Computer and Internet Crime

- Why are computer related crime on the rise?

Why Computer Incidents are So Prevalent

- Increasing complexity increases vulnerability
    - Number of entry points to a network expands continually, increasing the possibility of security breaches
    - **Cloud computing**: Environment where software and data storage are provided via the Internet
    - **Virtualization software**: Operates in a software layer that runs on top of the operating system
        - Enables multiple **virtual machines** to run on a single computer

Why Computer Incidents are So Prevalent

- Higher computer user expectations
  - Not verifying users’
  - Sharing of login IDs and passwords by users
- Expanding and changing systems require one to:
  - Keep up with the pace of technological change
  - Perform an ongoing assessment of new security risks
  - Implementing approaches for dealing with them

Why Computer Incidents are So Prevalent

- **Bring your own device (BYOD)**: Business policy that permits employees to use their own mobile devices to access company computing resources and applications
- Increased reliance on commercial software with known vulnerabilities
  - **Exploit**: Attack on an information system that takes advantage of a particular system vulnerability
  - **Zero-day attack**: Takes place before the security community or software developer knows about the vulnerability or has been able to repair it

Ethical Decisions Regarding IT Security

- To deal with computer crime, the firm should:
  - Pursue prosecution of the criminals at all costs
  - Maintain a low profile to avoid the negative publicity
  - Inform affected customers or take some other action
- Following decisions should be taken by the firm
  - How much resources should be spent to safeguard against computer crime
  - What actions should be taken when a software is found susceptible to hacking
  - What should be done if recommended computer security safeguards increase operating costs

Types of Exploits

Virus

- Piece of programming code, disguised as something else, that causes a computer to behave in an unexpected and undesirable manner

Worm

- Harmful program that resides in the active memory of the computer and duplicates itself

Trojan Horse

- Program in which malicious code is hidden inside a seemingly harmless program
- **Logic bomb**: Executes when it is triggered by a specific event

Types of Exploits

Spam

- Abuse of email systems to send unsolicited email to large numbers of people
- **CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart)**
  - Generates and grades tests that humans can pass but computer programs cannot

Distributed Denial-of-Service (DDoS) Attack

- Causes computers to flood a target site with demands for data and other small tasks

