Chapter 9

E-Commerce Security and Fraud Protection

Learning Objectives

1. Understand the importance and scope of 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 technical attacks.
4. Understand Internet fraud, phishing, and spam.
5. Describe the information assurance security principles.
6. Identify and assess major technologies and methods for securing EC access and communications.

Learning Objectives

7. Describe the major technologies for protection of EC networks.
8. Describe various types of controls and special defense mechanisms.
9. Describe consumer and seller protection from fraud.
10. Describe the role of business continuity and disaster recovery planning.
11. Discuss EC security's enterprisewide implementation issues.
12. Understand why it is not possible to stop computer crimes.

The Information Security Problem

- **information security**

  Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction

- **WHAT IS EC SECURITY?**
  - **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

The Information Security Problem

- **Personal Security**
- **National Security**
- **Security Risks for 2011–2012**
- **Cyberwars, Cyberespionage, and Cybercrimes Across Borders**
- **Types of Attacks**
  - Corporate espionage that plagues businesses around the world
  - Political espionage and warfare

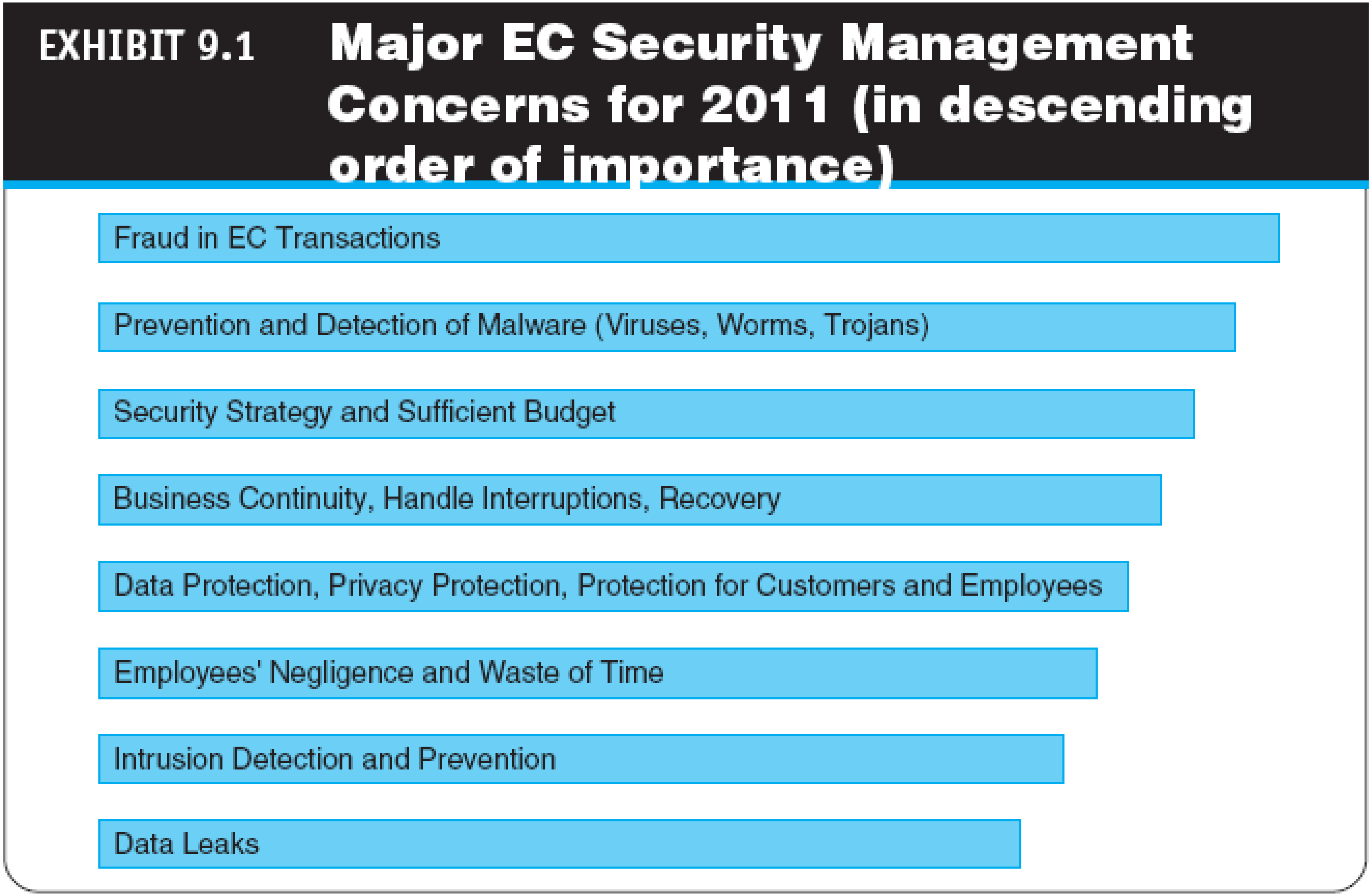


EXHIBIT 9.1 **Major EC Security Management Concerns for 2011 (in descending order of importance)**

