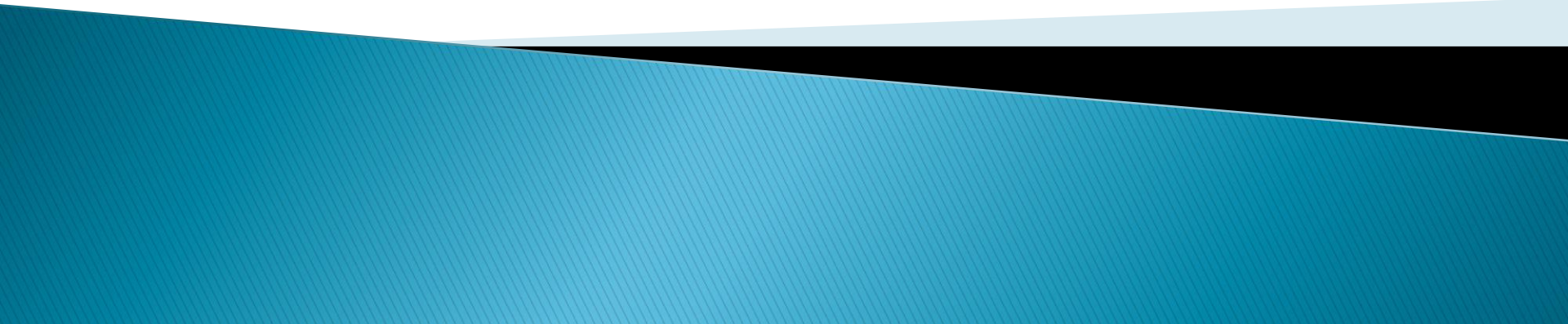


# Ethics in Information Technology, Fourth Edition

## *Chapter 3* *Computer and Internet Crime*



# Objectives

- ▶ As you read this chapter, consider the following questions:
  - What key trade-offs and ethical issues are associated with the safeguarding of data and information systems?
  - Why has there been a dramatic increase in the number of computer-related security incidents in recent years?
  - What are the most common types of computer security attacks?



# Why Computer Incidents Are So Prevalent

- ▶ Increasing complexity increases vulnerability
  - Computing environment is enormously complex
    - Continues to increase in complexity
    - Number of entry points expands continuously
    - Cloud computing and virtualization software
- ▶ Higher computer user expectations
  - Computer help desks under intense pressure
    - Forget to verify users' IDs or check authorizations
- ▶ Computer users share login IDs and passwords



# Why Computer Incidents Are So Prevalent (cont'd.)

- ▶ Increased reliance on commercial software with known vulnerabilities
  - Exploit
    - Attack on information system
    - Takes advantage of system vulnerability
    - Due to poor system design or implementation
  - Patch
    - “Fix” to eliminate the problem
    - Users are responsible for obtaining and installing
    - Delays expose users to security breaches
- ▶ Zero-day attack
  - Before a vulnerability is discovered or fixed