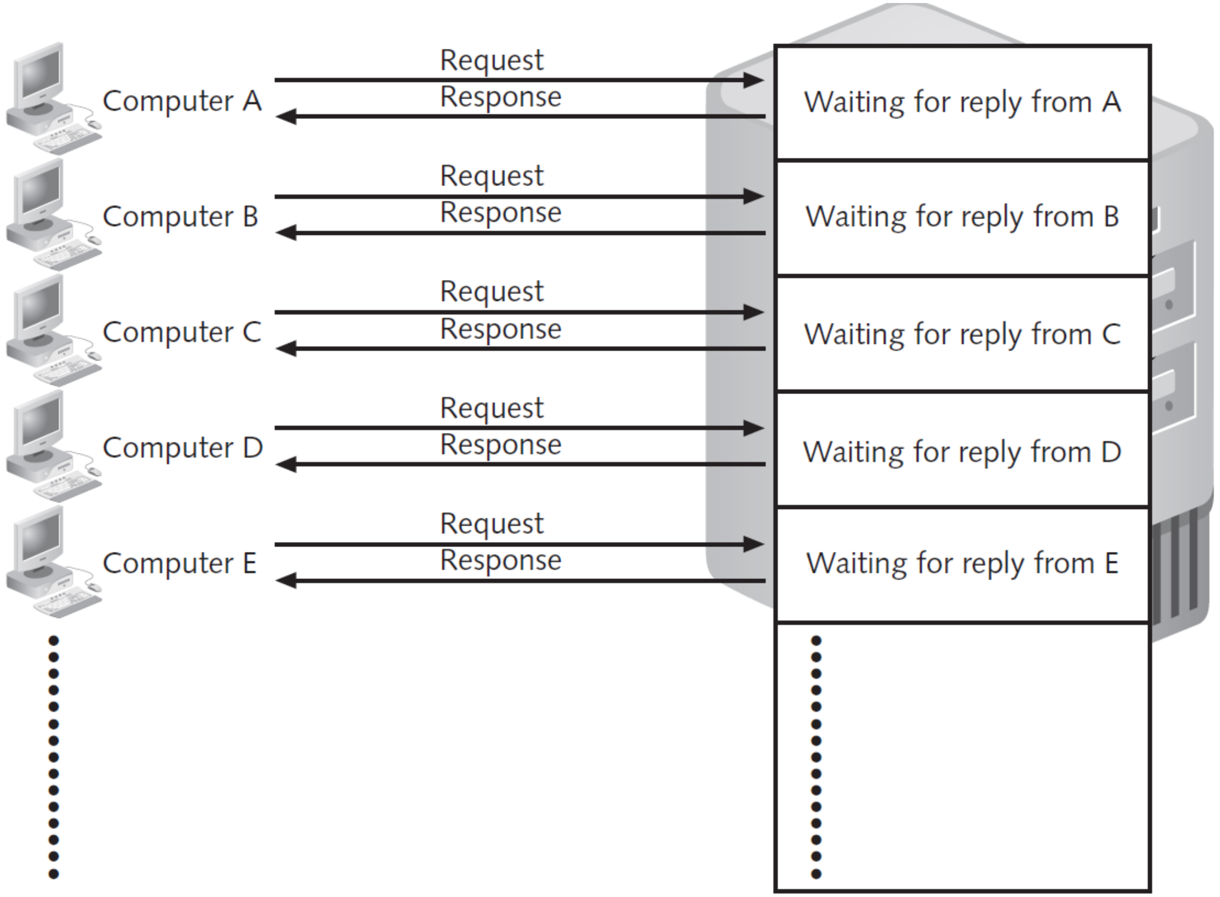
Rootkit

- Enables user to gain administrator-level access to a computer without the end user’s consent

Phishing

- Fraudulently using email to try to get the recipient to reveal personal data

Distributed Denial-of-Service Attack



Source Line: Course Technology/Cengage Learning.

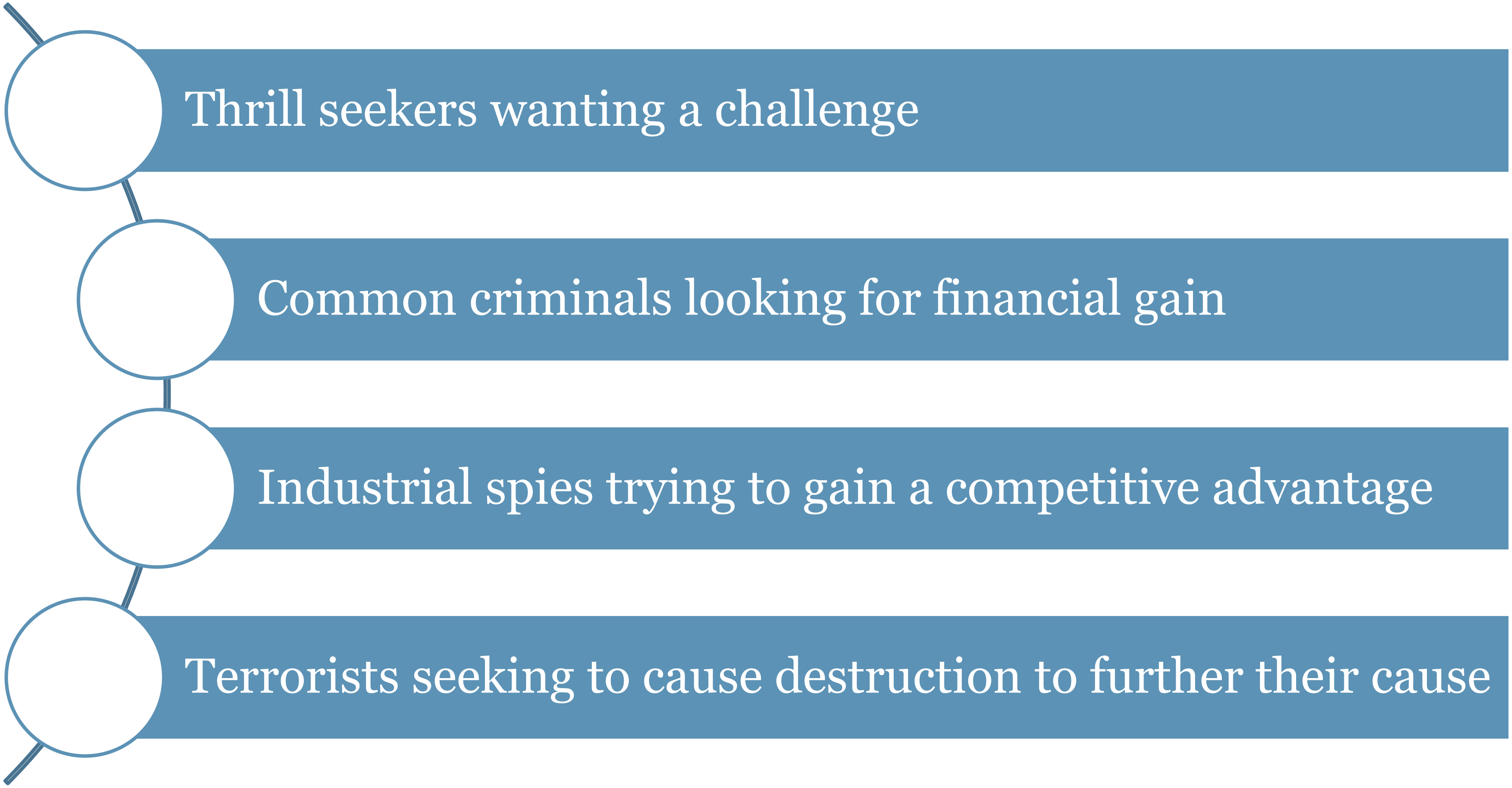
Botnet

- Group of computers which are controlled from one or more remote locations by hackers, without the knowledge or consent of their owners
- **Zombies**: Computers that are taken over
- used to distribute spam and malicious code

