電子商務安全
Secure Electronic Commerce

電子商務安全
(E-Commerce Security)

992SEC09
TGMXM0A
Fri. 6,7,8 (13:10-16:00) L526

Min-Yuh Day
戴敏育
Assistant Professor
專任助理教授
Dept. of Information Management, Tamkang University
淡江大學 資訊管理學系

http://mail.im.tku.edu.tw/~myday/

2011-04-29

Syllabus

週次 月／日　內容（Subject/Topics

1　100/02/18　電子商務安全課程簡介
(Course Orientation for Secure Electronic Commerce)

2　100/02/25　電子商務概論 (Introduction to E-Commerce)

3　100/03/04　電子市集 (E-Marketplaces)

4　100/03/11　電子商務環境下之零售：產品與服務
(Retailing in Electronic Commerce: Products and Services)

5　100/03/18　網路消費者行為、市場研究與廣告
(Online Consumer Behavior, Market Research, and Advertisement)

6　100/03/25　電子商務 B2B、B2C、C2C (B2B, B2C, C2C E-Commerce)

7　100/04/01　Web 2.0, Social Network, Social Media

8　100/04/08　教學行政觀摩日

9　100/04/15　行動運算與行動商務 (Mobile Computing and Commerce)

10　100/04/22　期中考試週

Syllabus (cont.)

週次	月／日	內容（Subject/Topics
11	100/04/29	電子商務安全 (E-Commerce Security)
12	100/05/06	數位憑證 (Digital Certificate)
13	100/05/13	網路與網站安全 (Network and Website Security)
14	100/05/20	交易安全、系統安全、IC卡安全、電子付款 (Transaction Security, System Security, IC Card Security, Electronic Commerce Payment Systems)
15	100/05/27	行動商務安全 (Mobile Commerce Security)
16	100/06/03	電子金融安全控管機制 (E-Finance Security Control Mechanisms)
17	100/06/10	營運安全管理 (Operation Security Management)
18	100/06/17	期末考試週

Chapter 9
E-Commerce Security and Fraud Protection

Source: Turban et al.,
Introduction to Electronic Commerce,
Third Edition, 2010, Pearson

LEARNING OBJECTIVES

1. Understand the importance and scope of the security of information systems for EC.
2. Describe the major concepts and terminology of EC security.
3. Learn about the major EC security threats, vulnerabilities, and risks.
4. Understand phishing and its relationship to financial crimes.
5. Describe the information assurance security principles.

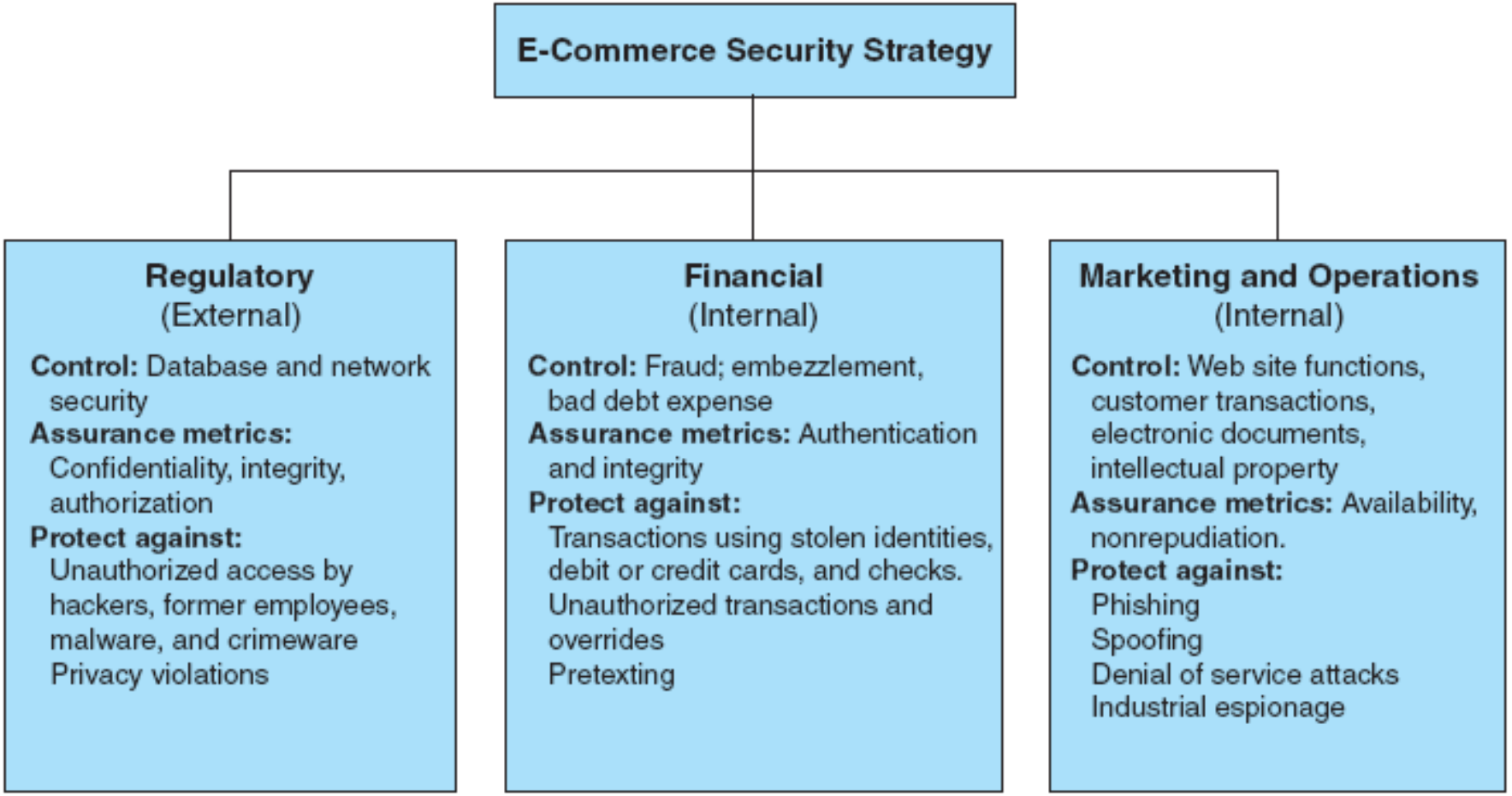
(Source: Turban et al., 2010)

LEARNING OBJECTIVES

6. Identify and assess major technologies and methods for securing EC communications.
7. Describe the major technologies for protection of EC networks.
8. Describe various types of controls and special defense mechanisms.
9. Describe the role of business continuity and disaster recovery planning.
10. Discuss EC security enterprise-wide implementation issues.
11. Understand why it is not possible to stop computer crimes.

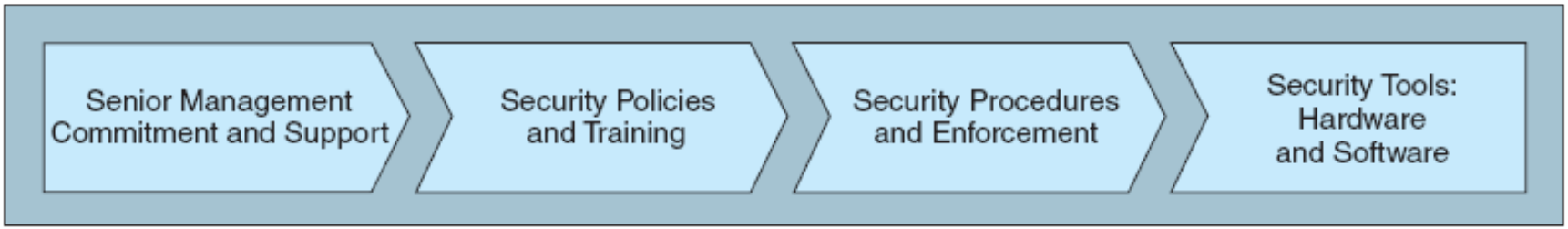
(Source: Turban et al., 2010)

E-Commerce Security Framework



(Source: Turban et al., 2010)

Enterprise-wide EC Security and Privacy Model



(Source: Turban et al., 2010)

THE INFORMATION SECURITY PROBLEM

- **WHAT IS EC SECURITY?**
  - *Computer security* refers to the protection of data, networks, computer programs, computer power, and other elements of computerized information systems

(Source: Turban et al., 2010)