- Fraud in EC Transactions
- Prevention and Detection of Malware (Viruses, Worms, Trojans)
- Security Strategy and Sufficient Budget
- Business Continuity, Handle Interruptions, Recovery
- Data Protection, Privacy Protection, Protection for Customers and Employees
- Employees' Negligence and Waste of Time
- Intrusion Detection and Prevention
- Data Leaks

The Information Security Problem

- **THE DRIVERS OF EC SECURITY PROBLEMS**
  - **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
  - **The Shift to Profit-Induced Crimes**

The Information Security Problem

- **Internet underground economy**

  E-markets for stolen information made up of thousands of websites 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

- **The Dynamic Nature of EC Systems and the Role of Insiders**

- **WHY IS AN E-COMMERCE SECURITY STRATEGY NEEDED?**
  - **The Computer Security Strategy Dilemma**

Basic E-commerce Security Issues and Landscape

- **BASIC SECURITY 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
  - **cybercriminal**

    A person who intentionally carries out crimes over the Internet

Basic E-commerce Security Issues and Landscape

- **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
- **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

Basic E-Commerce Security Issues and Landscape

- **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

- **spam**

  The electronic equivalent of junk mail

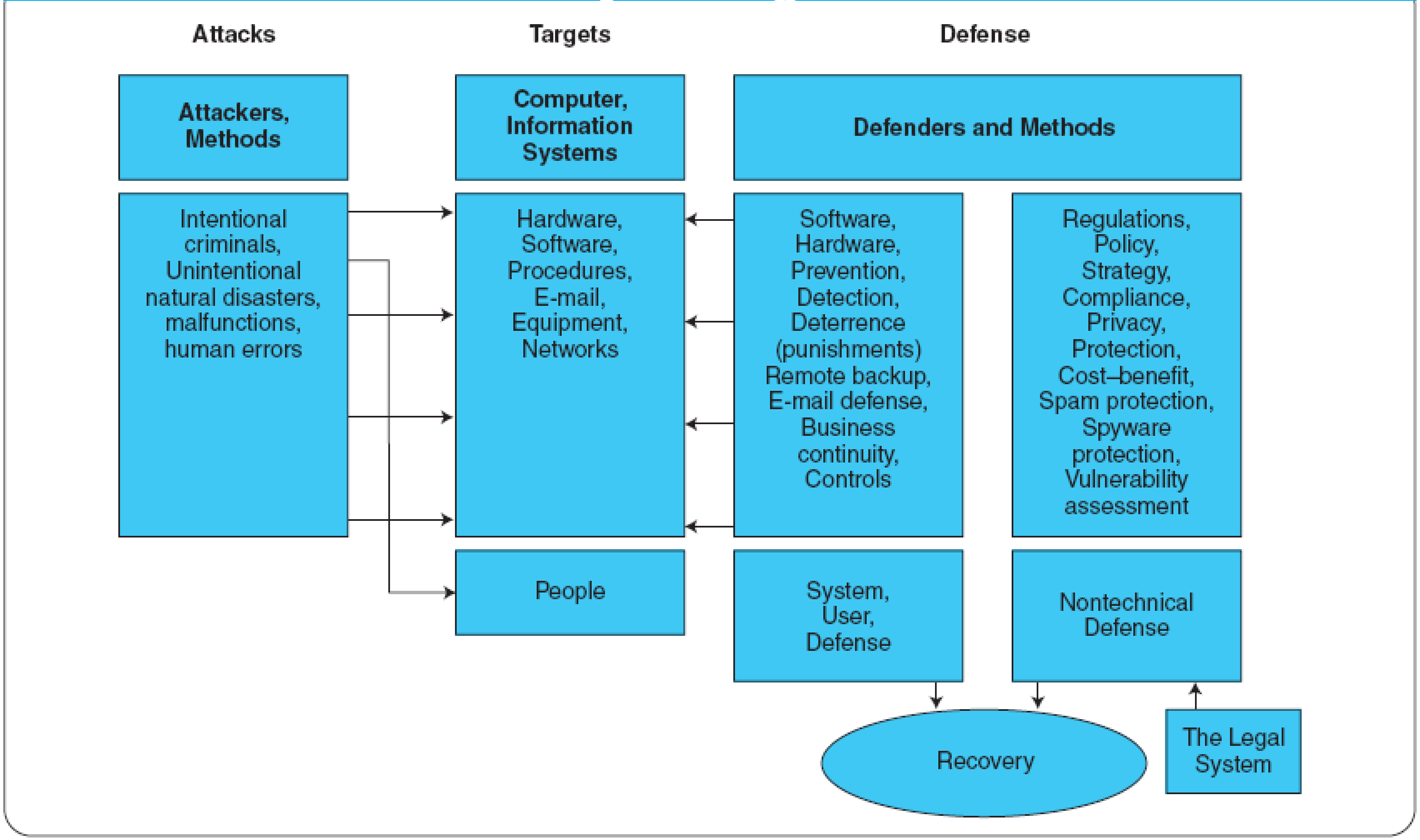
Basic E-commerce Security Issues and Landscape