# Why Computer Incidents Are So Prevalent (cont'd.)

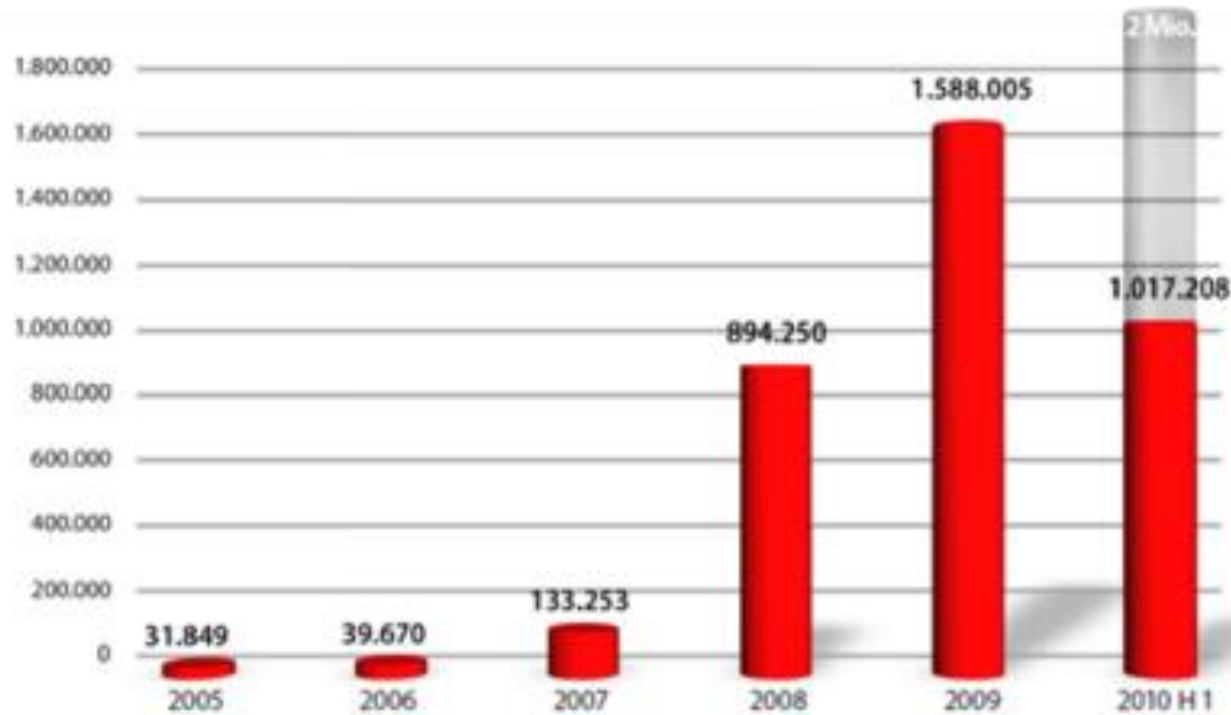


Diagram 1: Number of new malware programs per year since 2005 and in first half of 2010

# Types of Exploits

- ▶ Computers as well as smartphones can be target
- ▶ Types of attacks
  - Virus
  - Worm
  - Trojan horse
  - Distributed denial of service
  - Rootkit
  - Spam
  - Phishing (spear-phishing, smishing, and vishing)



# Viruses

- ▶ Pieces of programming code
- ▶ Usually disguised as something else
- ▶ Cause unexpected and undesirable behavior
- ▶ Often attached to files
- ▶ Deliver a “payload”
- ▶ Spread by actions of the “infected” computer user
  - Infected e-mail document attachments
  - Downloads of infected programs
  - Visits to infected Web sites



# Worms

- ▶ Harmful programs
  - Reside in active memory of a computer
  - Duplicate themselves
- ▶ Can propagate without human intervention
- ▶ Negative impact of worm attack
  - Lost data and programs
  - Lost productivity
  - Additional effort for IT workers





# Trojan Horses

- ▶ Malicious code hidden inside seemingly harmless programs
- ▶ Users are tricked into installing them
- ▶ Delivered via email attachment, downloaded from a Web site, or contracted via a removable media device
- ▶ Logic bomb
  - Executes when triggered by certain event



# Distributed Denial-of-Service (DDoS) Attacks

- ▶ Malicious hacker takes over computers on the Internet and causes them to flood a target site with demands for data and other small tasks
  - The computers that are taken over are called zombies
  - Botnet is a very large group of such computers
- ▶ Does not involve a break-in at the target computer
  - Target machine is busy responding to a stream of automated requests
  - Legitimate users cannot access target machine



# Rootkits

- ▶ Set of programs that enables its user to gain administrator-level access to a computer without the end user's consent or knowledge
- ▶ Attacker can gain full control of the system and even obscure the presence of the rootkit
- ▶ Fundamental problem in detecting a rootkit is that the operating system currently running cannot be trusted to provide valid test results



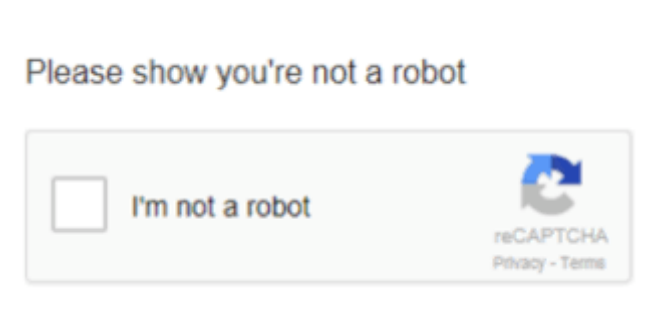
# Spam

- ▶ Abuse of email systems to send unsolicited email to large numbers of people
  - Low-cost commercial advertising for questionable products
  - Method of marketing also used by many legitimate organizations
- ▶ Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act
  - Legal to spam if basic requirements are met