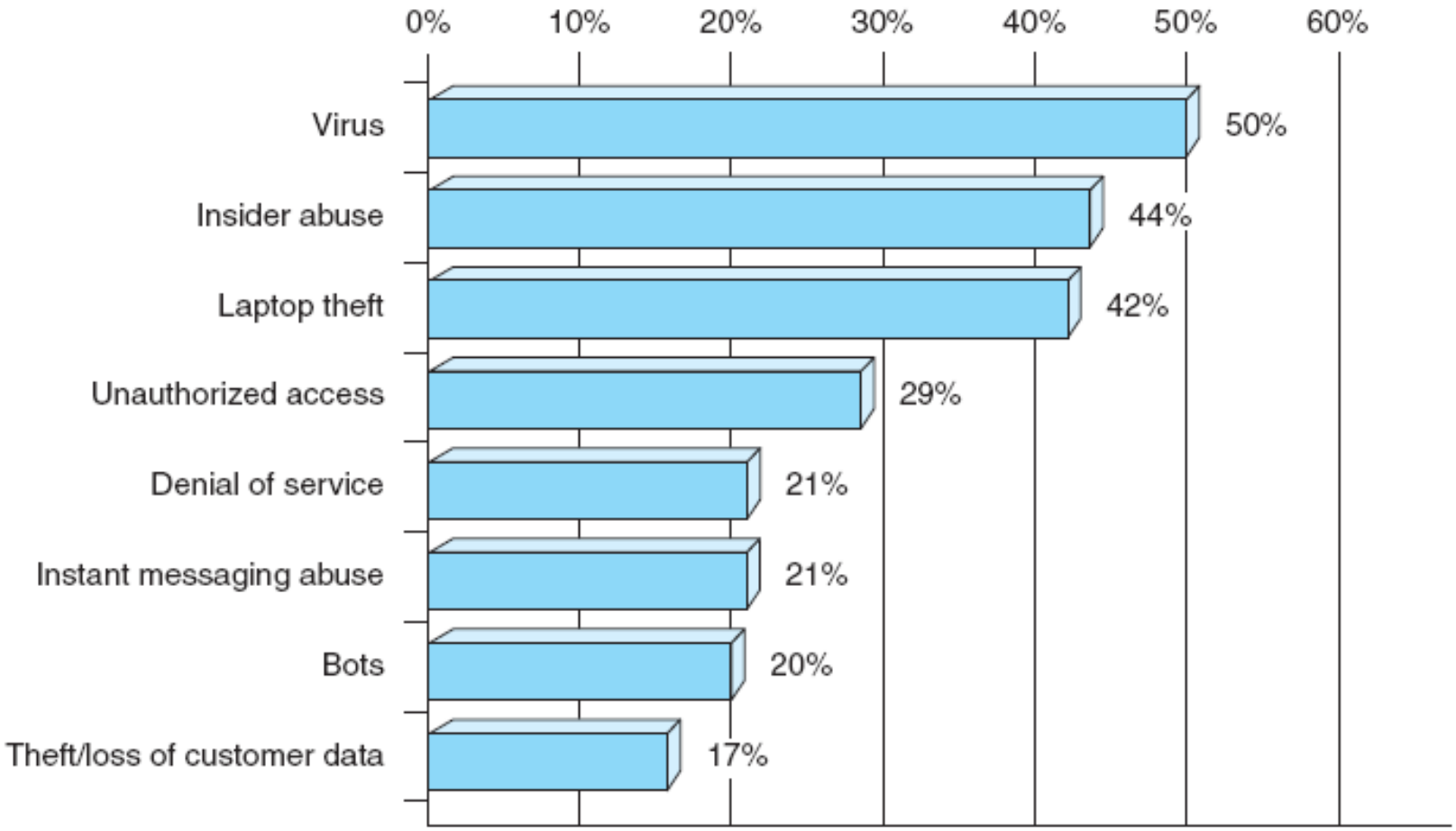
The Status of Computer Security in the United States

- **CSI Computer Crime and Security Survey**

  Annual security survey of U.S. corporations, government agencies, financial and medical institutions, and universities conducted by the Computer Security Institute.
- **National Security**
  - Cyber Security Preparedness and the National Cyber Alert System
  - US-CERT Operations
  - National Cyber Response Coordination Group
  - CyberCop Portal

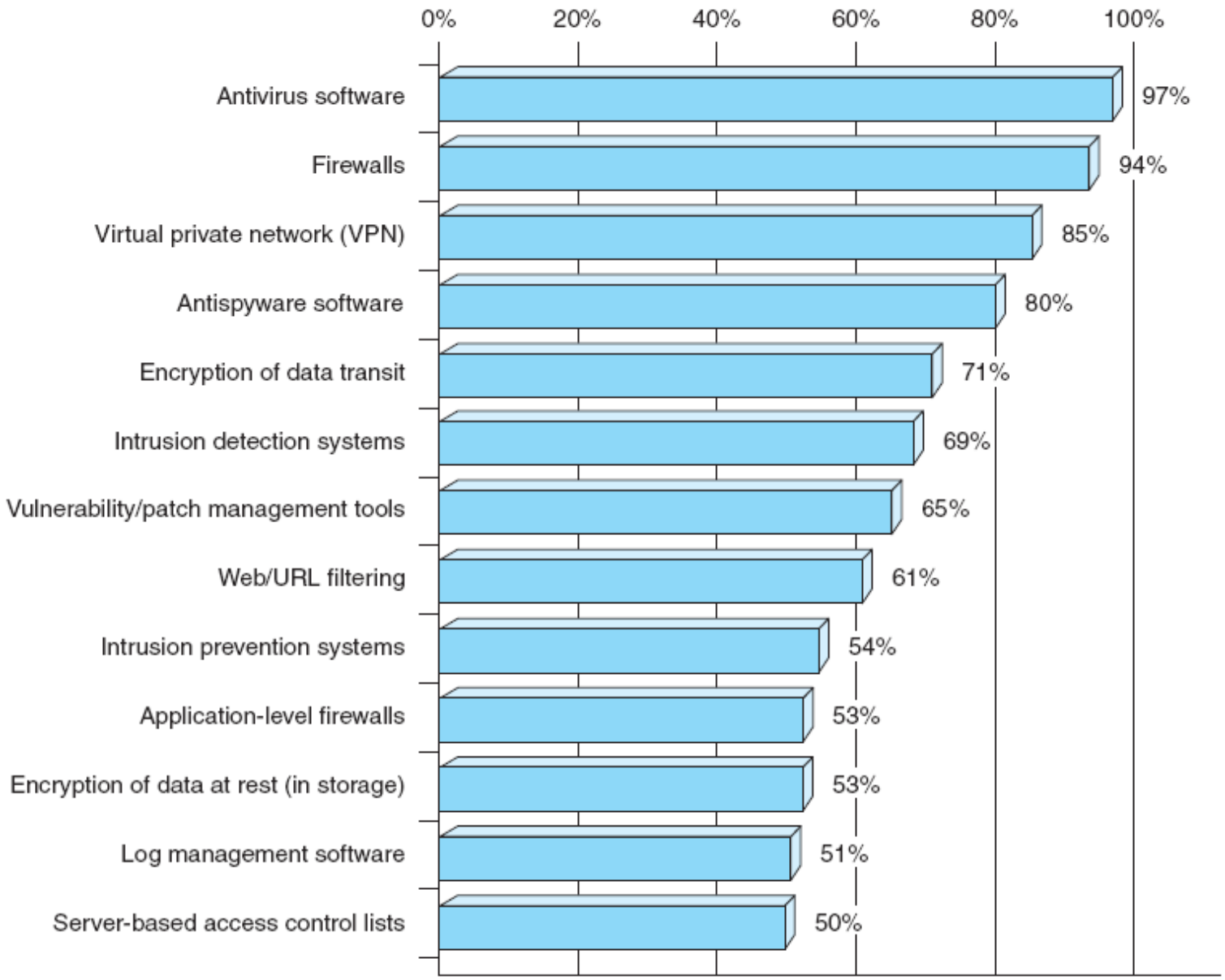
(Source: Turban et al., 2010)

EXHIBIT 9.1 Major Computer Attack Incidents in 2008



(Source: Turban et al., 2010)

EXHIBIT 9.2 Major Security Methods Used in 2008



(Source: Turban et al., 2010)

THE DRIVERS OF EC SECURITY PROBLEMS

- **The Internet's Vulnerable Design**
- **The Shift to Profit-Induced Crimes**
- **Internet Underground Economy**
- **The Dynamic Nature of EC Systems and the Role of Insiders**

(Source: Turban et al., 2010)

The Internet's Vulnerable Design

- **domain name system (DNS)**

  Translates (converts) domain names to their numeric IP addresses.

- **IP address**

  An address that uniquely identifies each computer connected to a network or the Internet.

(Source: Turban et al., 2010)

Internet underground economy

- **Internet underground economy**

  E-markets for stolen information made up of thousands of Web sites that sell credit card numbers, social security numbers, other data such as numbers of bank accounts, social network IDs, passwords, and much more.

  - **keystroke logging (keylogging)**

    A method of capturing and recording user keystrokes.

(Source: Turban et al., 2010)

WHY IS E-COMMERCE SECURITY STRATEGY NEEDED?