Types of Phishing

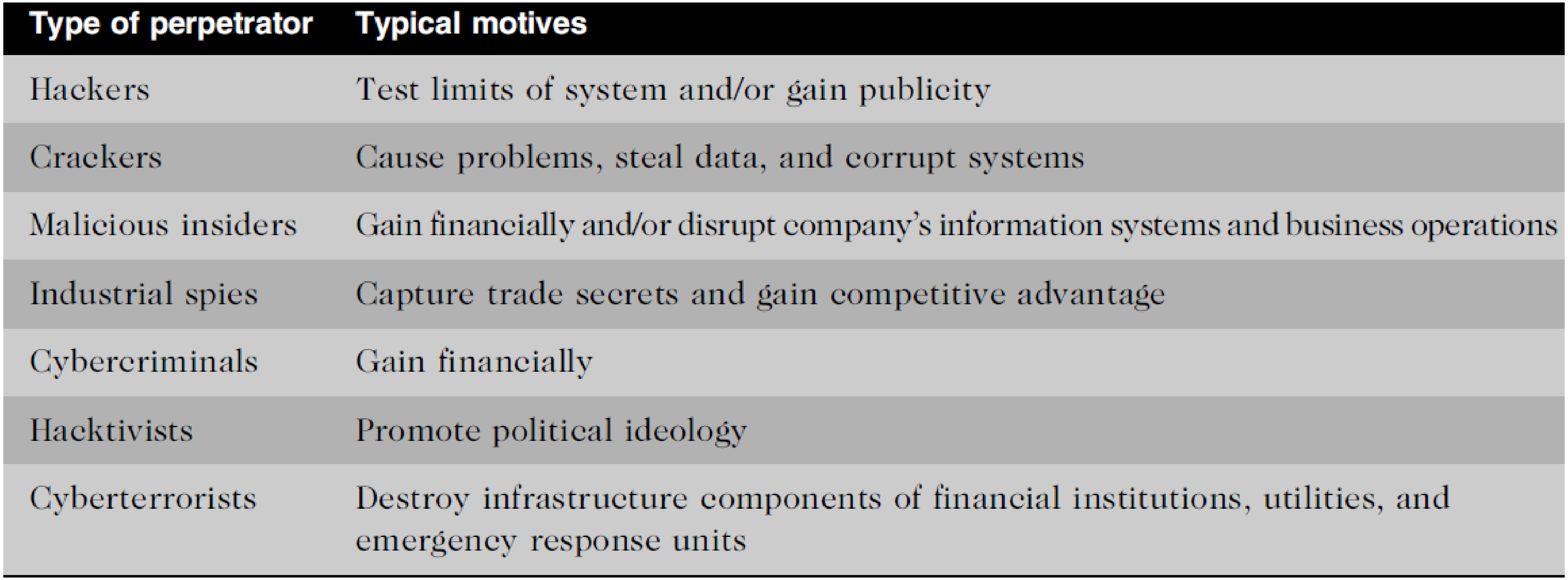
- **Spear-phishing**: Phisher sends fraudulent emails to a certain organization’s employees
  - Emails are designed to look like they came from high-level executives within the organization
- **Smishing**: Legitimate-looking text message sent to people, telling them to call a specific phone number or to log on to a Web site
- **Vishing**: Victims receive a voice mail telling them to call a phone number or access a Web site

Types of Perpetrators



- Thrill seekers wanting a challenge
- Common criminals looking for financial gain
- Industrial spies trying to gain a competitive advantage
- Terrorists seeking to cause destruction to further their cause

Classifying Perpetrators of Computer Crime



Type of perpetrator	Typical motives
Hackers	Test limits of system and/or gain publicity
Crackers	Cause problems, steal data, and corrupt systems
Malicious insiders	Gain financially and/or disrupt company's information systems and business operations
Industrial spies	Capture trade secrets and gain competitive advantage
Cybercriminals	Gain financially
Hacktivists	Promote political ideology
Cyberterrorists	Destroy infrastructure components of financial institutions, utilities, and emergency response units

Source Line: Course Technology/Cengage Learning.

