systems

IS Security is a critical aspect of managing in the digital world

MS in Information Technology Auditing and Cyber-Security



The Career

- Public Accounting
- Internal Accounting
- Government Service
- Corporate Security
- IT Management

U.S. Citizenship and Immigration Services

S.T.E.M.

The MS ITACS Program

Ten plus courses, professional MS program
Professional certification (CISA) preparation
$1,000 per credit
Scholarships available

Looking for:

- Accounting, Finance, MIS, or Risk majors
- Some systems background
- GPA 3.0 or higher

For more information about ITACS check out:

community.mis.temple.edu/itacs

Or contact:

Rich Flanagan, Director ITACS Program

215 204 3077

richard.flanagan@temple.edu

Worldwide losses due to software piracy in 2005 exceeded $34 billion.

Business Software Alliance, 2006

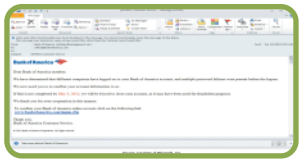
Worldwide losses due to software piracy in 2008 exceeded $50 billion.

Business Software Alliance, 2009

Worldwide losses due to software piracy in 2010 exceeded $59 billion.

Business Software Alliance, 2011

Chapter 10 Learning Objectives

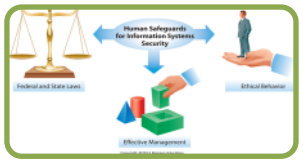


Computer Crime

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

Cyberwar and Cyberterrorism

- Describe and explain the differences between cyberwar and cyberterrorism.



Information Systems Security

- Explain what is meant by the term "IS security" and describe both technology and human based safeguards for information systems.

Managing IS Security

- Discuss how to better manage IS security and explain the process of developing an IS security plan.

Information Systems Controls, Auditing, and the Sarbanes-Oxley Act

- Describe how organizations can establish IS controls to better ensure IS security.

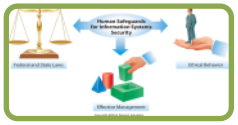
Computer Crime

Computer Crime

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

Cyberwar and Cyberterrorism

Describe and explain the differences between cyberwar and cyberterrorism.



Information Systems Security

Explain what is meant by the term "IS security" and describe both technology and human based safeguards for information systems.

Managing IS Security

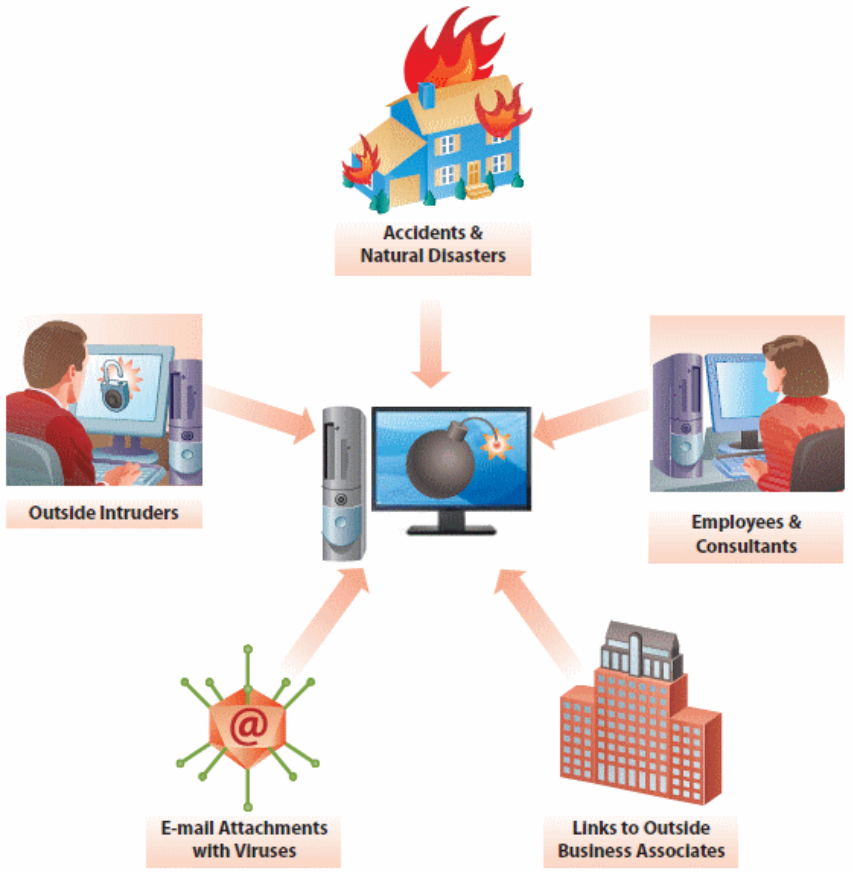
Discuss how to better manage IS security and explain the process of developing an IS security plan.

Information Systems Controls, Auditing, and the Sarbanes-Oxley Act

Describe how organizations can establish IS controls to better ensure IS security.