- **Three categories of Computer Security**
  - **Threats**
    - **Unintentional**
    - **Intentional**
      - **Cybercrimes**
  - **Defense**
  - **Management**

- **The Computer Security Dilemma**

(Source: Turban et al., 2010)

BASIC E-COMMERCE SECURITY ISSUES AND LANDSCAPE

- **THE SECURITY BASIC TERMINOLOGY**
  - **business continuity plan**

    A plan that keeps the business running after a disaster occurs. Each function in the business should have a valid recovery capability plan.
  - **cybercrime**

    Intentional crimes carried out on the Internet.
  - **exposure**

    The estimated cost, loss, or damage that can result if a threat exploits a vulnerability.
  - **fraud**

    Any business activity that uses deceitful practices or devices to deprive another of property or other rights.

(Source: Turban et al., 2010)

BASIC E-COMMERCE SECURITY ISSUES AND LANDSCAPE

- **THE SECURITY BASIC TERMINOLOGY (cont.)**
  - **malware (malicious software)**

    A generic term for malicious software.
  - **phishing**

    A crimeware technique to steal the identity of a target company to get the identities of its customers.
  - **risk**

    The probability that a vulnerability will be known and used.
  - **social engineering**

    A type of nontechnical attack that uses some ruse to trick users into revealing information or performing an action that compromises a computer or network.

(Source: Turban et al., 2010)

BASIC E-COMMERCE SECURITY ISSUES AND LANDSCAPE

- **THE SECURITY BASIC TERMINOLOGY (cont.)**
  - **spam**

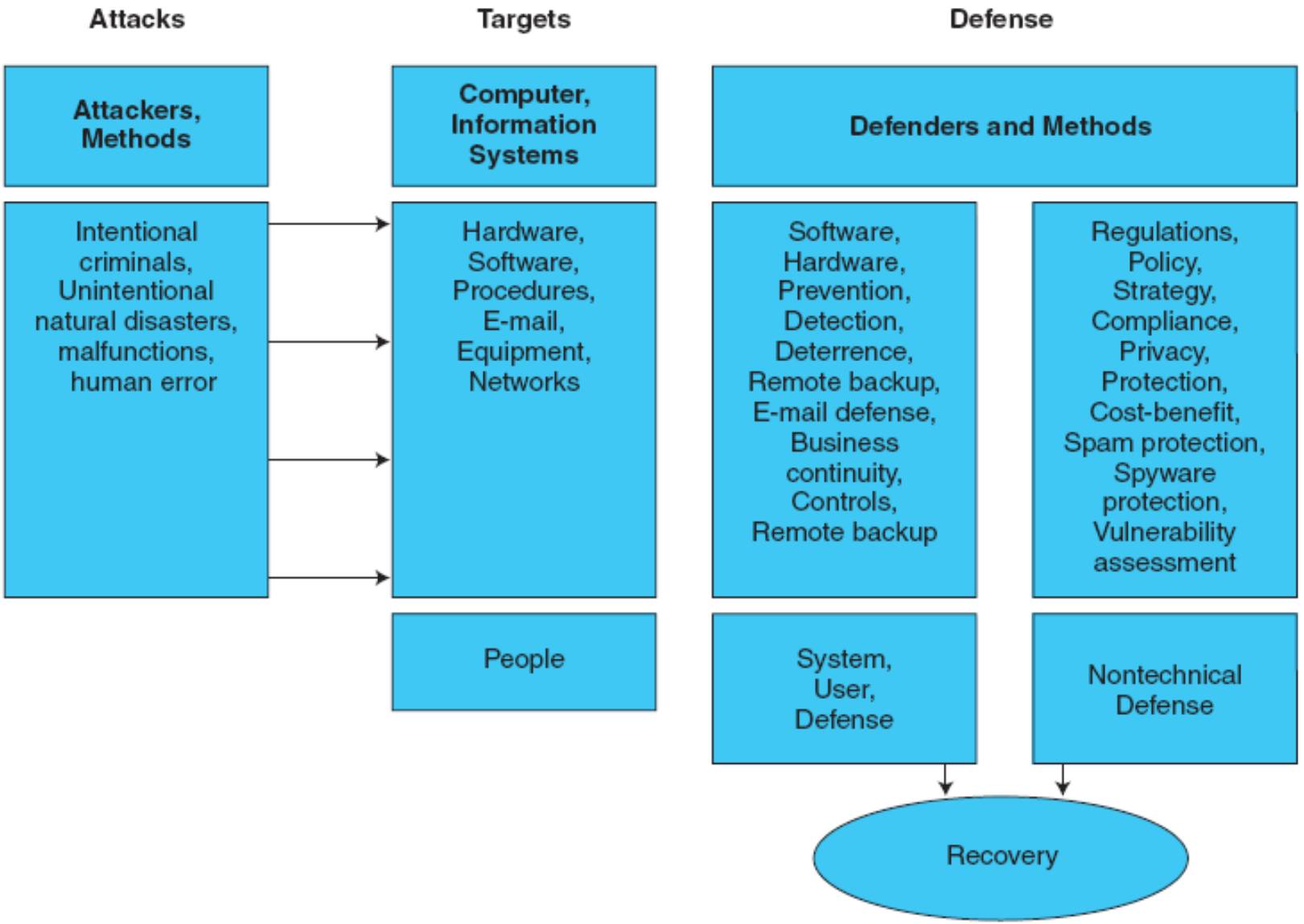
    The electronic equivalent of junk mail.
  - **vulnerability**

    Weakness in software or other mechanism that threatens the confidentiality, integrity, or availability of an asset (recall the CIA model). It can be directly used by a hacker to gain access to a system or network.
  - **zombies**

    Computers infected with malware that are under the control of a spammer, hacker, or other criminal.

(Source: Turban et al., 2010)

EXHIBIT 9.3 The EC Security Battleground



(Source: Turban et al., 2010)

Threats and Attacks: Unintentional and Intentional

- Unintentional Threats
  - Human error
  - Environmental hazards
  - Malfunctions in the computer system
- Intentional Attacks and Crimes

(Source: Turban et al., 2010)

Criminals and Social Engineering

- **cybercriminal**

  A person who intentionally carries out crimes over the Internet.
- **hacker**

  Someone who gains unauthorized access to a computer system.
- **cracker**

  A malicious hacker, such as Maxwell in the opening case, who may represent a serious problem for a corporation.
- **Social Engineering**

  A Collection of tactics used to manipulate people into performing actions or divulging confidential informaiton.

(Source: Turban et al., 2010)

Vulnerable Areas Are Being Attacked

- **Vulnerability**
  - **Common Vulnerabilities and Exposures (CVE)**
    - **Vulnerabilities create risk**
    - **Exposure can result if a threat exploit a vulnerability**

(Source: Turban et al., 2010)

EC Security Requirements

- **Authentication**

  Process to verify (assure) the real identity of an individual, computer, computer program, or EC Web site.

- **Authorization**

  Process of determining what the authenticated entity is allowed to access and what operations it is allowed to perform.

- Auditing
- Availability
- **Nonrepudiation**

  Assurance that online customers or trading partners cannot falsely deny (repudiate) their purchase or transaction.

(Source: Turban et al., 2010)

THE DEFENSE: DEFENDERS AND THEIR STRATEGY

- **EC Defense Programs and Strategy**
- **Defense Methods and Technologies**
- **Recovery**

(Source: Turban et al., 2010)

EC Defense Programs and Strategy

- **EC security strategy**

  A strategy that views EC security as the process of preventing and detecting unauthorized use of the organization's brand, identity, Web site, e-mail, information, or other asset and attempts to defraud the organization, its customers, and employees.

(Source: Turban et al., 2010)

EC Defense Programs and Strategy

- **deterring measures**

  Actions that will make criminals abandon their idea of attacking a specific system (e.g., the possibility of losing a job for insiders).
- **prevention measures**

  Ways to help stop unauthorized users (also known as "intruders") from accessing any part of the EC system.
- **detection measures**

  Ways to determine whether intruders attempted to break into the EC system, whether they were successful, and what they may have done.