Types of Perpetrators

- **Hackers**: Test the limitations of information systems out of intellectual curiosity
  - **Lamers** or **script kiddies**: Terms used to refer to technically inept hackers
- **Malicious insiders**
  - Employees, consultants, or contractors
  - Have some form of collusion
    - **Collusion**: Cooperation between an employee and an outsider
  - **Negligent insiders**: Poorly trained and inadequately managed employees who cause damage accidently

Types of Perpetrators

- **Industrial spies**
  - **Competitive intelligence**: Legally obtained data gathered using sources available to the public
  - **Industrial espionage**: Using illegal means to obtain information that is not available to the public
- **Cybercriminals**
  - Hack into computers to steal and engage in computer fraud
  - **Data breach**: Unintended release of sensitive data or the access of sensitive data by unauthorized individuals

Types of Perpetrators

- **Hacktivists**: Hack to achieve a political or social goal
- **Cyberterrorists**: Launch computer-based attacks to intimidate or coerce an organization in order to advance certain political or social objectives
  - Use techniques that destroy or disrupt services
  - Consider themselves to be at war
  - Have a very high acceptance of risk
  - Seek maximum impact

Strategies to Reduce Online Credit Card Fraud

- Use encryption technology
- Verify the address submitted online against the issuing bank
- Request a card verification value (CVV)
- Use transaction-risk scoring software
- Use smart cards
  - **Smart cards**: Memory chips are updated with encrypted data every time the card is used

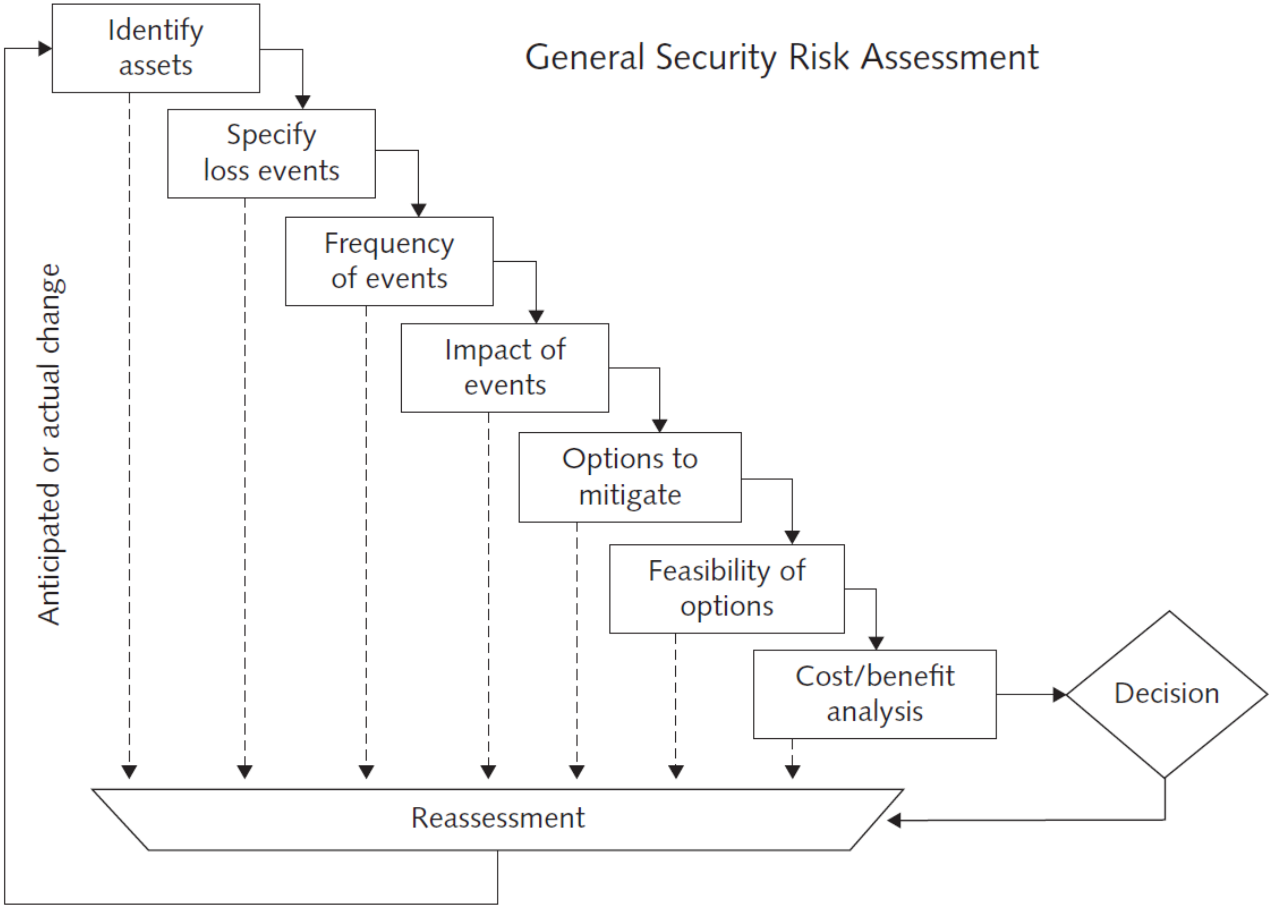
Trustworthy Computing

Delivers secure, private, and reliable computing experiences based on sound business practices

Risk Assessment

- Assessing security-related risks to an organization’s computers and networks from internal and external threats
- Identify investments that will protect the organization from most likely and serious threats
- Asset - Hardware, software, information system, network, or database used by an organization to achieve its business objectives
- Loss event - Any occurrence that has a negative impact on an asset

General Security Risk Assessment



Source Line: General Security Risk Assessment Guidelines, ASIS International (2003). See the Standards and Guidelines page of the ASIS International website (www.asisonline.org) for revisions and/or updates..