Primary Threats to Information Systems Security

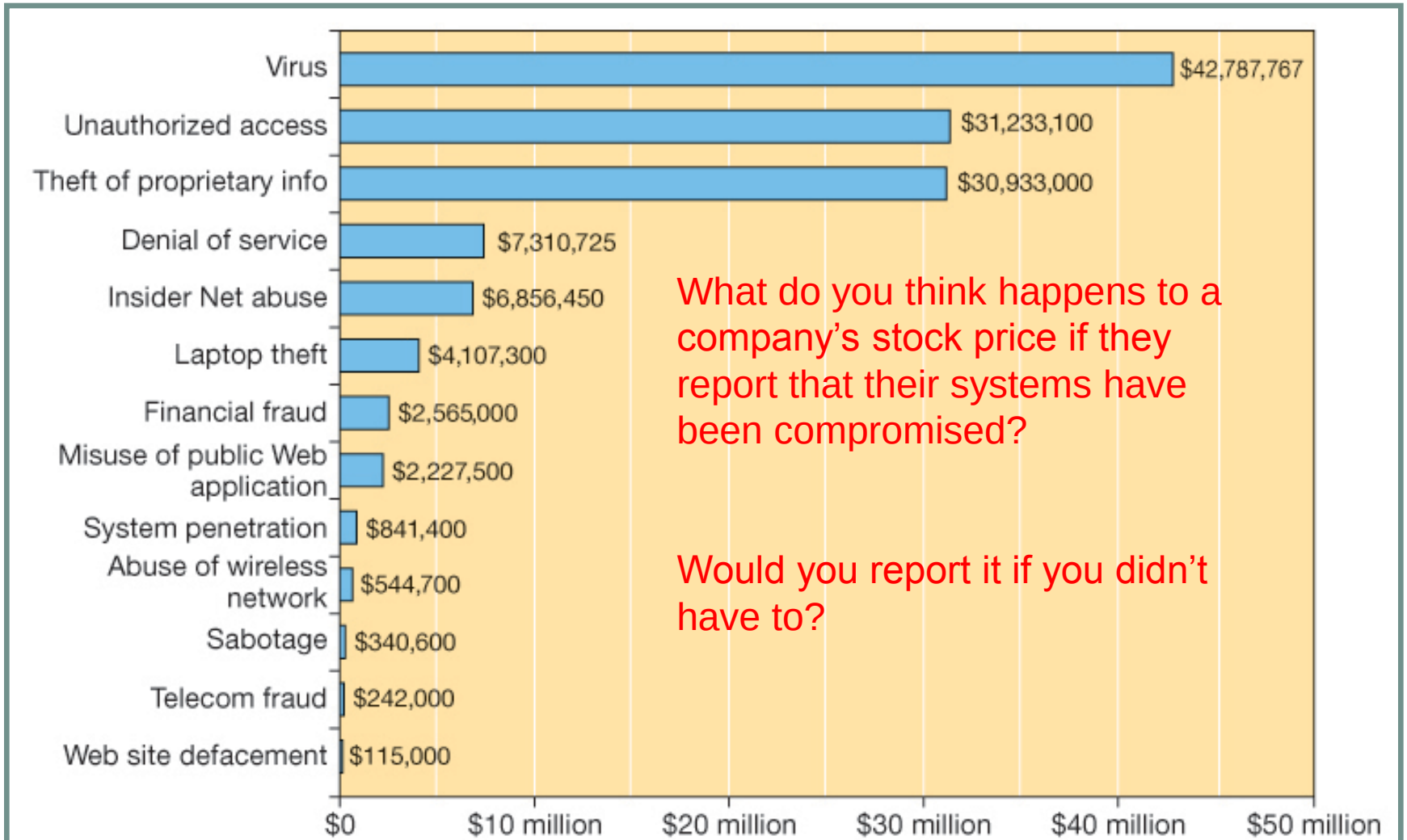
- Natural disasters
  - Power outages, hurricanes, floods, and so on
- Accidents
  - Power outages, cats walking across keyboards
- Employees and consultants
- Links to outside business contacts
  - Travel between business affiliates
- Outsiders
  - Viruses



Computer Crime

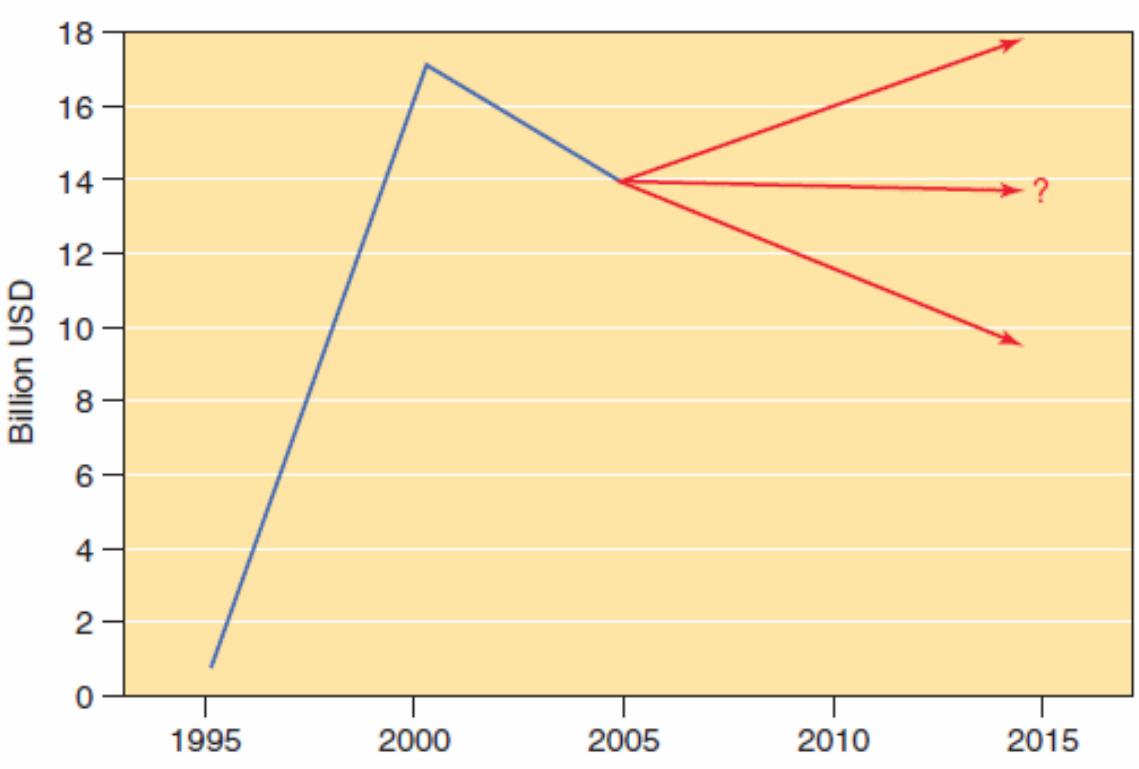
- Computer crime—The act of using a computer to commit an illegal act.
  - Targeting a computer while committing an offense.
  - Using a computer to commit an offense.
  - Using computers to support a criminal activity.
- Overall trend for computer crime has been declining over the past several years (CSI, 2011).
- Many incidents are never reported.

Types of Computer Crimes and Financial Losses



Computer Virus Attacks

- Financial impact of virus attacks, 1995–2006, and beyond.
- Source: Based on: http://www.computereconomics.com.