(Source: Turban et al., 2010)

EC Defense Programs and Strategy

- **information assurance (IA)**

  The protection of information systems against unauthorized access to or modification of information whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

(Source: Turban et al., 2010)

TECHNICAL ATTACK METHODS

- **TECHNICAL AND NONTECHNICAL ATTACKS: AN OVERVIEW**
  - Software and systems knowledge are used to perpetrate *technical attacks* (computer virus)
  - *Nontechnical attacks* are those in which a perpetrator uses some form of deception or persuasion to trick people into revealing information or performing actions that can compromise the security of a network

(Source: Turban et al., 2010)

TECHNICAL ATTACK METHODS

- **MALICIOUS CODE**
  - **virus**

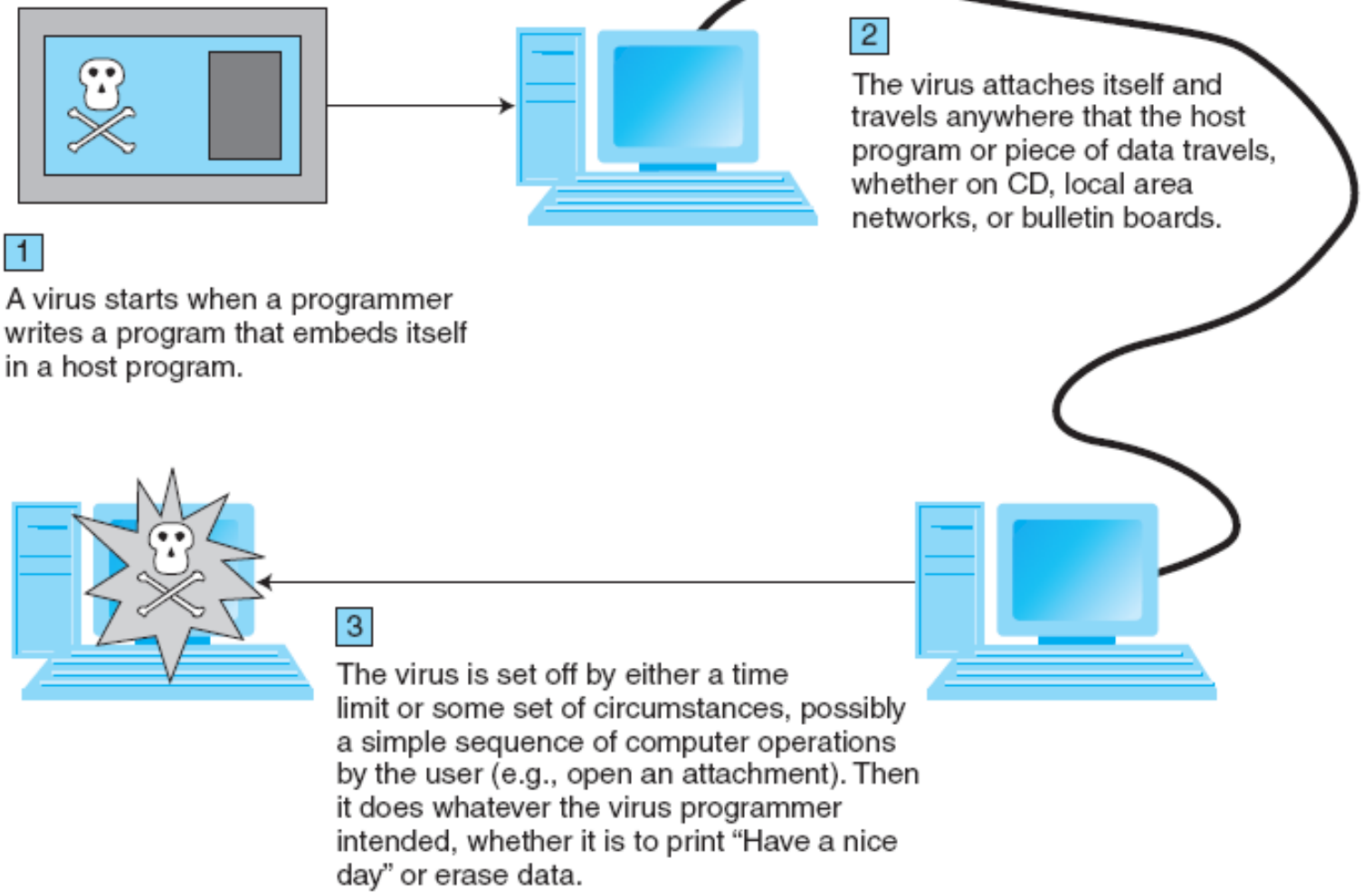
    A piece of software code that inserts itself into a host, including the operating systems, in order to propagate; it requires that its host program be run to activate it.
  - **worm**

    A software program that runs independently, consuming the resources of its host in order to maintain itself, that is capable of propagating a complete working version of itself onto another machine.

(Source: Turban et al., 2010)

EXHIBIT 9.4 How a Computer Virus Can Spread

Just as a biological virus disrupts living cells to cause disease, a computer virus—introduced maliciously—invades the inner workings of computers and disrupts normal operations of the machines.



(Source: Turban et al., 2010)

TECHNICAL ATTACK METHODS

- **macro virus (macro worm)**

  A macro virus or macro worm is executed when the application object that contains the macro is opened or a particular procedure is executed.
- **Trojan horse**

  A program that appears to have a useful function but that contains a hidden function that presents a security risk.
- **banking Trojan**

  A Trojan that comes to life when computer owners visit one of a number of online banking or e-commerce sites.

(Source: Turban et al., 2010)

TECHNICAL ATTACK METHODS

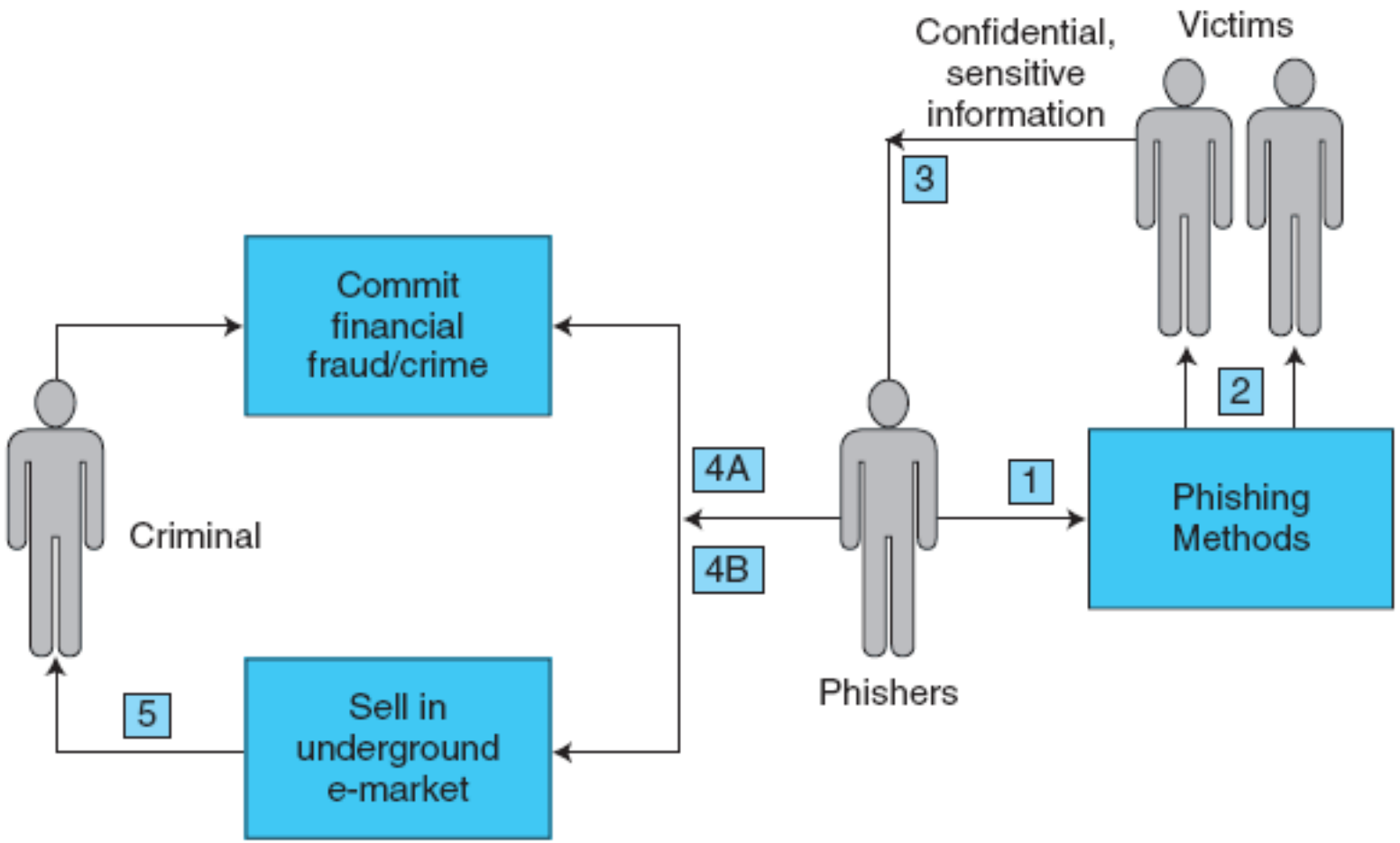
- **denial of service (DoS) attack**

  An attack on a Web site in which an attacker uses specialized software to send a flood of data packets to the target computer with the aim of overloading its resources.
- **Web Server and Web Page Hijacking**
- **botnet**

  A huge number (e.g., hundreds of thousands) of hijacked Internet computers that have been set up to forward traffic, including spam and viruses, to other computers on the Internet.