Security Policy

- Defines an organization’s security requirements and the controls and sanctions needed to meet those requirements
- Delineates responsibilities and expected behavior
- Outlines what needs to be done and not how it should be done

Establishing a Security Policy

- Areas of concern
  - Use of email attachments
  - Use of wireless devices
- **Virtual private network (VPN)**: Works by using the Internet to relay communications
  - Encrypts data at the sending end and decrypts it at the receiving end

Educating Employees and Contract Workers

- Motivates them to understand and follow the security policies
- Users must help protect an organization’s information systems and data by:
  - Guarding their passwords
  - Prohibiting others from using their passwords
  - Applying strict access controls
  - Reporting all unusual activity to the organization’s IT security group
  - Ensuring that portable computing and data storage devices are protected

Prevention

Install a corporate firewall

- Limits network access based on the organization’s access policy

Intrusion detection system (IDS)

- Monitors system and network resources and activities
- Notifies network security personnel when network traffic attempts to circumvent the security measures

Antivirus software

- Scans for a specific sequence of bytes, known as a virus signature
  - **Virus signature**: Indicates the presence of a specific virus

Prevention

Implement safeguards against attacks by malicious insiders

- Promptly delete the computer accounts, login IDs, and passwords of departing employees and contractors

Defend against cyberterrorism

- Aim to secure critical infrastructure and information systems

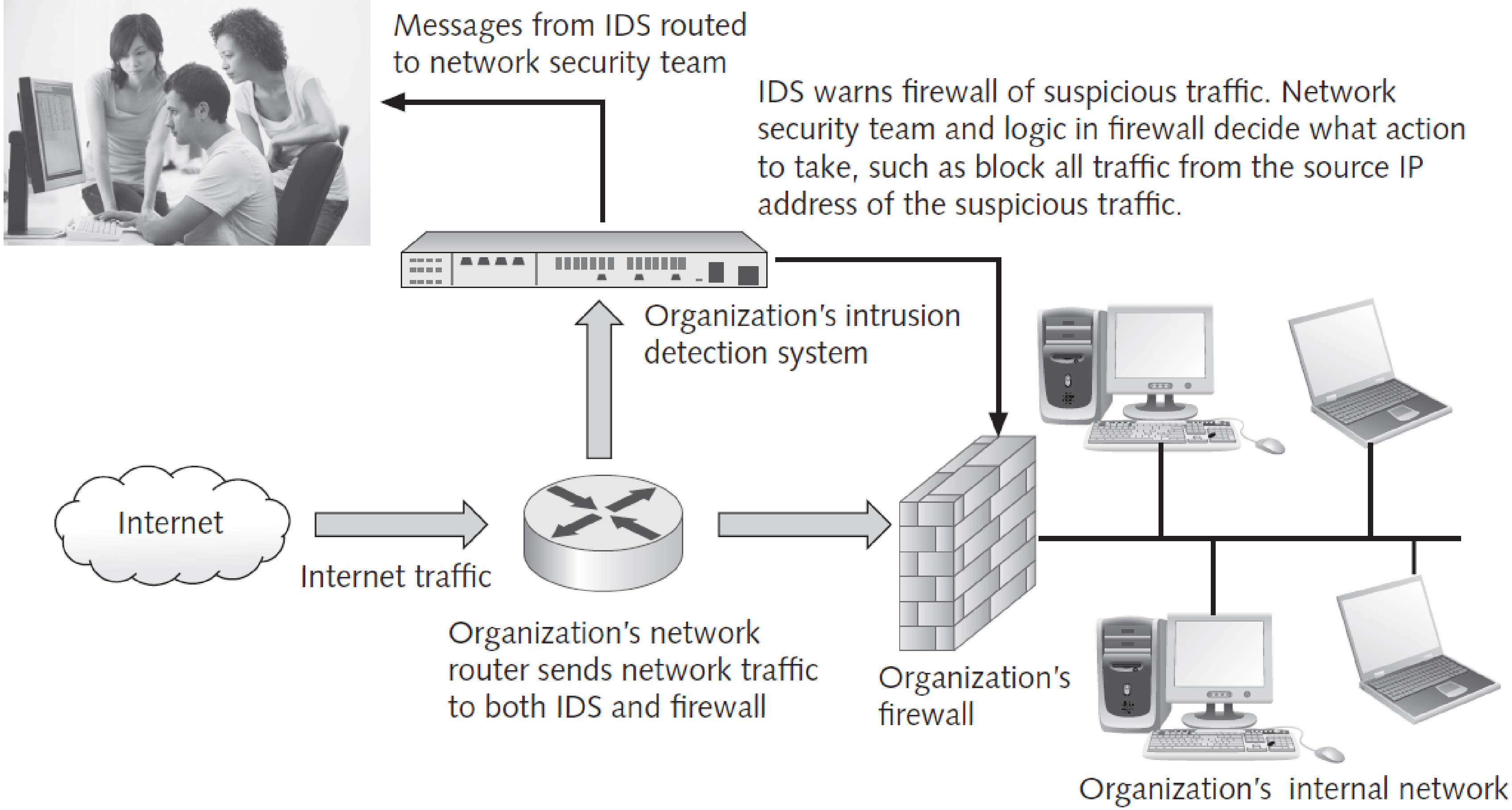
Address critical internet security threats