Federal and State Laws

- The two main federal laws against computer crime are:
  - Computer Fraud and Abuse Act of 1986
    - Stealing or compromising data about national defense, foreign relations, atomic energy, or other restricted information
    - Violating data belonging to banks or other financial institutions
    - Intercepting or otherwise intruding on communications between states or foreign countries
    - Threatening to damage computer systems in order to extort money or other valuables from persons, businesses, or institutions
  - Electronic Communications Privacy Act of 1986
    - makes it a crime to break into any electronic communications service, including telephone services
    - prohibits the interception of any type of electronic communications

Other Federal Laws

- Patent protection
- U.S. Copyright Act
  - amended in 1980 for computer software
- Financial Privacy Act
  - protects information: credit card, credit reporting , bank loan applications
- Enforcement responsibilities
  - FBI—espionage, terrorism, banking, organized crime, and threats to national security
  - Secret Service—crimes against U.S. Treasury Department computers and against violations of the Right to Financial Privacy Act

Hacking and Cracking

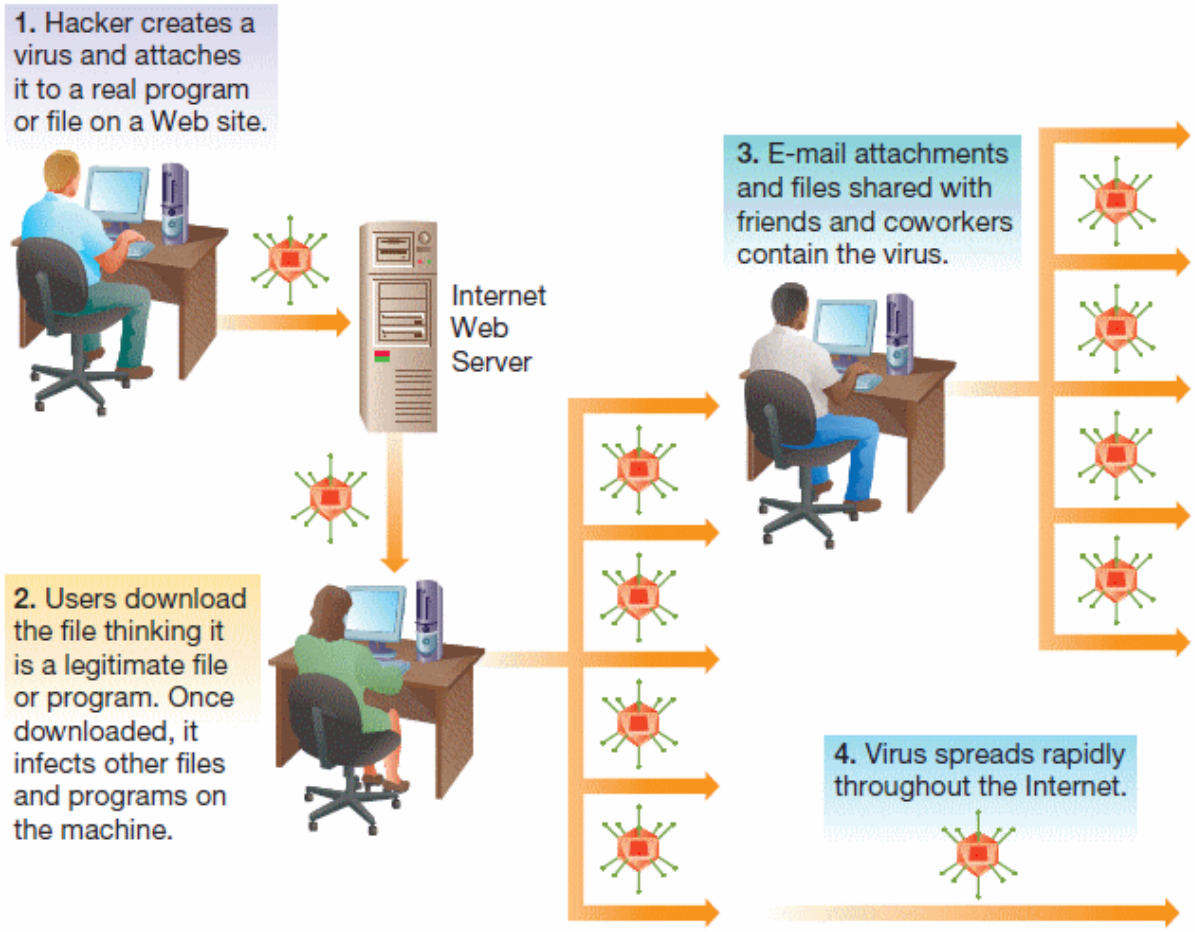
- Which one is the “bad guy”?
  - Hackers
  - Crackers
  - Hacktivists

Types of Criminals

- No clear profile as to who commits computer crimes
- Four groups of computer criminals
  1. Current or former employees
     - 85–95% of theft from businesses comes from the inside
  2. People with technical knowledge committing crimes for personal gain
  3. Career criminals using computers to assist them in crimes
  4. Outside crackers hoping to find information of value
     - About 12 percent of cracker attacks cause damage

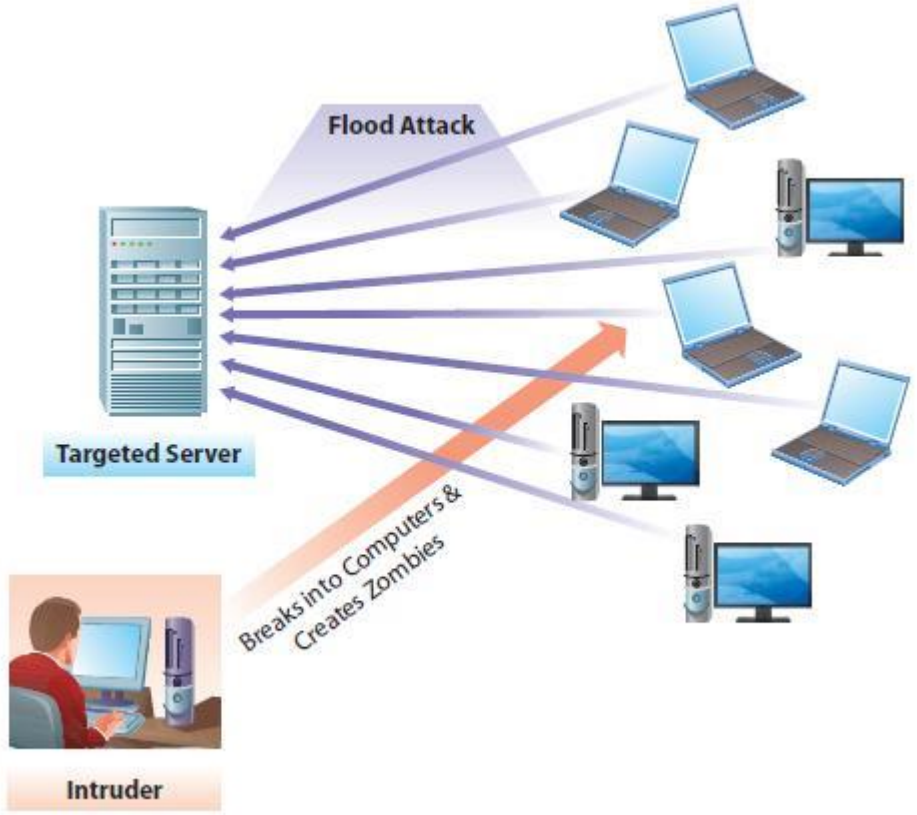
Computer Viruses and Other Destructive Code

- What is your favorite virus?