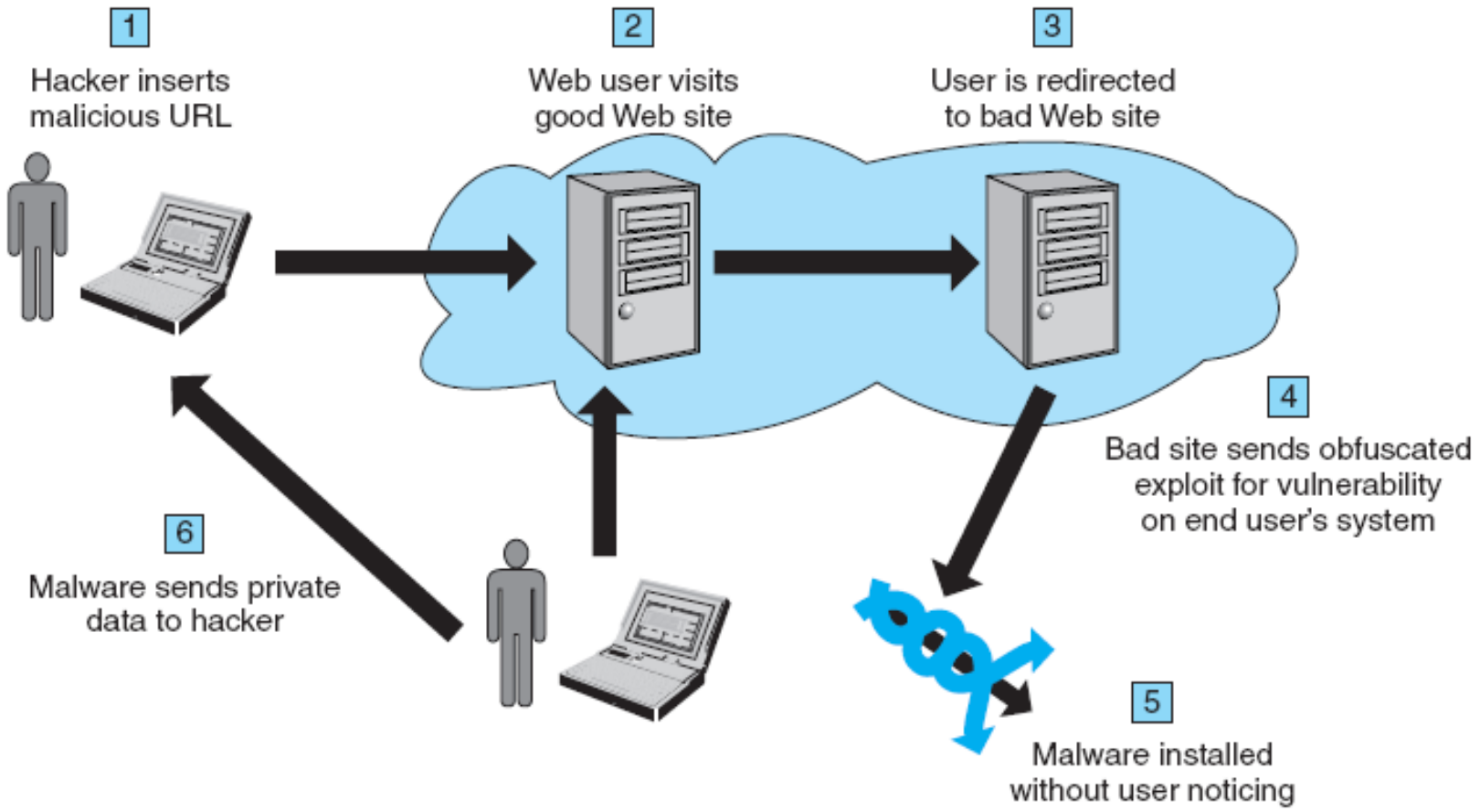
(Source: Turban et al., 2010)

EXHIBIT 9.5 From Phishing to Financial Fraud and Crime



(Source: Turban et al., 2010)

EXHIBIT 9.6 How Phishing Is Accomplished



(Source: Turban et al., 2010)

PHISHING, FINANCIAL FRAUD, AND SPAM

- **FRAUD ON THE INTERNET**
  - **Examples of Typical Online Fraud Attempts**
  - **identity theft**

    Fraud that involves stealing an identity of a person and then the use of that identity by someone pretending to be someone else in order to steal money or get other benefits.
  - **Other Financial Fraud**

(Source: Turban et al., 2010)

PHISHING, FINANCIAL FRAUD, AND SPAM

- **SPAM AND SPYWARE ATTACKS**
  - **e-mail spam**

    A subset of spam that involves nearly identical messages sent to numerous recipients by e-mail.
  - **spyware**

    Software that gathers user information over an Internet connection without the user's knowledge.

(Source: Turban et al., 2010)

PHISHING, FINANCIAL FRAUD, AND SPAM

- **search engine spam**

  Pages created deliberately to trick the search engine into offering inappropriate, redundant, or poor-quality search results.
- **spam site**

  Page that uses techniques that deliberately subvert a search engine's algorithms to artificially inflate the page's rankings.
- **splog**

  Short for *spam blog. A* site created solely for marketing purposes.

(Source: Turban et al., 2010)

THE INFORMATION ASSURANCE MODEL AND DEFENSE STRATEGY

- **CIA security triad (CIA triad)**

  Three security concepts important to information on the Internet: confidentiality, integrity, and availability.

EXHIBIT 9.7 CIA Security Triad

(Source: Turban et al., 2010)

THE INFORMATION ASSURANCE MODEL AND DEFENSE STRATEGY

- **confidentiality**

  Assurance of data privacy and accuracy. Keeping private or sensitive information from being disclosed to unauthorized individuals, entities, or processes.

- **integrity**

  Assurance that stored data has not been modified without authorization; a message that was sent is the same message as that which was received.

- **availability**

  Assurance that access to data, the Web site, or other EC data service is timely, available, reliable, and restricted to authorized users.

(Source: Turban et al., 2010)

THE INFORMATION ASSURANCE MODEL AND DEFENSE STRATEGY

- **E-COMMERCE SECURITY STRATEGY**
  1. Prevention and deterrence
  2. Detection
  3. Containment (contain the damage)
  4. Recovery
  5. Correction
  6. Awareness and compliance

(Source: Turban et al., 2010)

THE INFORMATION ASSURANCE MODEL AND DEFENSE STRATEGY

- **EC security programs**

  All the policies, procedures, documents, standards, hardware, software, training, and personnel that work together to protect information, the ability to conduct business, and other assets.

(Source: Turban et al., 2010)

THE DEFENSE I: ACCESS CONTROL, ENCRYPTION, AND PKI

- **access control**

  Mechanism that determines who can legitimately use a network resource.
  - **Authentication and Passwords**
  - **biometric control**

    An automated method for verifying the identity of a person based on physical or behavioral characteristics.
  - **biometric systems**

    Authentication systems that identify a person by measurement of a biological characteristic, such as fingerprints, iris (eye) patterns, facial features, or voice.

(Source: Turban et al., 2010)

THE DEFENSE I: ACCESS CONTROL, ENCRYPTION, AND PKI

- **ENCRYPTION AND THE ONE-KEY (SYMMETRIC) SYSTEM**
  - **encryption**

    The process of scrambling (encrypting) a message in such a way that it is difficult, expensive, or time-consuming for an unauthorized person to unscramble (decrypt) it.
  - **plaintext**

    An unencrypted message in human-readable form.
  - **ciphertext**

    A plaintext message after it has been encrypted into a machine-readable form.
  - **encryption algorithm**

    The mathematical formula used to encrypt the plaintext into the ciphertext, and vice versa.

(Source: Turban et al., 2010)

THE DEFENSE I: ACCESS CONTROL, ENCRYPTION, AND PKI

- **key (key value)**

  The secret code used to encrypt and decrypt a message.

- **key space**

  The large number of possible key values (keys) created by the algorithm to use when transforming the message.

- **symmetric (private) key encryption**

  An encryption system that uses the same key to encrypt and decrypt the message.