- High-impact vulnerabilities should be fixed on priority basis

Conducting periodic IT security audits

- **Security audit**: Evaluates whether an organization has a well-considered security policy in place and if it is being followed

Intrusion Detection System



Messages from IDS routed to network security team

IDS warns firewall of suspicious traffic. Network security team and logic in firewall decide what action to take, such as block all traffic from the source IP address of the suspicious traffic.

Organization's intrusion detection system

Internet

Internet traffic

Organization's network router sends network traffic to both IDS and firewall

Organization's firewall

Organization's internal network

Credit: Monkey Business Images/Shutterstock.com.

Detection Systems

Catch Intruders in the Act

Minimize the Impact of Intruders

Response Plan

- Incident notification
  - Define who to notify and who not to notify
  - Refrain from giving out specific information about a compromise in public forums
- Protection of evidence and activity logs
  - Document all details of a security incident to help with future prosecution and incident eradication
- Incident containment
  - Determine if an attack is dangerous enough to warrant shutting down the systems

Response

- Eradication
  - Collect and log all criminal evidence from the system
  - Verify that all backups are current, complete, and free of any virus
- Incident follow-up
  - Determine how the security was compromised
  - Conduct a review to evaluate how the organization responded
  - Create a detailed chronology of all events
  - Estimate the monetary damage

Computer Forensics

- Combines elements of law and computer science to:
  - Identify, collect, examine, and preserve data from computer systems
  - Collect data in a manner that preserves the integrity of the data gathered so that it is admissible as evidence in a court of law

Constitutional acts governing the Collection of Evidence

Summary

- Ethical decisions in determining which information systems and data most need protection
- Most common computer exploits
  - Viruses and worms
  - Trojan horses
  - Distributed denial-of-service attacks
  - Rootkits and spam
  - Phishing and spear-fishing
  - Smishing and vishing

Summary

- Perpetrators include:
  - Hackers
  - Crackers
  - Malicious insider
  - Industrial spies
  - Cybercriminals
  - Hacktivist
  - Cyberterrorists

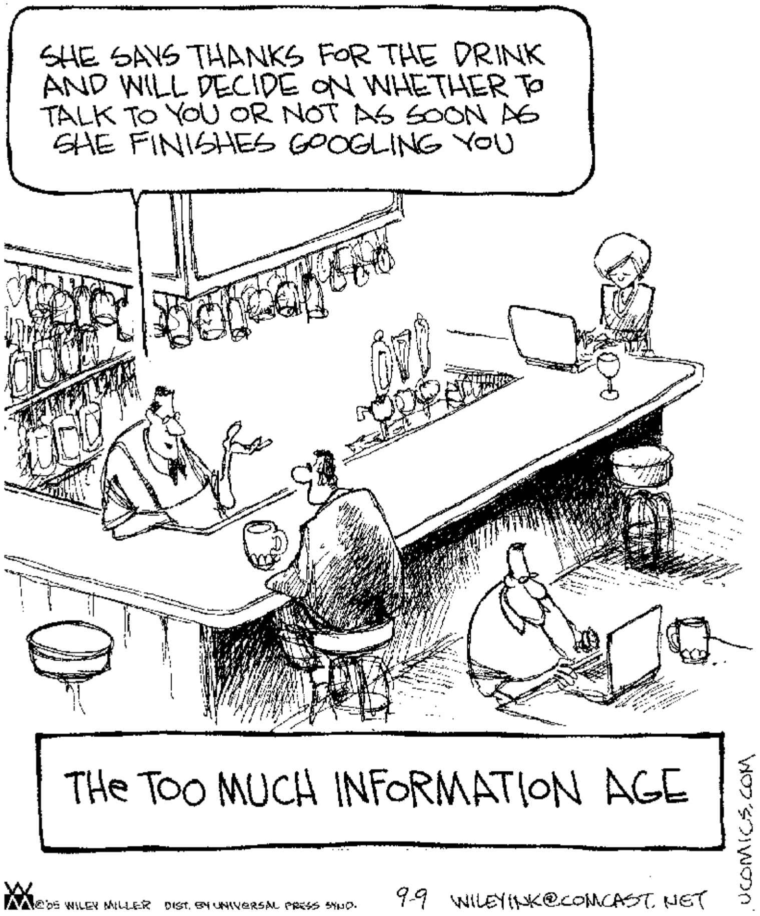
Summary

- Must implement multilayer process for managing security vulnerabilities, including:
  - Assessment of threats
  - Identifying actions to address vulnerabilities
  - User education
- IT must lead the effort to implement:
  - Security policies and procedures
  - Hardware and software to prevent security breaches
- Computer forensics is key to fighting computer crime in a court of law

Discussion

- Develop a strong argument against the adoption of BYOD policy for a large financial services organization.
- Now develop a strong argument in favor of the adoption of BYOD policy
- Do research on the Web to find three DDoS mitigation service providers. How are their services similar? How are they different? Which DDoS service provider do you think is the best?