Denial of Service Attack

- Attackers prevent legitimate users from accessing services.
- Zombie computers
  - Created by viruses or worms
  - Attack Web sites
- Servers crash under increased load.
  - MyDoom attack on Microsoft's Web site



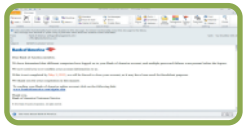
Cybersquatting

- The practice of registering a domain name and later reselling it.
- Some of the victims include:
  - Eminem
  - Panasonic
  - Hertz
  - Avon
- Anti-Cybersquatting Consumer Protection Act in 1999
  - Fines as high as $100,000
  - Some companies pay the cybersquatters to speed up the process of getting the domain.

Cyber Harassment, Stalking, and Bullying

- Cyber harassment—Crime that broadly refers to the use of a computer to communicate obscene, vulgar, or threatening content.
- Cyber stalking
  - Making false accusations that damage reputation of another
  - Gaining information on a victim by monitoring online activities
  - Using the Internet to encourage others to harass a victim
  - Attacking data and equipment of a victim by sending e-mail viruses or other destructive code
  - Using the Internet to place false orders for goods or services

Cyberwar and Cyberterrorism

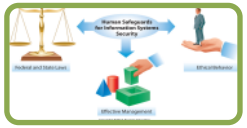


Computer Crime

Define computer crime and describe several types of computer crime.

Cyberwar and Cyberterrorism

- Describe and explain the differences between cyberwar and cyberterrorism.

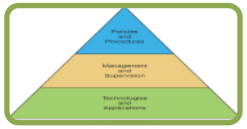


Information Systems Security

Explain what is meant by the term "IS security" and describe both technology and human based safeguards for information systems.

Managing IS Security

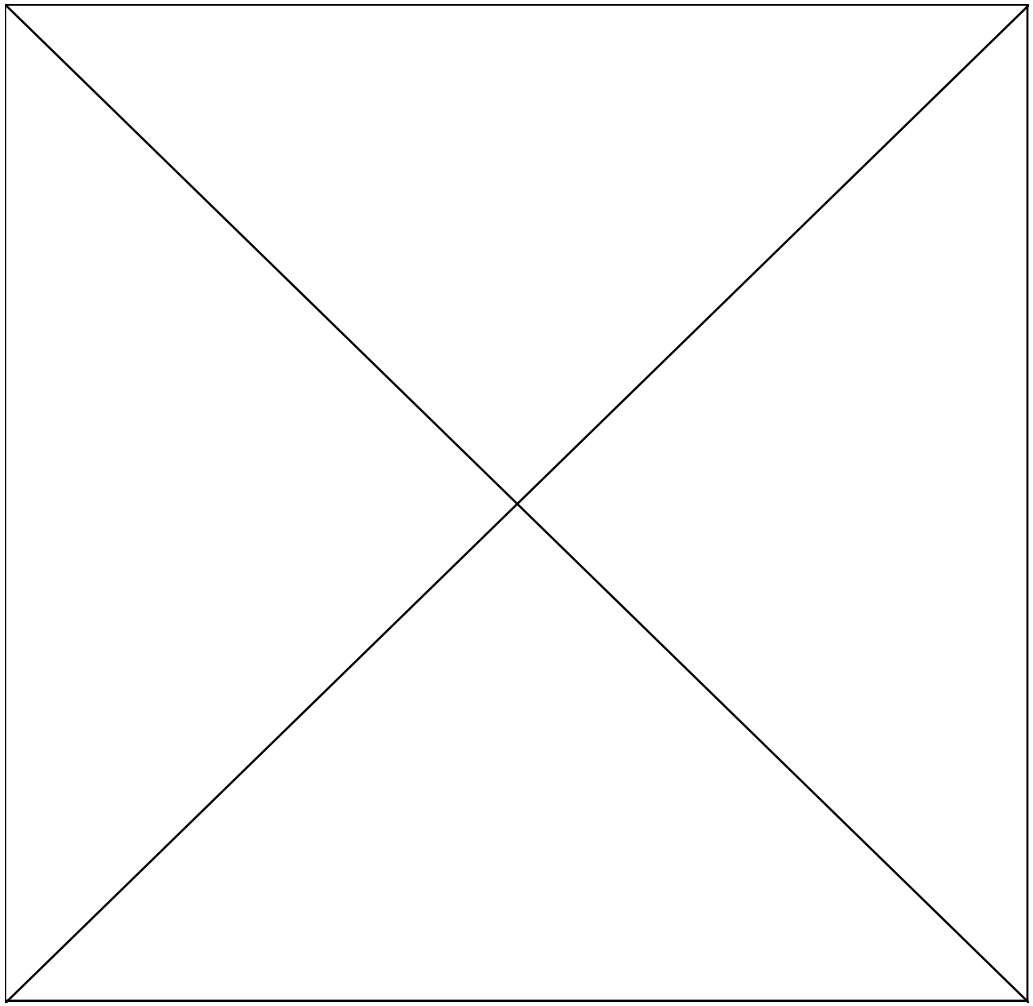
Discuss how to better manage IS security and explain the process of developing an IS security plan.



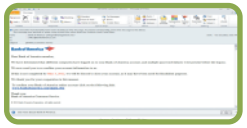
Information Systems Controls, Auditing, and the Sarbanes-Oxley Act

Describe how organizations can establish IS controls to better ensure IS security.

Cyberterrorism



Information Systems Security

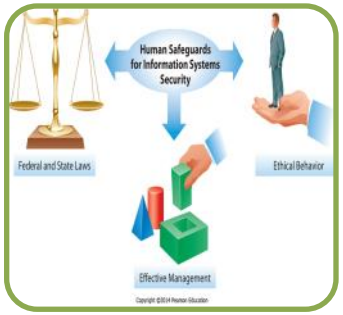


Computer Crime

Define computer crime and describe several types of computer crime.

Cyberwar and Cyberterrorism

Describe and explain the differences between cyberwar and cyberterrorism.



Information Systems Security

- Explain what is meant by the term “IS security” and describe both technology and human based safeguards for information systems.

Managing IS Security

Discuss how to better manage IS security and explain the process of developing an IS security plan.

Information Systems Controls, Auditing, and the Sarbanes-Oxley Act

Describe how organizations can establish IS controls to better ensure IS security.