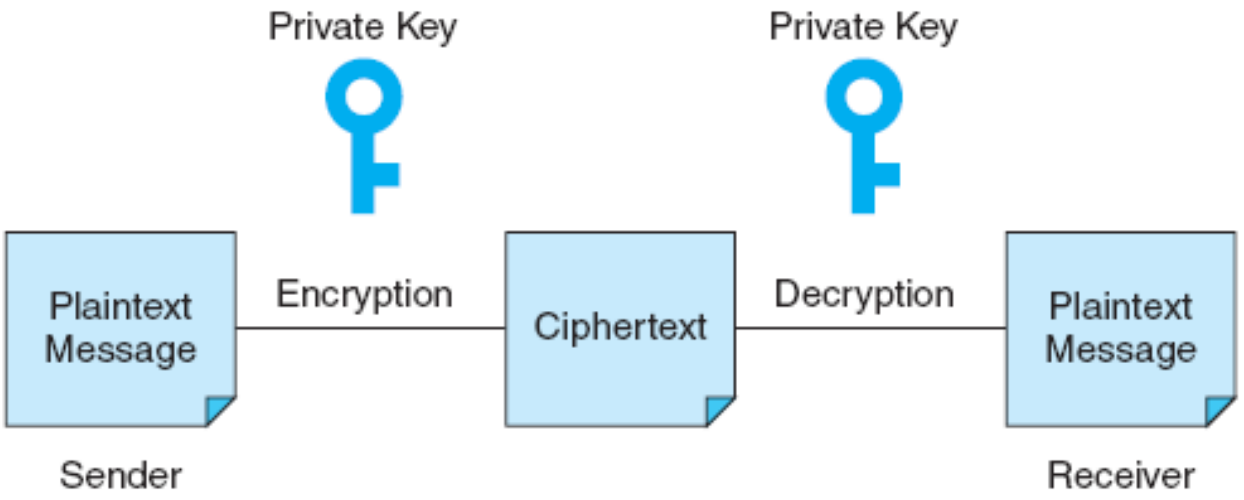
- **Data Encryption Standard (DES)**

  The standard symmetric encryption algorithm supported by the NIST and used by U.S. government agencies until October 2000.

(Source: Turban et al., 2010)

THE DEFENSE I:
ACCESS CONTROL, ENCRYPTION, AND PKI

EXHIBIT 9.10 Symmetric (Private) Key Encryption



(Source: Turban et al., 2010)

THE DEFENSE I: ACCESS CONTROL, ENCRYPTION, AND PKI

- **public key infrastructure (PKI)**

  A scheme for securing e-payments using public key encryption and various technical components.

  – **public (asymmetric) key encryption**

    Method of encryption that uses a pair of matched keys—a public key to encrypt a message and a private key to decrypt it, or vice versa.

    - **public key**

      Encryption code that is publicly available to anyone.

    - **private key**

      Encryption code that is known only to its owner.

(Source: Turban et al., 2010)

THE DEFENSE I: ACCESS CONTROL, ENCRYPTION, AND PKI

– **public (asymmetric) key encryption**

Method of encryption that uses a pair of matched keys—a public key to encrypt a message and a private key to decrypt it, or vice versa.

- **public key**

  Encryption code that is publicly available to anyone.

- **private key**

  Encryption code that is known only to its owner.

(Source: Turban et al., 2010)

THE DEFENSE I: ACCESS CONTROL, ENCRYPTION, AND PKI

- **The PKI Process**
  - **digital signature or digital certificate**

    Validates the sender and time stamp of a transaction so it cannot be later claimed that the transaction was unauthorized or invalid.
    - **hash**

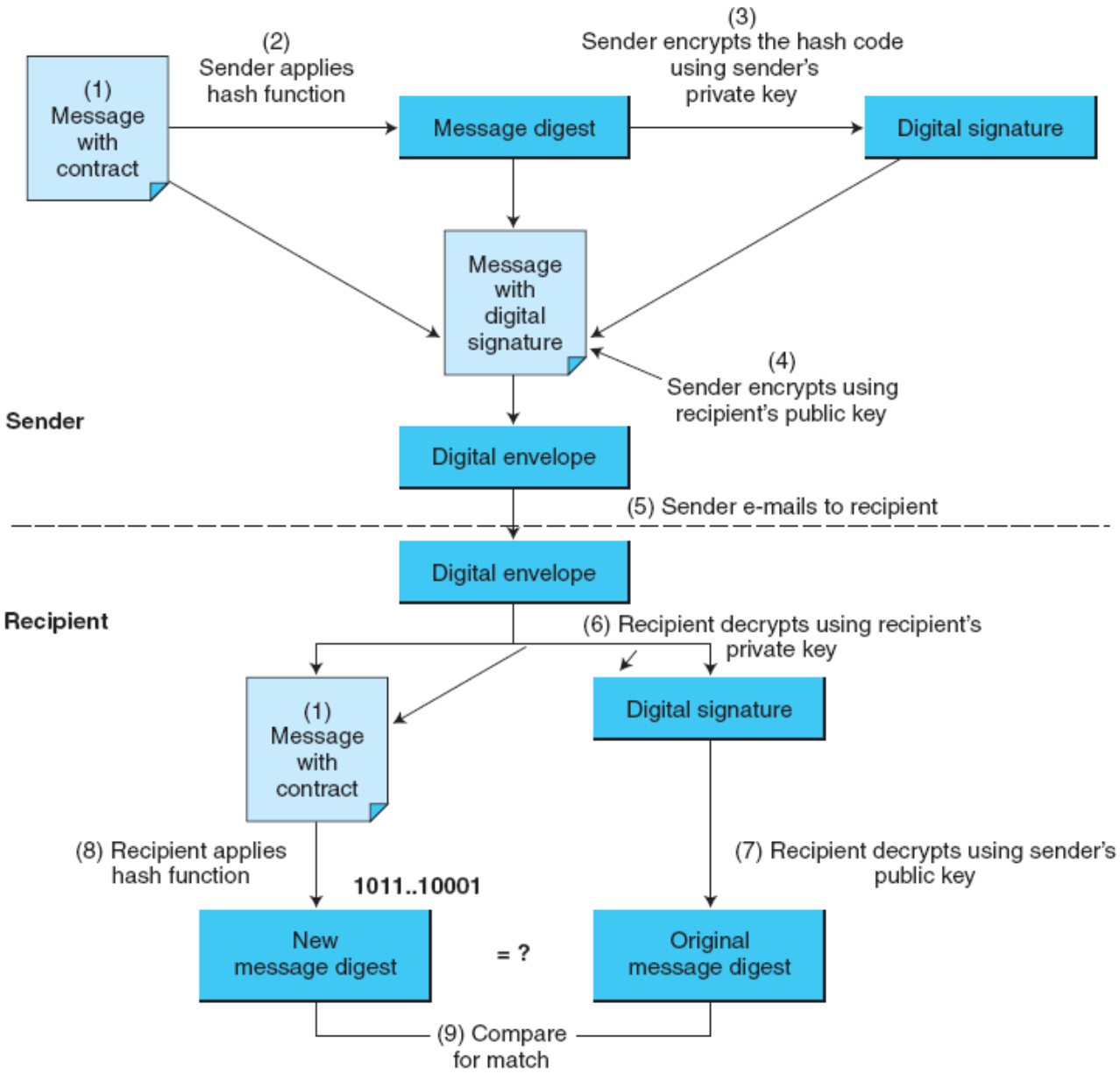
      A mathematical computation that is applied to a message, using a private key, to encrypt the message.
    - **message digest (MD)**

      A summary of a message, converted into a string of digits after the hash has been applied.
    - **digital envelope**

      The combination of the encrypted original message and the digital signature, using the recipient's public key.

(Source: Turban et al., 2010)

EXHIBIT 9.11 Digital Signatures



(Source: Turban et al., 2010)

THE DEFENSE I: ACCESS CONTROL, ENCRYPTION, AND PKI

- **certificate authorities (CAs)**

  Third parties that issue digital certificates.
- **Secure Socket Layer (SSL)**

  Protocol that utilizes standard certificates for authentication and data encryption to ensure privacy or confidentiality.
- **Transport Layer Security (TLS)**

  As of 1996, another name for the SSL protocol.

(Source: Turban et al., 2010)

THE DEFENSE II: SECURING E-COMMERCE NETWORKS

- **firewall**

  A single point between two or more networks where all traffic must pass (choke point); the device authenticates, controls, and logs all traffic.

  - **packet**

    Segment of data sent from one computer to another on a network.

  - **personal firewall**

    A network node designed to protect an individual user's desktop system from the public network by monitoring all the traffic that passes through the computer's network interface card.

(Source: Turban et al., 2010)

THE DEFENSE II: SECURING E-COMMERCE NETWORKS

- **virtual private network (VPN)**

  A network that uses the public Internet to carry information but remains private by using encryption to scramble the communications, authentication to ensure that information has not been tampered with, and access control to verify the identity of anyone using the network.

  - **protocol tunneling**

    Method used to ensure confidentiality and integrity of data transmitted over the Internet by encrypting data packets, sending them in packets across the Internet, and decrypting them at the destination address.