Privacy


SHE SAYS THANKS FOR THE DRINK AND WILL DECIDE ON WHETHER TO TALK TO YOU OR NOT AS SOON AS SHE FINISHES GOOGLING YOU
THE TOO MUCH INFORMATION AGE
©05 WILEY MILLER DIST. BY UNIVERSAL PRESS SYND.
9-9 WILEYINK@COMCAST.NET
UCOMICS.COM

Privacy Protection and the Law

- **Right of privacy**: Right to be left alone, the most comprehensive of rights, and most valued by free people

Do People Have the Right to Be Left Alone?

PhamousFotos / Splash News/Newscom

Defining Privacy

- Privacy related to notion of access
- Access
  - Physical proximity to a person
  - Knowledge about a person
- Privacy is a “zone of inaccessibility”
- Privacy violations are an affront to human dignity
- Too much individual privacy can harm society
- Where to draw the line?

Case Study: New Parents

- A couple have a baby girl
- Both work; they are concerned about performance of full-time nanny
- Purchase program that allows monitoring through laptop’s camera placed in family room
- They do not inform nanny she is being monitored

Rule Utilitarian Evaluation

- If everyone monitored nannies, it would not remain a secret for long
- Consequences
  - Nannies would be on best behavior in front of camera
  - Might reduce child abuse and parents’ peace of mind
  - Would also increase stress and reduce job satisfaction of child care providers
  - Might result in higher turnover rate and less experienced pool of nannies, who would provide lower-quality care
- If harms appear greater than benefits, we conclude action was wrong or vice versa

Social Contract Theory Evaluation

- It is reasonable for society to give people privacy in their own homes
- Nanny has a reasonable expectation that her interactions with baby inside home are private
- Paul’s decision to secretly monitor the nanny is wrong because it violates her privacy

Kantian Evaluation

- Imagine rule, “An employer may secretly monitor the work of an employee who works with vulnerable people”
- If universalized, there would be no expectation of privacy by employees, so *secret* monitoring would be impossible
- Proposed rule is self-defeating, so it is wrong for Pauls to act according to the rule

Virtue Ethics Evaluation

- Pauls are responsible for well-being of their daughter
- Chose nanny through concern for baby: characteristic of good parents
- Daughter is truly defenseless, unable to communicate with them
- Decision to monitor can be viewed as characteristic of good parents
- Would also expect them to cease monitoring once assured nanny is doing well

Information Privacy

- Combination of communications privacy and data privacy
  - Communications privacy - Ability to communicate with others without those communications being monitored by other persons or organizations
  - Data privacy - Ability to limit access to one's personal data in order to exercise control over that data and its use

Privacy Laws, Applications, and Court Rulings

Key Privacy and Anonymity Issues

- Data breaches
- Electronic discovery
- Consumer profiling
- Workplace monitoring
- Advanced surveillance technology

Data Breaches

- Caused by:
  - Hackers breaking into a database
  - Failure to follow proper security procedures

Electronic Discovery (e-discovery)

- Collection, preparation, review, and production of electronically stored information for use in criminal and civil actions and proceedings
- **Electronically stored information (ESI)**: Any form of digital information stored on any form of electronic storage device
- E-discovery software helps:
  - Analyze large volumes of ESI quickly
  - Simplify and streamline data collection
  - Identify all participants in an investigation to determine who knew what and when

Consumer Profiling

- Information about Web surfers can be obtained through the use of:
  - **Cookies**
  - Tracking software
- Criticism - Personal data may be gathered and sold to other companies without the permission of consumers who provide the data

Workplace Monitoring

- Privacy advocates stress on the need for federal legislation to keep employers from infringing upon the privacy rights of employees

Camera Surveillance

- Goal - Deter crime and terrorist activities
- Criticism - May provide leeway for abuse and blackmail

Stalking App

- Cell phone spy software that can be loaded onto a cell phone or smartphone
- Performs location tracking, records calls, views text messages sent or received, and records the URLs of any Web site visited on the phone
- Illegal to install the software on a phone without the permission of the phone owner

Problem Scenario

- Your friend is going through a tough time with his current significant other and believe she is cheating on him. He is aware of your technical prowess and has asked you to help him purchase and install a stalking app on her cell phone. What would you do?