Safeguarding IS Resources

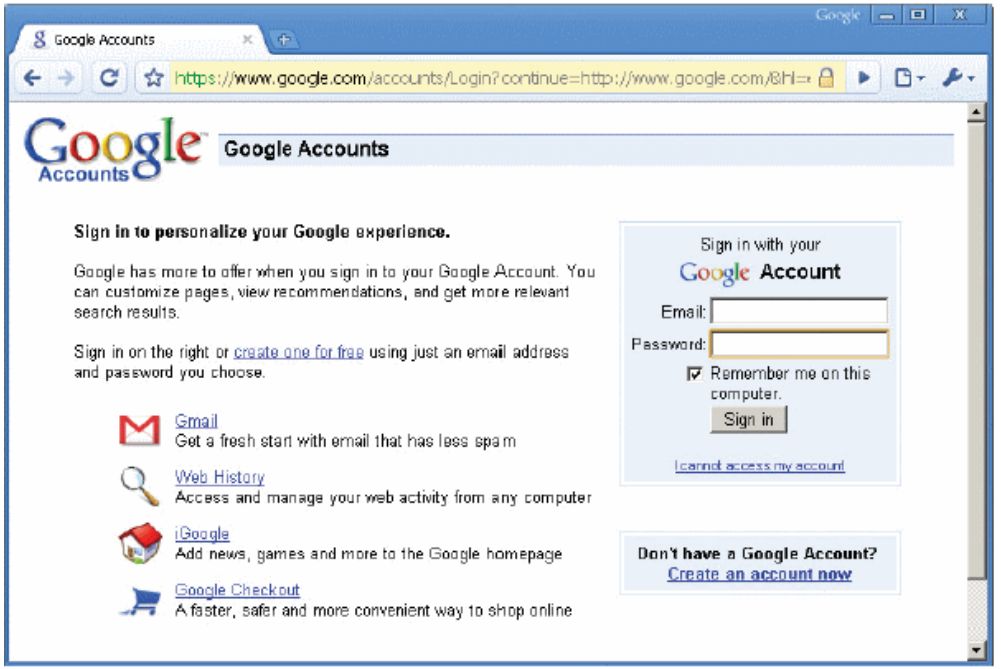
- Risk Reduction
  - Actively installing countermeasures
- Risk Acceptance
  - Accepting any losses that occur
- Risk Transference
  - Insurance
  - Outsourcing

Information Systems Security

- All systems connected to a network are at risk.
  - Internal threats
  - External threats
- Information systems security
  - Precautions to keep IS safe from unauthorized access and use
- Increased need for good computer security with increased use of the Internet

Technological Safeguards

- Physical access restrictions
- Authentication
  - Use of passwords
  - Photo ID cards, smart cards
  - Keys to unlock a computer
  - Combination
- Authentication dependent on
  - Something you have
  - Something you know
  - Something you are



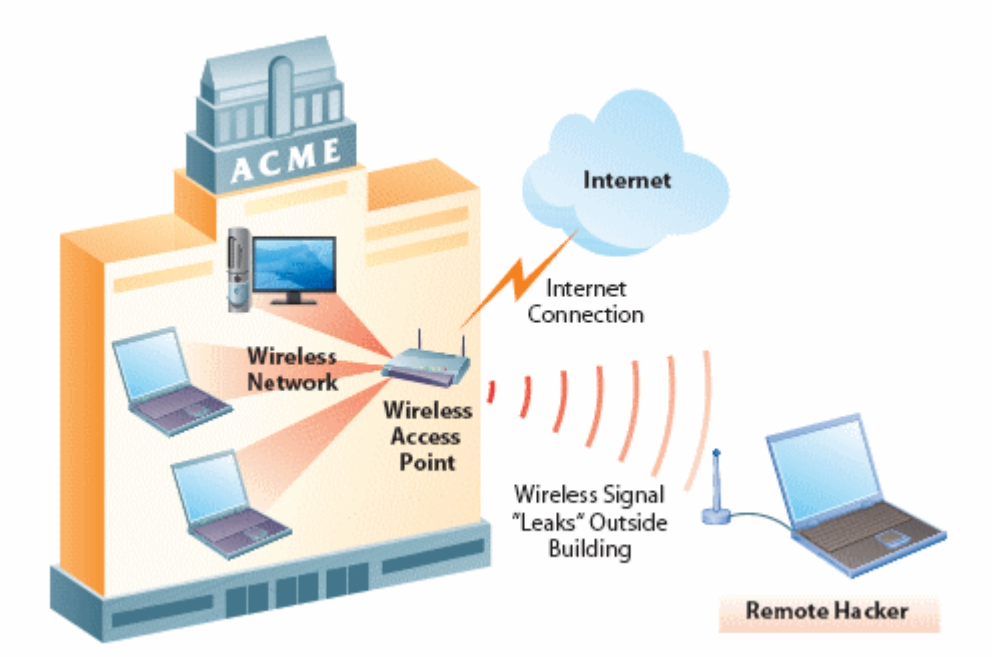
Biometrics

- Form of authentication
  - Fingerprints
  - Retinal patterns
  - Facial features and so on
- Fast authentication
- High security

- Recent visit to Disney ESPN Wide World of Sports…

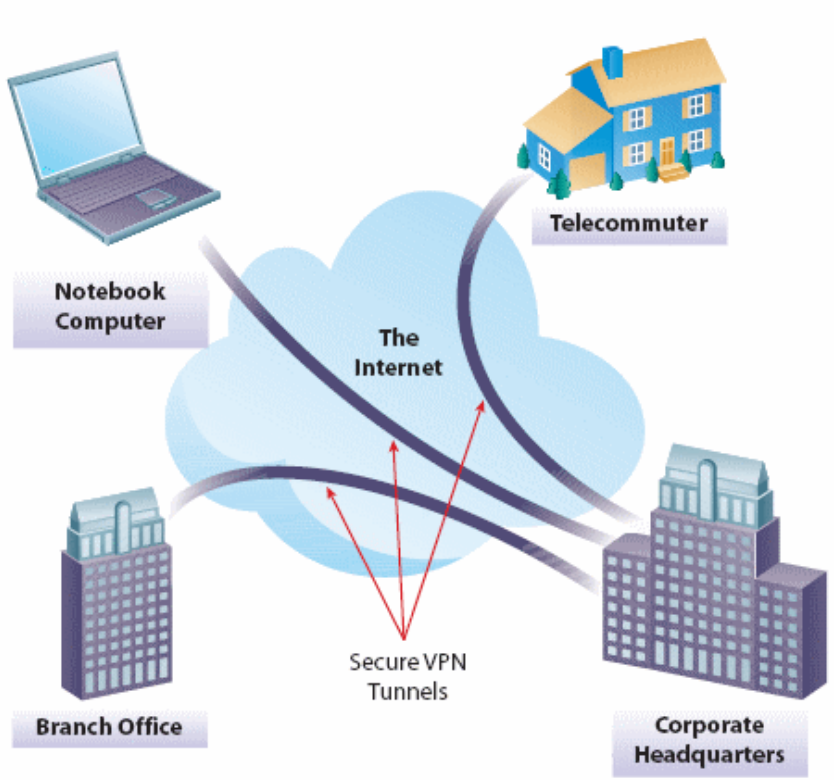
Wireless LAN Control

- Wireless LAN cheap and easy to install
- Use on the rise
- Signal transmitted through the air
  - Susceptible to being intercepted
  - Drive-by hacking