# Spam (cont'd.)

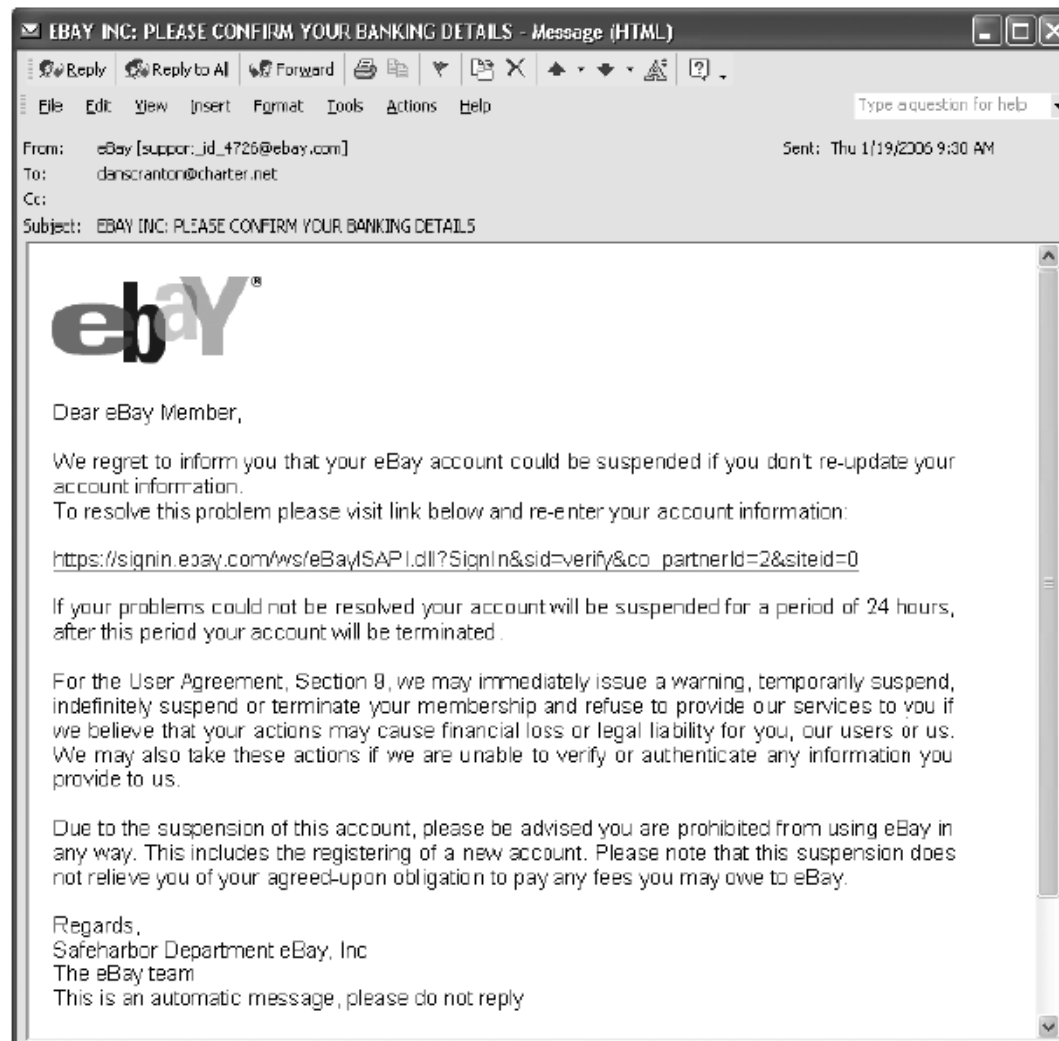
- ▶ Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA)
  - Software generates tests that humans can pass but computer programs cannot



# Phishing

- ▶ Act of using email fraudulently to try to get the recipient to reveal personal data
- ▶ Legitimate-looking emails lead users to counterfeit Web sites
- ▶ Spear-phishing
  - Fraudulent emails to an organization's employees
- ▶ Smishing
  - Phishing via text messages
- ▶ Vishing
  - Phishing via voice mail messages





**FIGURE 3-3** Example of phishing

Source Line: Course Technology/Cengage Learning.