Problem scenario

- Your friend is considering using an online service to identify people with compatible personalities and attractive physical features who would be interesting to date. Your friend must first submit some basic personal information, then complete a five-page personality survey, and finally provide several recent photos. Would you advice your friend to do this? Why or why not?

Case: Security class

- Prof. Blake teaches computer security. In his computer security class, he teaches students how easy it is to intercept e-mail and IMs. As an assignment, students are required to intercept e-mails and IMs from the university's network and post them to the class blog.
- When Jessica, one of his students, objected to the assignment on the grounds that it was an invasion of privacy, the Prof. disagreed for two reasons:
  - It is very easy to intercept e-mails, so e-mails cannot be considered private
  - The e-mail accounts are on university servers, the contents of which are actually public, so reading them is not a privacy violation

Reflection questions

- When you write e-mail using USIU-A e-mail account, do you expect it to be private? Why?
- Should the Prof. be allowed to continue to use this assignment? Why or why not?
- Should the Prof. be allowed to continue to teach students how to intercept e-mails and IMs, if he does not have students use this skills to actually intercept IMs or e-mails? Why or why not?

Information Disclosures

Public Records

- Public record: information about an incident or action reported to a government agency for purpose of informing the public
- Examples: birth certificates, marriage licenses, motor vehicle records, criminal records, deeds to property
- Computerized databases and Internet have made public records much easier to access

Records Held by Private Organizations

- Credit card purchases
- Purchases made with loyalty cards
- Voluntary disclosures
- Posts to social network sites

Data Gathering and Privacy Implications

- Facebook tags
- Enhanced 911 services (in the US)
- Rewards or loyalty programs
- Body scanners
- RFID tags
- Implanted chips
- OnStar
- Automobile "black boxes" (in the US)
- Medical records
- Digital video recorders
- Cookies and flash cookies

Facebook Tags

- Tag: Label identifying a person in a photo
- Facebook allows users to tag people who are on their list of friends
- About 100 million tags added per day in Facebook
- Facebook uses facial recognition to suggest name of friend appearing in photo
- Does this feature increase risk of improper tagging?

Enhanced 911 Services

- Cell phone providers in United States required to track locations of active cell phones to within 100 meters
- Allows emergency response teams to reach people in distress
- What if this information is sold or shared?

Rewards or Loyalty Programs

- Shoppers who belong to store’s rewards program can save money on many of their purchases
- Computers use information about buying habits to provide personalized service
- Do card users pay less, or do non-users get overcharged?

Body Scanners

- Some department stores have 3-D body scanners
- Computer can use this information to recommend clothes
- Scans can also be used to produce custom-made clothing

Body Scanner Takes Measurements

RFID Tags

- RFID: Radio frequency identification
- An RFID tag is a tiny wireless transmitter
- Manufacturers are replacing bar codes with RFID tags
  - Contain more information
  - Can be scanned more easily
- If tag cannot be removed or disabled, it becomes a tracking device

Implanted Chips

- Taiwan: Every domesticated dog must have an implanted microchip
  - Size of a grain of rice; implanted into ear
  - Chip contains name, address of owner
  - Allows lost dogs to be returned to owners
- RFID tags approved for use in humans
  - Can be used to store medical information
  - Can be used as a "debit card"

OnStar

- OnStar manufactures communication system incorporated into rear-view mirror
- Emergency, security, navigation, and diagnostics services provided subscribers
- Two-way communication and GPS
- Automatic communication when airbags deploy
- Service center can even disable gas pedal

RFID Tags Speed Inventory Process

© Marc F. Henning / Alamy

Automobile “Black Boxes”

- Modern automobiles come equipped with a “black box”
- Maintains data for five seconds:
  - Speed of car
  - Amount of pressure being put on brake pedal
  - Seat belt status
- After an accident, investigators can retrieve and gather information from “black box”

Medical Records

- Advantages of changing from paper-based to electronic medical records
- Quicker and cheaper for information to be shared among caregivers
  - Lower medical costs
  - Improve quality of medical care
- Once information in a database, more difficult to control how it is disseminated

Digital Video Recorders

- TiVo service allows subscribers to record programs and watch them later
- TiVo collects detailed information about viewing habits of its subscribers
- Data collected second by second, making it valuable to advertisers and others interested in knowing viewing habits

Cookies

- Cookie: File placed on computer's hard drive by a Web server
- Contains information about visits to a Web site
- Allows Web sites to provide personalized services
- Put on hard drive without user's permission
- You can set Web browser to alert you to new cookies or to block cookies entirely

Flash Cookies

- Flash cookie: File placed on your computer's hard drive by a Web server running the Adobe Flash Player
- Flash cookie can hold 25 times as much information as a browser cookie
- Flash cookies not controlled by browser's privacy controls
- Some Web sites use flash cookies as a way of backing up browser cookies. If you delete browser cookie, it can be "respawned" from the flash cookie
- Half of 100 most popular Web sites use flash cookies

CASE: MICHAEL'S ESSAY