- **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

EXHIBIT 9.2 The EC Security Battleground



Attacks

Attackers, Methods

Intentional criminals, Unintentional natural disasters, malfunctions, human errors

Targets

Computer, Information Systems

Hardware, Software, Procedures, E-mail, Equipment, Networks

People

Defense

Defenders and Methods

Software, Hardware, Prevention, Detection, Deterrence (punishments) Remote backup, E-mail defense, Business continuity, Controls

Regulations, Policy, Strategy, Compliance, Privacy, Protection, Cost–benefit, Spam protection, Spyware protection, Vulnerability assessment

System, User, Defense

Nontechnical Defense

Recovery

The Legal System

Basic E-Commerce Security Issues and Landscape

- **THE THREATS, ATTACKS, AND ATTACKERS**
  - **Unintentional Threats**
  - **Intentional Attacks and Crimes**
  - **The Criminals and Methods**
    - **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

Basic E-Commerce Security Issues and Landscape

- **THE TARGETS OF THE ATTACKS IN VULNERABLE AREAS**
  - **Vulnerable Areas Are Being Attacked**
  - **The Vulnerabilities in Business IT and EC Systems**
- **SECURITY SCENARIOS AND REQUIREMENTS IN E-COMMERCE**
  - **The Content of Information Security**

Basic E-Commerce Security Issues and Landscape

- **EC Security Requirements**
  - **authentication**

    Process to verify (assure) the real identity of an individual, computer, computer program, or EC website
  - **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

Basic E-Commerce Security Issues and Landscape

- **THE DEFENSE: DEFENDERS, STRATEGY, AND METHODS**
  - **EC security strategy**

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

Basic E-Commerce Security Issues and Landscape

- **prevention measures**

  Ways to help stop unauthorized users (also known as “intruders”) from accessing any part of the EC system

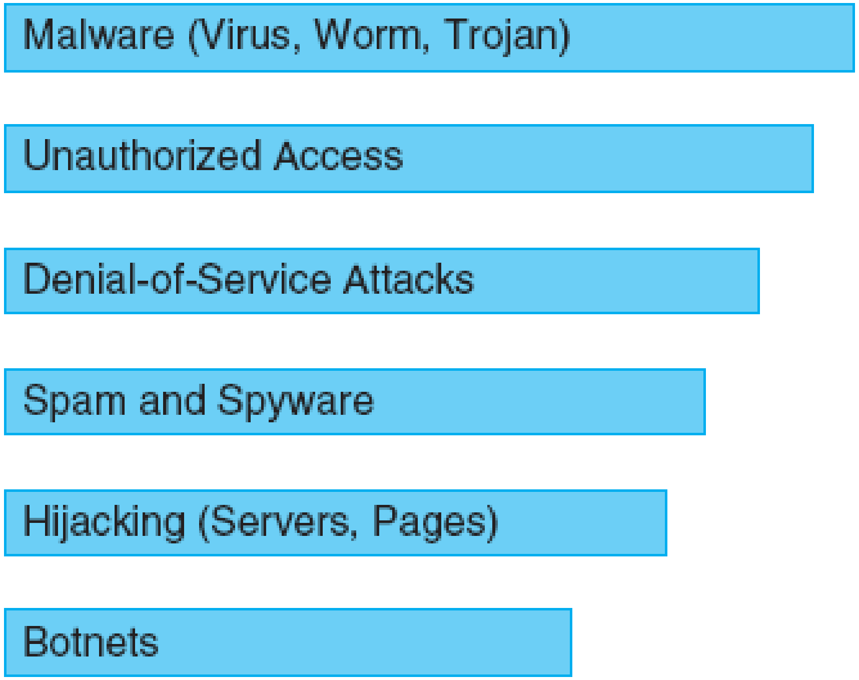
- **detection measures**

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

- **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

EXHIBIT 9.3 The Major Technical Security Attack Methods (in descending order of importance)