# Types of Perpetrators (cont'd.)

**TABLE 3-4** Classifying perpetrators of computer crime

| Type of perpetrator | Typical motives  |
|---------------------|--|
| Hacker              | Test limits of system and/or gain publicity  |
| Cracker             | Cause problems, steal data, and corrupt systems  |
| Malicious insider   | Gain financially and/or disrupt company's information systems and business operations                |
| Industrial spy      | Capture trade secrets and gain competitive advantage   |
| Cybercriminal       | Gain financially   |
| Hacktivist          | Promote political ideology   |
| Cyberterrorist      | Destroy infrastructure components of financial institutions, utilities, and emergency response units |

Source Line: Course Technology/Cengage Learning.





# Hackers and Crackers

## ▶ Hackers

- Test limitations of systems out of intellectual curiosity
  - Some smart and talented
  - Others inept; termed “lamers” or “script kiddies”

## ▶ Crackers

- Cracking is a form of hacking
- Clearly criminal activity



# Malicious Insiders

- ▶ Major security concern for companies
- ▶ Fraud within an organization is usually due to weaknesses in internal control procedures
- ▶ Collusion
  - Cooperation between an employee and an outsider
- ▶ Insiders are not necessarily employees
  - Can also be consultants and contractors
- ▶ Extremely difficult to detect or stop
  - Authorized to access the very systems they abuse
- ▶ Negligent insiders have potential to cause damage



# Industrial Spies

- ▶ Use illegal means to obtain trade secrets from competitors
- ▶ Trade secrets are protected by the Economic Espionage Act of 1996
- ▶ Competitive intelligence
  - Uses legal techniques
  - Gathers information available to the public
- ▶ Industrial espionage
  - Uses illegal means
  - Obtains information not available to the public



# Cybercriminals

- ▶ Hack into corporate computers to steal
- ▶ Engage in all forms of computer fraud
- ▶ Chargebacks are disputed transactions
- ▶ Loss of customer trust has more impact than fraud
- ▶ To reduce potential for 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



# Cybercriminals (cont'd.)

## ▶ Smart cards

- Contain a memory chip
- Updated with encrypted data each time card is used
- Used widely in Europe
- Not widely used in the U.S.



# Hacktivists and Cyberterrorists

## ▶ Hacktivism

- Hacking to achieve a political or social goal

## ▶ Cyberterrorist

- Attacks computers or networks in an attempt to intimidate or coerce a government in order to advance certain political or social objectives
- Seeks to cause harm rather than gather information
- Uses techniques that destroy or disrupt services



# Federal Laws for Prosecuting Computer Attacks

**TABLE 3-5** Federal laws that address computer crime

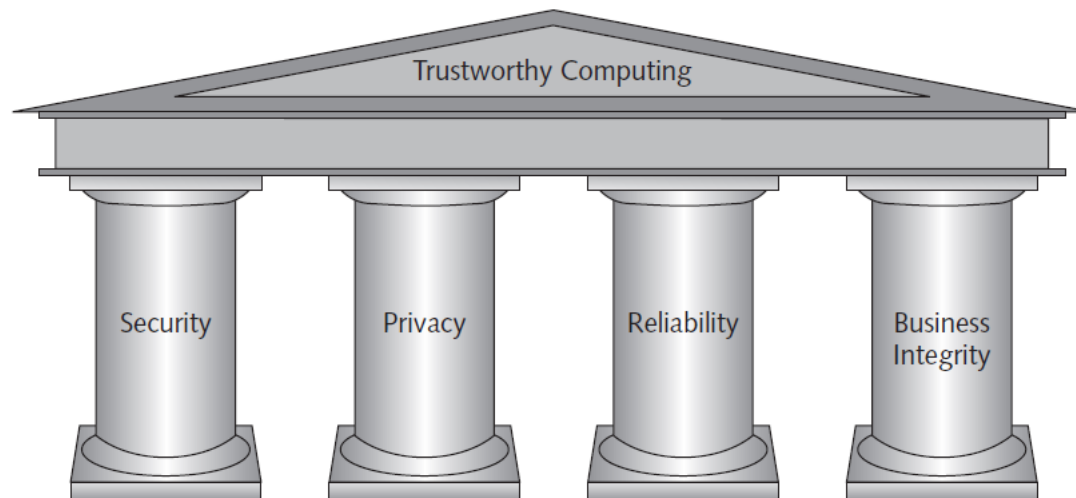
| Federal law   | Subject area  |
|---|---|
| USA Patriot Act   | Defines cyberterrorism and penalties  |
| Identity Theft and Assumption Deterrence Act (U.S. Code Title 18, Section 1028)                                       | Makes identity theft a Federal crime with penalties up to 15 years imprisonment and a maximum fine of \$250,000   |
| Fraud and Related Activity in Connection with Access Devices Statute (U.S. Code Title 18, Section 1029)               | False claims regarding unauthorized use of credit cards   |
| Computer Fraud and Abuse Act (U.S. Code Title 18, Section 1030)   | Fraud and related activities in association with computers: <ul style="list-style-type: none"><li>• Accessing a computer without authorization or exceeding authorized access</li><li>• Transmitting a program, code, or command that causes harm to a computer</li><li>• Trafficking of computer passwords</li><li>• Threatening to cause damage to a protected computer</li></ul> |
| Stored Wire and Electronic Communications and Transactional Records Access Statutes (U.S. Code Title 18, Chapter 121) | Unlawful access to stored communications to obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage   |