(Source: Turban et al., 2010)

THE DEFENSE II: SECURING E-COMMERCE NETWORKS

- **intrusion detection system (IDS)**

  A special category of software that can monitor activity across a network or on a host computer, watch for suspicious activity, and take automated action based on what it sees.
- **honeynet**

  A network of honeypots.
- **honeypot**

  Production system (e.g., firewalls, routers, Web servers, database servers) that looks like it does real work, but that acts as a decoy and is watched to study how network intrusions occur.
- **penetration test (pen test)**

  A method of evaluating the security of a computer system or a network by simulating an attack from a malicious source, (e.g., a cracker).

(Source: Turban et al., 2010)

THE DEFENSE III: GENERAL CONTROLS AND OTHER DEFENSE MECHANISMS

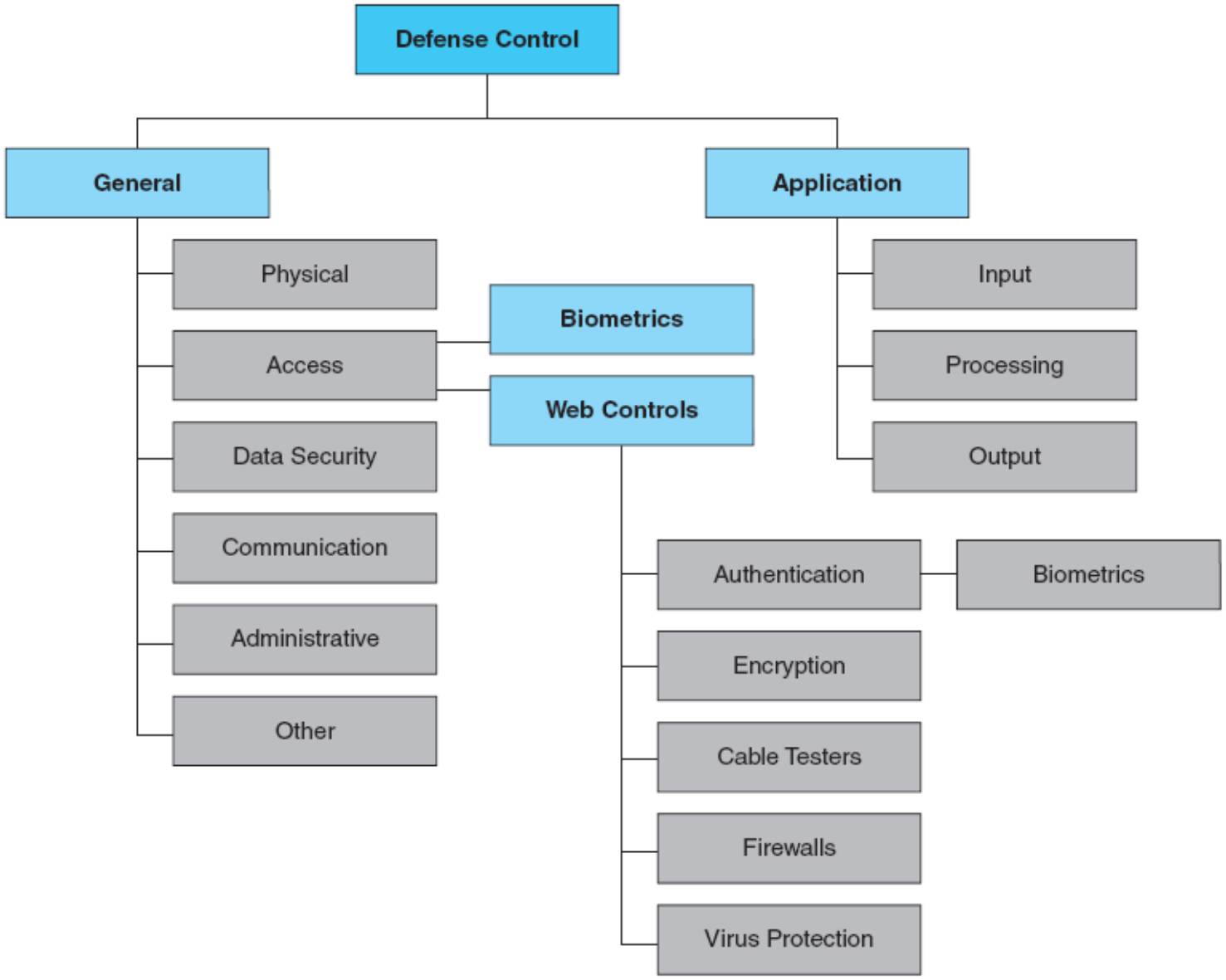
- **general controls**

  Controls established to protect the system regardless of the specific application. For example, protecting hardware and controlling access to the data center are independent of the specific application.
- **application controls**

  Controls that are intended to protect specific applications.

(Source: Turban et al., 2010)

EXHIBIT 9.12 Major Defense Controls



(Source: Turban et al., 2010)

THE DEFENSE III:
GENERAL CONTROLS AND OTHER DEFENSE MECHANISMS

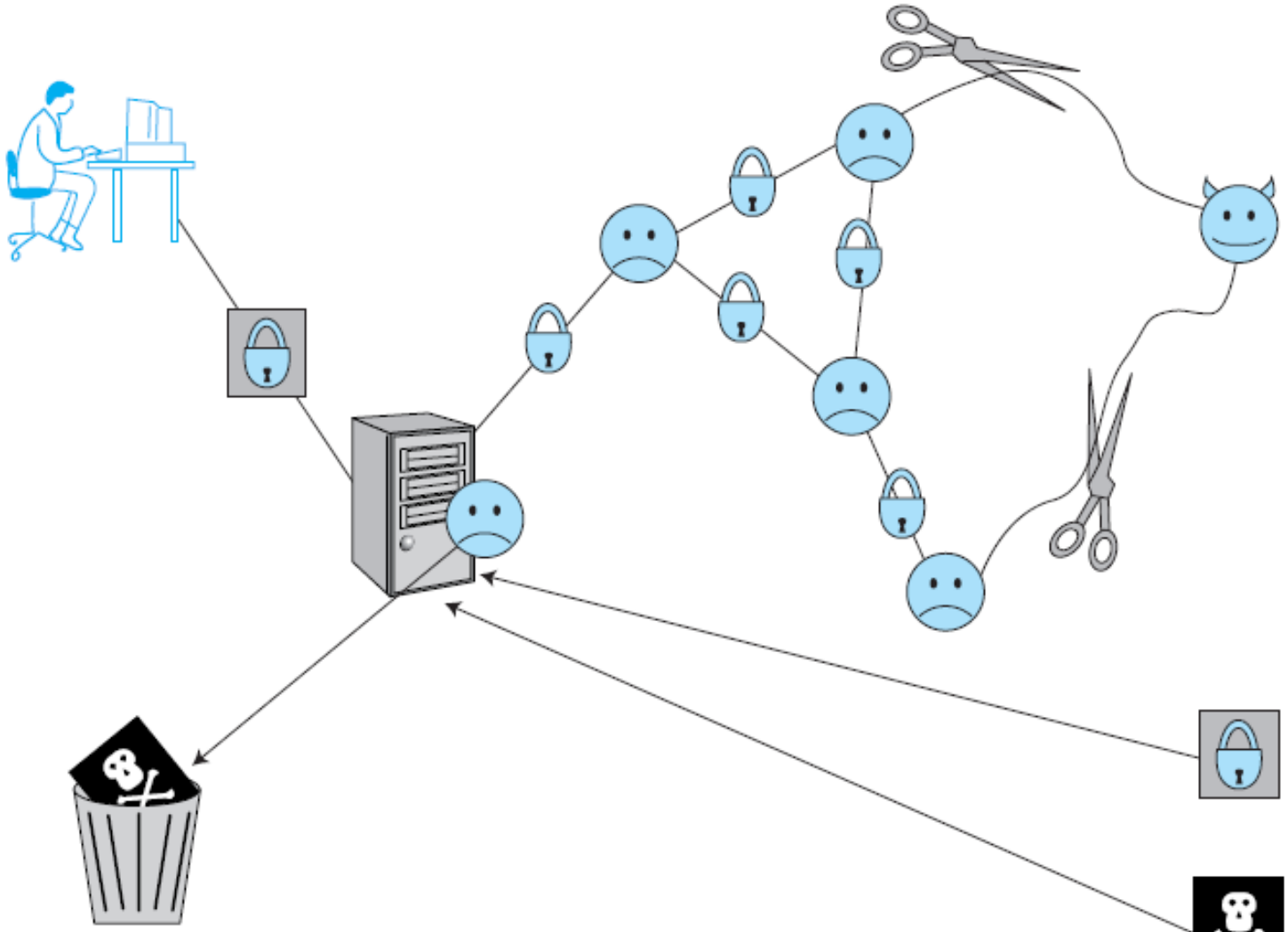
- **APPLICATION CONTROLS**
  - **intelligent agents**

    Software applications that have some degree of reactivity, autonomy, and adaptability—as is needed in unpredictable attack situations. An agent is able to adapt itself based on changes occurring in its environment.
  - **internal control environment**

    The work atmosphere that a company sets for its employees.