Malware (Virus, Worm, Trojan)

Unauthorized Access

Denial-of-Service Attacks

Spam and Spyware

Hijacking (Servers, Pages)

Botnets

Technical Attack Methods: From Viruses to Denial of Service

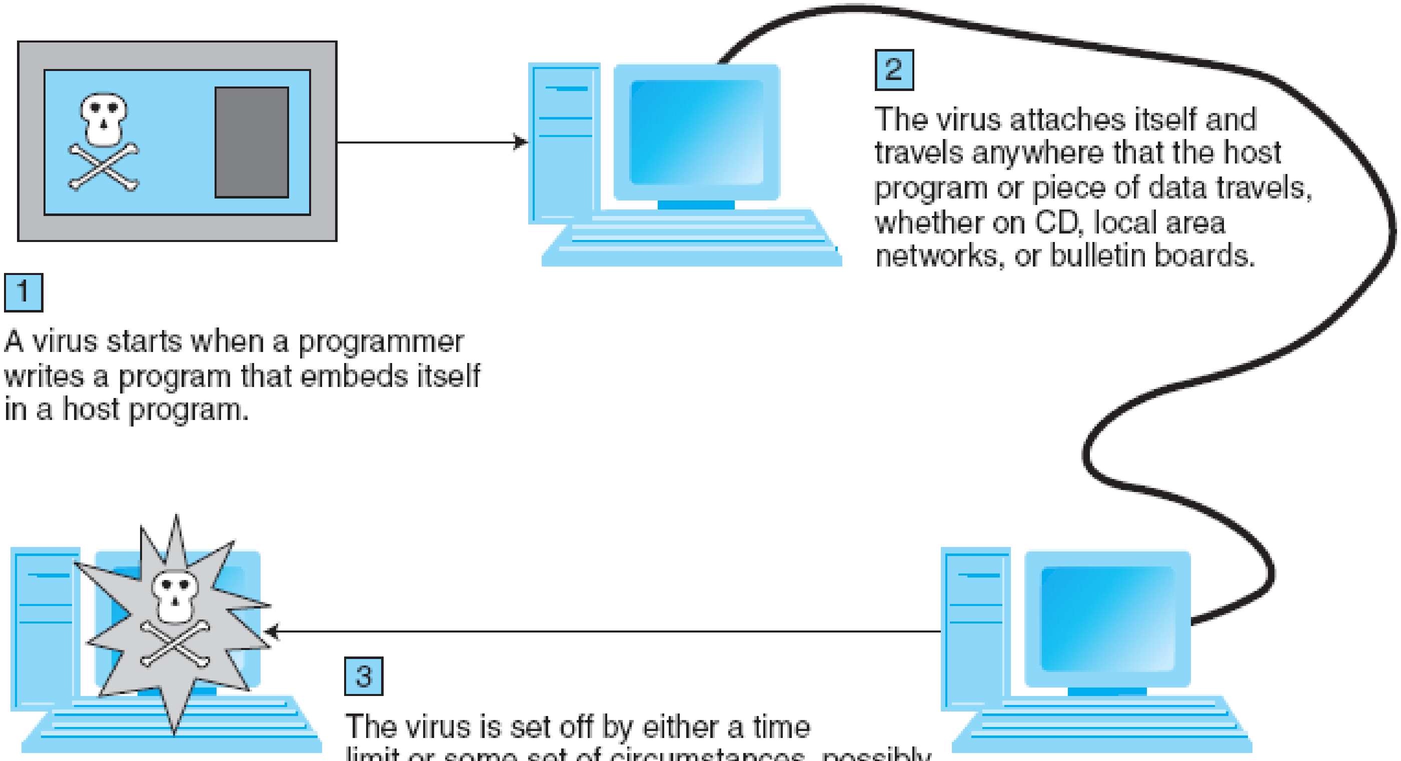
- **MALICIOUS CODE: VIRUSES, WORMS, AND TROJAN HORSES**
  - **virus**

    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

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.



1

A virus starts when a programmer writes a program that embeds itself in a host program.

2

The virus attaches itself and travels anywhere that the host program or piece of data travels, whether on CD, local area networks, or bulletin boards.

3

The virus is set off by either a time limit or some set of circumstances, possibly a simple sequence of computer operations by the user (e.g., open an attachment). Then it does whatever the virus programmer intended, whether it is to print "Have a nice day" or erase data.