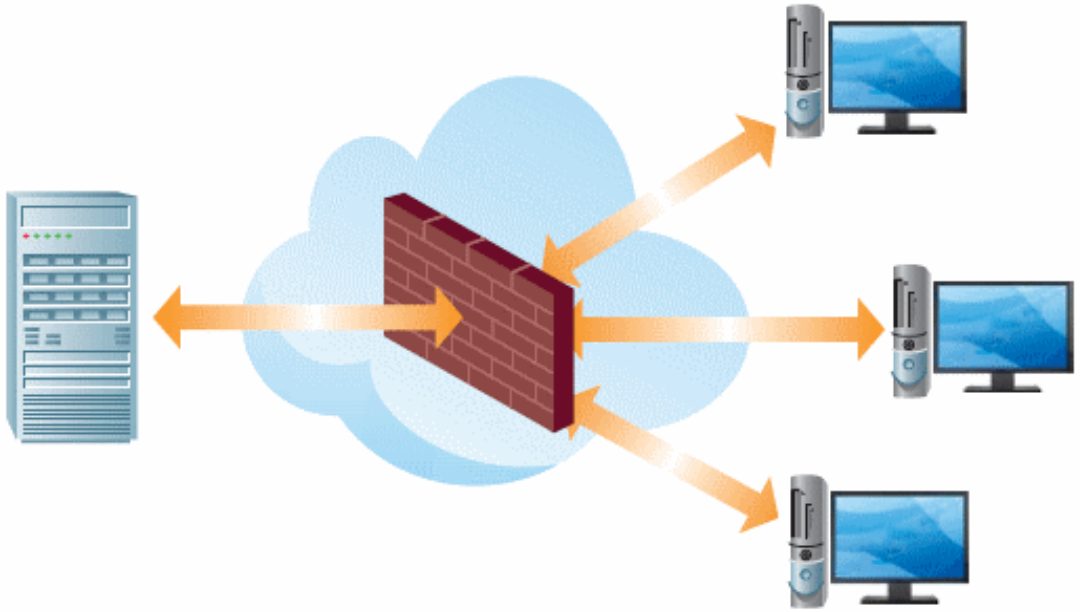
Virtual Private Networks

- Connection constructed dynamically within an existing network
- Tunneling
  - Send private data over public network
  - Encrypted information



Firewalls

- Firewall—A system designed to detect intrusion and prevent unauthorized access
- Implementation
  - Hardware, software, mixed



Encryption

- Message encoded before sending
- Message decoded when received

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

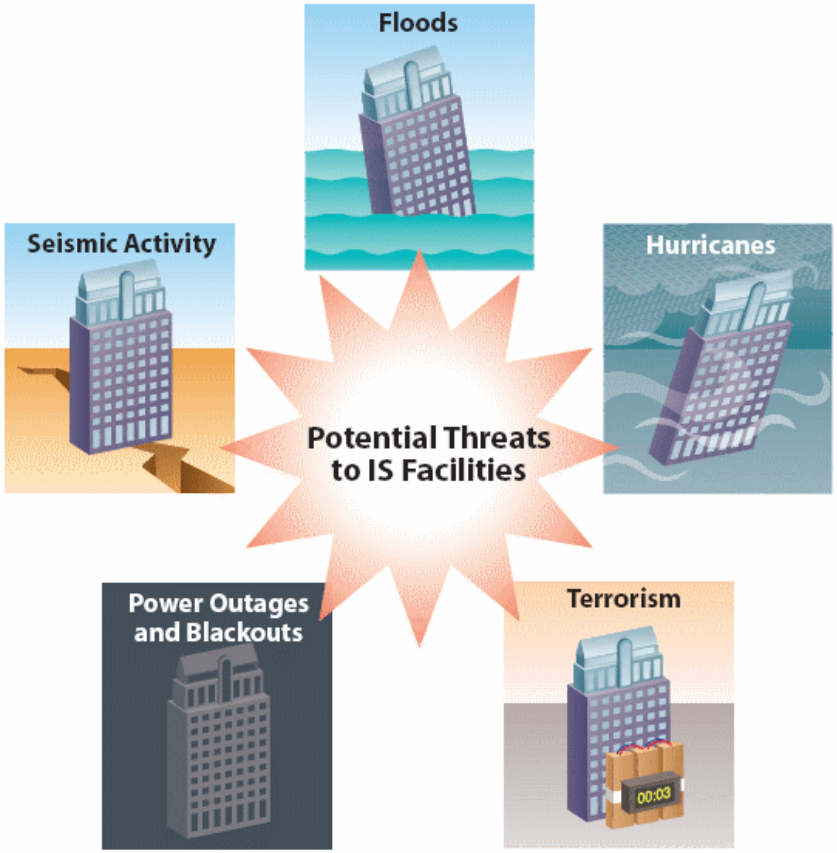
- Cryptography—the science of encryption.
  - It requires use of a key for decoding.
- Certificate authority—manages distribution of keys on a busy Web site.
- Secure Sockets Layer (SSL)—popular public key encryption method.

Virus Monitoring and Prevention

- Virus prevention
  - Purchase and install antivirus software.
    - Update frequently.
  - Do not download data from unknown sources.
    - Flash drives, disks, Web sites
  - Delete (without opening) e-mails from unknown sources.
  - Do not blindly open e-mail attachments
    - Even if they come from a known source.
  - Report any viruses to the IT department.

Secure Data Centers

- Specialized facilities are important.
- Technical Requirements
  - Power
  - Cooling
- How do organizations reliably protect themselves from threats?