(Source: Turban et al., 2010)

EXHIBIT 9.14 Intelligent Agents



Agents in collective communicate over secured links on the Internet or an intranet. Malicious agents (with horns) are detected and cut off from the collective. Property authenticated data is allowed into the collective, but bad information is rejected.

(Source: Turban et al., 2010)

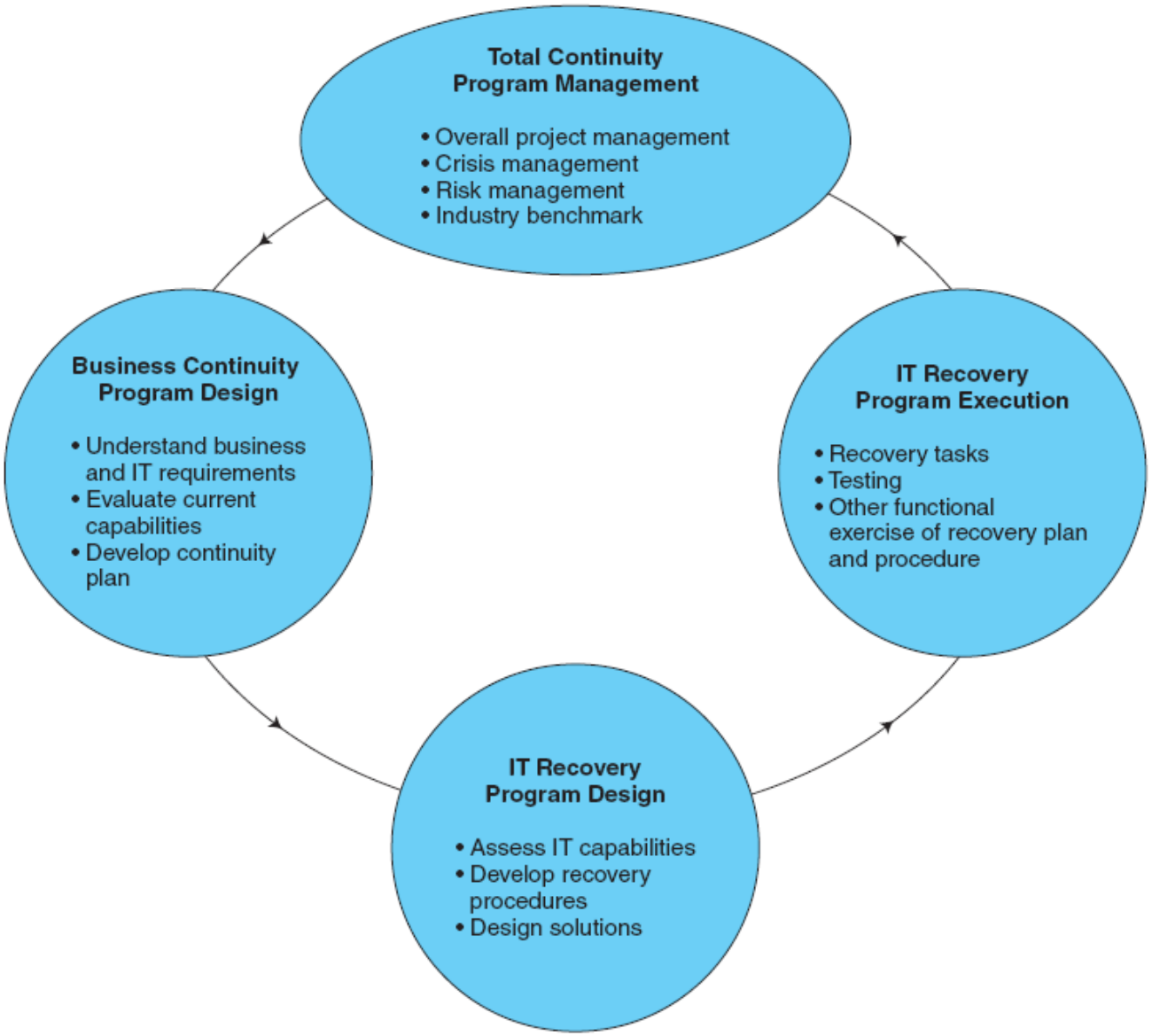
THE DEFENSE III:
GENERAL CONTROLS AND OTHER DEFENSE MECHANISMS

- **PROTECTING AGAINST SPAM**
  - **Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act**

    Law that makes it a crime to send commercial e-mail messages with false or misleading message headers or misleading subject lines.
- **PROTECTING AGAINST POP-UP ADS**
- **PROTECTION AGAINST PHISHING**
- **PROTECTING AGAINST SPYWARE**

(Source: Turban et al., 2010)

EXHIBIT 9.15 Business Continuity Services



(Source: Turban et al., 2010)

BUSINESS CONTINUITY, SECURITY AUDITING, AND RISK MANAGEMENT

- **BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING**
  - **disaster avoidance**

    An approach oriented toward prevention. The idea is to minimize the chance of avoidable disasters (such as fire or other human-caused threats).
- **RISK-MANAGEMENT AND COST-BENEFIT ANALYSIS**
  - **Risk-Management Analysis**
  - **Ethical Issues**

(Source: Turban et al., 2010)

IMPLEMENTING ENTERPRISE-WIDE E-COMMERCE SECURITY

- **SENIOR MANAGEMENT COMMITMENT AND SUPPORT**
- **EC SECURITY POLICIES AND TRAINING**
  - **acceptable use policy (AUP)**

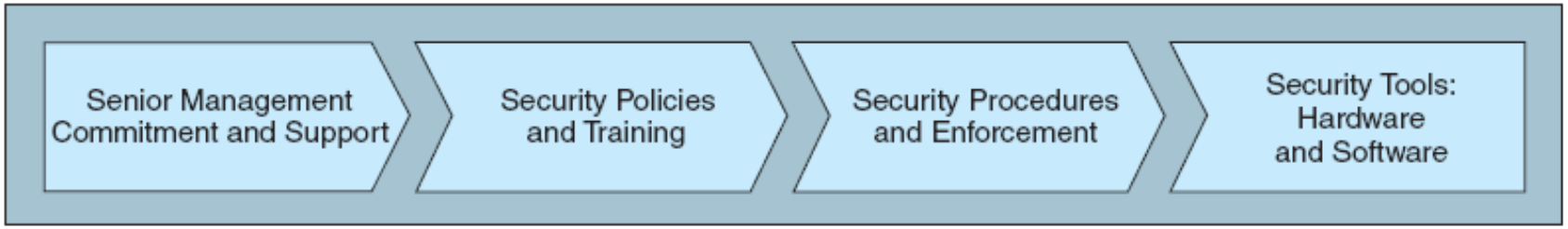
    Policy that informs users of their responsibilities when using company networks, wireless devices, customer data, and so forth.
- **EC SECURITY PROCEDURES AND ENFORCEMENT**
  - **business impact analysis (BIA)**

    An exercise that determines the impact of losing the support of an EC resource to an organization and establishes the escalation of that loss over time, identifies the minimum resources needed to recover, and prioritizes the recovery of processes and supporting systems.

(Source: Turban et al., 2010)

IMPLEMENTING ENTERPRISE-WIDE E-COMMERCE SECURITY

EXHIBIT 9.16 Enterprise-wide EC Security and Privacy Model



(Source: Turban et al., 2010)

IMPLEMENTING ENTERPRISE-WIDE E-COMMERCE SECURITY

- **INDUSTRY STANDARDS FOR CREDIT CARD PROTECTION (PCI DSS)**
  - Payment Card Industry Data Security Standards (PCI DSS)

(Source: Turban et al., 2010)

IMPLEMENTING ENTERPRISE-WIDE E-COMMERCE SECURITY

- **WHY IS IT DIFFICULT TO STOP INTERNET CRIME?**
  - **Making Shopping Inconvenient**
  - **Shoppers' Negligence**
  - **Ignoring EC Security Best Practices**
    - **Computing Technology Industry Association (CompTIA)**

      Nonprofit trade group providing information security research and best practices.
  - **Design and Architecture Issues**
  - **Standard of due care**

    Care that a company is reasonably expected to take based on the risks affecting its EC business and online transactions.

(Source: Turban et al., 2010)

MANAGERIAL ISSUES

1. What is the EC security strategy of your company
2. Is the budget for IT security adequate?
3. What steps should businesses follow in establishing a security plan?
4. Should organizations be concerned with internal security threats?
5. What is the key to establishing strong e-commerce security?

(Source: Turban et al., 2010)

References

- Turban et al., Introduction to Electronic Commerce, Third Edition, 2010, Pearson