Source Line: Course Technology/Cengage Learning.



# Implementing Trustworthy Computing

- ▶ Trustworthy computing
  - Delivers secure, private, and reliable computing
  - Based on sound business practices



**FIGURE 3-4** Microsoft's four pillars of trustworthy computing

Source Line: Course Technology/Cengage Learning.



# Risk Assessment (cont'd.)

**TABLE 3-7** Risk assessment for hypothetical company

| <b>Risk</b>                          | <b>Business objective threatened</b> | <b>Estimated probability of such an event occurring</b> | <b>Estimated cost of a successful attack</b> | <b>Probability × cost = expected cost</b> | <b>Assessment of current level of protection</b> | <b>Relative priority to be fixed</b> |
|--------------------------------------|--------------------------------------|---|--|---|--|--------------------------------------|
| Distributed denial-of-service attack | 24/7 operation of a retail Web site  | 40%   | \$500,000                                    | \$200,000                                 | Poor   | 1                                    |

(Continued)



# Risk Assessment (cont'd.)

| Risk                               | Business objective threatened                                   | Estimated probability of such an event occurring | Estimated cost of a successful attack | Probability × cost = expected cost | Assessment of current level of protection | Relative priority to be fixed |
|------------------------------------|---|--|---------------------------------------|------------------------------------|---|-------------------------------|
| Email attachment with harmful worm | Rapid and reliable communications among employees and suppliers | 70%  | \$200,000                             | \$140,000                          | Poor                                      | 2                             |
| Harmful virus                      | Employees' use of personal productivity software                | 90%  | \$50,000                              | \$45,000                           | Good                                      | 3                             |
| Invoice and payment fraud          | Reliable cash flow  | 10%  | \$200,000                             | \$20,000                           | Excellent                                 | 4                             |

Source Line: Course Technology/Cengage Learning.

“Ethics in information technology” Reynolds, Chapter 3

US



# Prevention

- ▶ Implement a layered security solution
  - Make computer break-ins harder
- ▶ Installing a corporate firewall
  - Limits network access
- ▶ Intrusion prevention systems
  - Block viruses, malformed packets, and other threats
- ▶ Installing antivirus software
  - Scans for sequence of bytes or virus signature
  - United States Computer Emergency Readiness Team (US-CERT) serves as clearinghouse




# Prevention (cont'd.)

- ▶ Safeguards against attacks by malicious insiders
  - Departing employees and contractors
    - Promptly delete computer accounts, login IDs, and passwords
  - Carefully define employee roles and separate key responsibilities
  - Create roles and user accounts to limit authority



# Computer Forensics

- ▶ Combines elements of law and computer science to identify, collect, examine, and preserve data and preserve its integrity so it is admissible as evidence
- ▶  Computer forensics investigation requires extensive training and certification and knowledge of laws that apply to gathering of criminal evidence



# Summary

- ▶ Ethical decisions in determining which information systems and data most need protection
- ▶ Most common computer exploits
  - Viruses
  - Worms
  - Trojan horses
  - Distributed denial-of-service attacks
  - Rootkits
  - Spam
  - Phishing, spear-fishing, smishing, vishing



# Summary (cont'd.)

## ▶ Perpetrators include:

- Hackers
- Crackers
- Malicious insider
- Industrial spies
- Cybercriminals
- Hacktivist
- Cyberterrorists



# Summary (cont'd.)

- ▶ Personal safety on internet:
  - Bank accounts, data accounts with multilayer security verification
- ▶ Company/business accounts:
  - Reputed financial institutions only
  - Limit access
  - Layered security through anti-virus, firewalls, VPNs
  - Mandatory to protect data related to financial institution, health and federal agencies





# Summary (cont'd.)

- ▶ 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