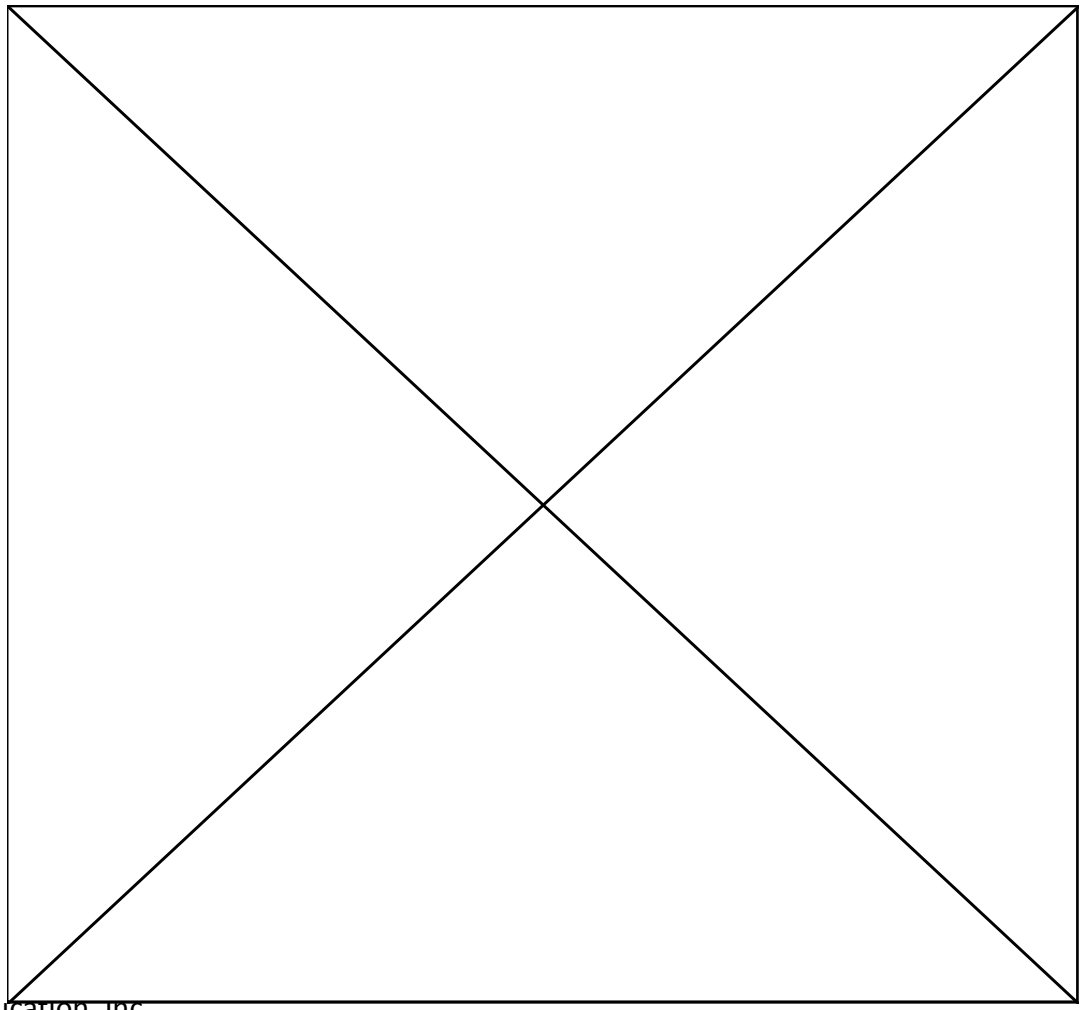
Ensuring Availability

- High-availability facilities
  - To ensure uninterrupted service
  - Self-sufficient
  - Backup cooling systems
  - Raised floors (to more easily reconfigure systems)
  - Built to withstand storms
- Collocation facilities
- UPS servers need 24/7/365 reliability

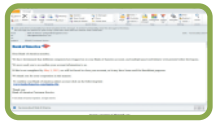
Securing the Facilities Infrastructure

- Backups
  - Secondary storage devices
  - Regular intervals
- Backup sites
  - Cold backup site
  - Hot backup site
- Redundant data centers
  - Different geographic areas
- Closed-circuit television (CCTV)
  - Monitoring for physical intruders
  - Video cameras display and record all activity
  - Digital video recording
- Uninterruptible power supply (UPS)
  - Protection against power surges

What is “Computer Forensics”?



Managing IS Security

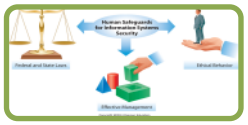


Computer Crime

Define computer crime and describe several types of computer crime.

Cyberwar and Cyberterrorism

Describe and explain the differences between cyberwar and cyberterrorism.



Information Systems Security

Explain what is meant by the term "IS security" and describe both technology and human based safeguards for information systems.

Managing IS Security

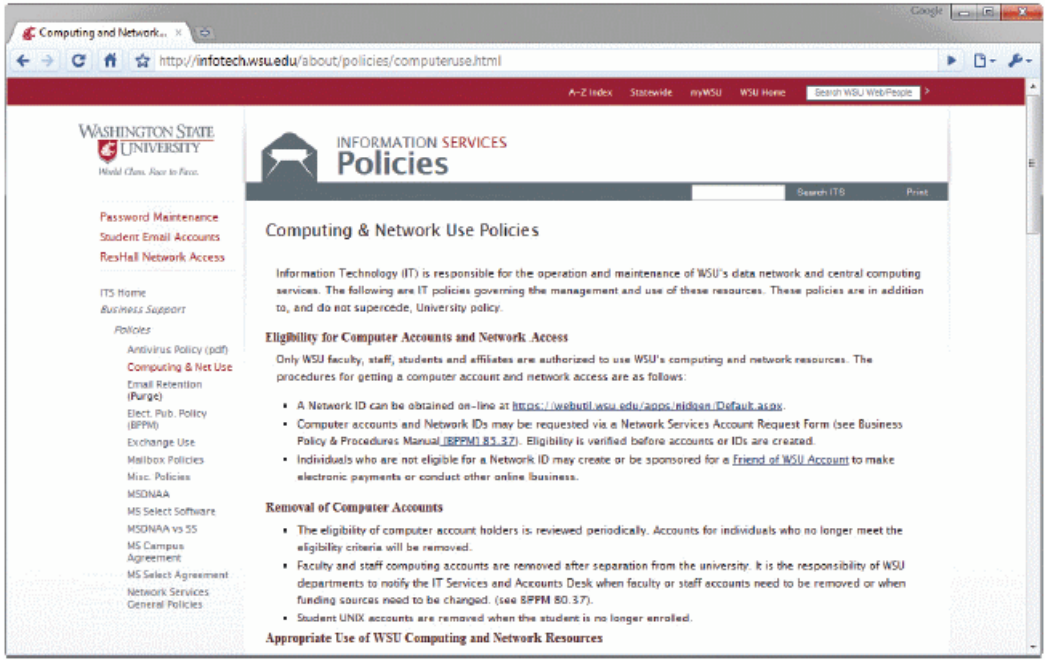
- Discuss how to better manage IS security and explain the process of developing an IS security plan.

Information Systems Controls, Auditing, and the Sarbanes-Oxley Act

Describe how organizations can establish IS controls to better ensure IS security.

Managing Information Systems Security

- Non-technical safeguards
  - Management of people's use of IS
    - Acceptable use policies
  - Trustworthy employees
  - Well-treated employees



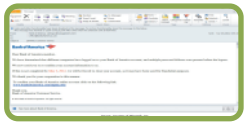
Disaster Planning

- Disasters can't be completely avoided. Need to be prepared.
- Business continuity plan
  - describes how a business resumes operation after a disaster
- Disaster recovery plan
  - Subset of business continuity plan
  - Procedures for recovering from systems-related disasters
  - Two types of objectives
    - Recovery time objectives (Maximum time allowed to recover)
    - Recovery point objectives (How current should the backup material be?)

Responding to a Security Breach

- Restore lost data
- Perform new risk audit
- Implement additional safeguards
- Contact law enforcement (yeah, right!)
  - Computer Emergency Response Team Coordination Center (Federal government center of Internet security expertise)

Information Systems Controls, Auditing, and the Sarbanes-Oxley Act



Computer Crime

Define computer crime and describe several types of computer crime.

Cyberwar and Cyberterrorism

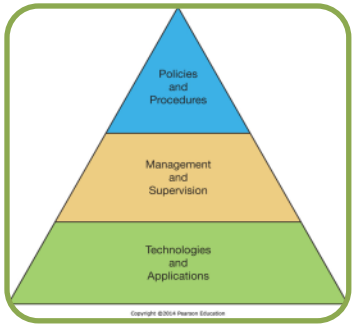
Describe and explain the differences between cyberwar and cyberterrorism.

Information Systems Security

Explain what is meant by the term "IS security" and describe both technology and human based safeguards for information systems.

Managing IS Security

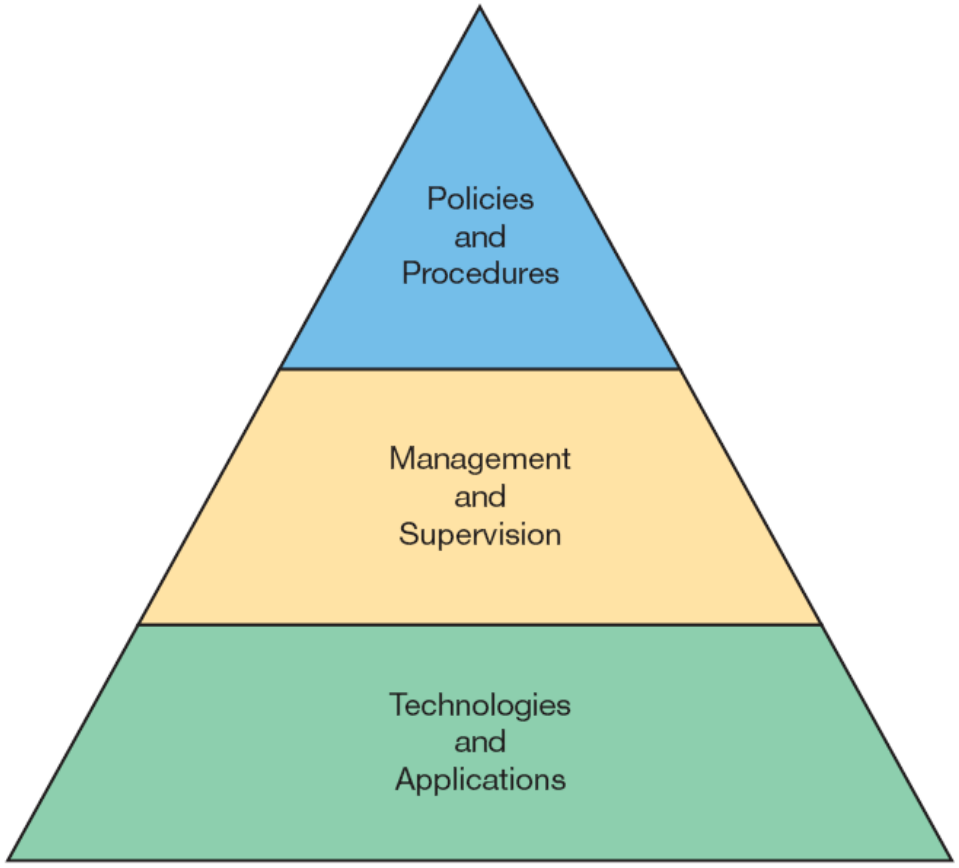
Discuss how to better manage IS security and explain the process of developing an IS security plan.



Information Systems Controls, Auditing, and the Sarbanes-Oxley Act

- Describe how organizations can establish IS controls to better ensure IS security.

Hierarchy of IS Controls



Types of IS Controls

- Policies
  - Define aim and objectives.
- Standards
  - Support the requirements of policies.
- Organization and management
  - Define the lines of reporting.
- Physical and environmental controls
  - Protect the organization's IS assets.

Types of IS Controls (cont'd)

- Systems software controls
  - Enable applications and users to utilize the systems.
- Systems development and acquisition controls
  - Ensure systems meet the organization's needs.
- Application-based controls
  - Ensures correct input, processing, storage, and output of data; maintain record of data as it moves through the system.

IS Auditing

- Information Systems audit
  - Performed by external auditors to help organizations assess the state of their IS controls.
    - To determine necessary changes
    - To assure the IS availability, confidentiality, and integrity
- Risk assessment
  - Determine what type of risks the IS infrastructure faces.
- Computer-Assisted Auditing Tools (CAAT)
  - Specific software to test applications and data, using test data or simulations.

The Sarbanes-Oxley Act

- The Sarbanes-Oxley Act was formed as a reaction to large-scale accounting scandals.
  - WorldCom, Enron
- It primarily addresses the accounting side of organizations.
- Companies have to demonstrate that:
  - controls are in place to prevent misuse and fraud,
  - controls are in place to detect potential problems, and
  - measures are in place to correct problems
- COBIT (Control Objectives for Information and Related Technology)
  - Set of best practices
    - Help organizations to maximize the benefits from their IS infrastructure
    - Establish appropriate controls