Technical Attack Methods: From Viruses to Denial of Service

- **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

Technical Attack Methods: From Viruses to Denial of Service

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

  An attack on a website 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

- **page hijacking**

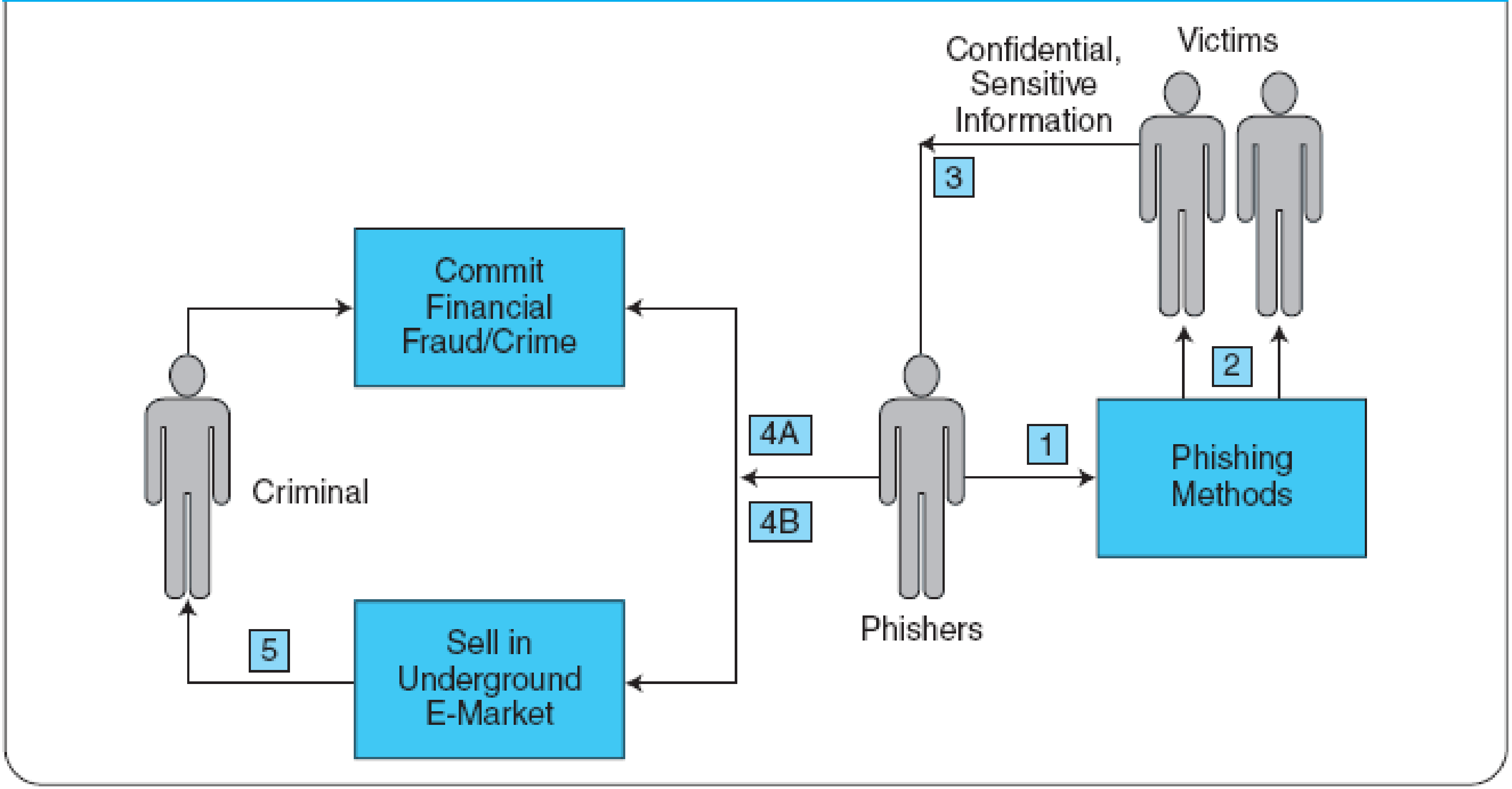
  Creating a rogue copy of a popular website that shows contents similar to the original to a Web crawler; once there, an unsuspecting user is redirected to malicious websites

Technical Attack Methods: From Viruses to Denial of Service

- **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
- **Malvertising**

EXHIBIT 9.5 Social Engineering: From Phishing to Financial Fraud and Crime



Confidential, Sensitive Information

Victims

3

Commit Financial Fraud/Crime

2

4A

1

Phishing Methods

Criminal

4B

Phishers

5

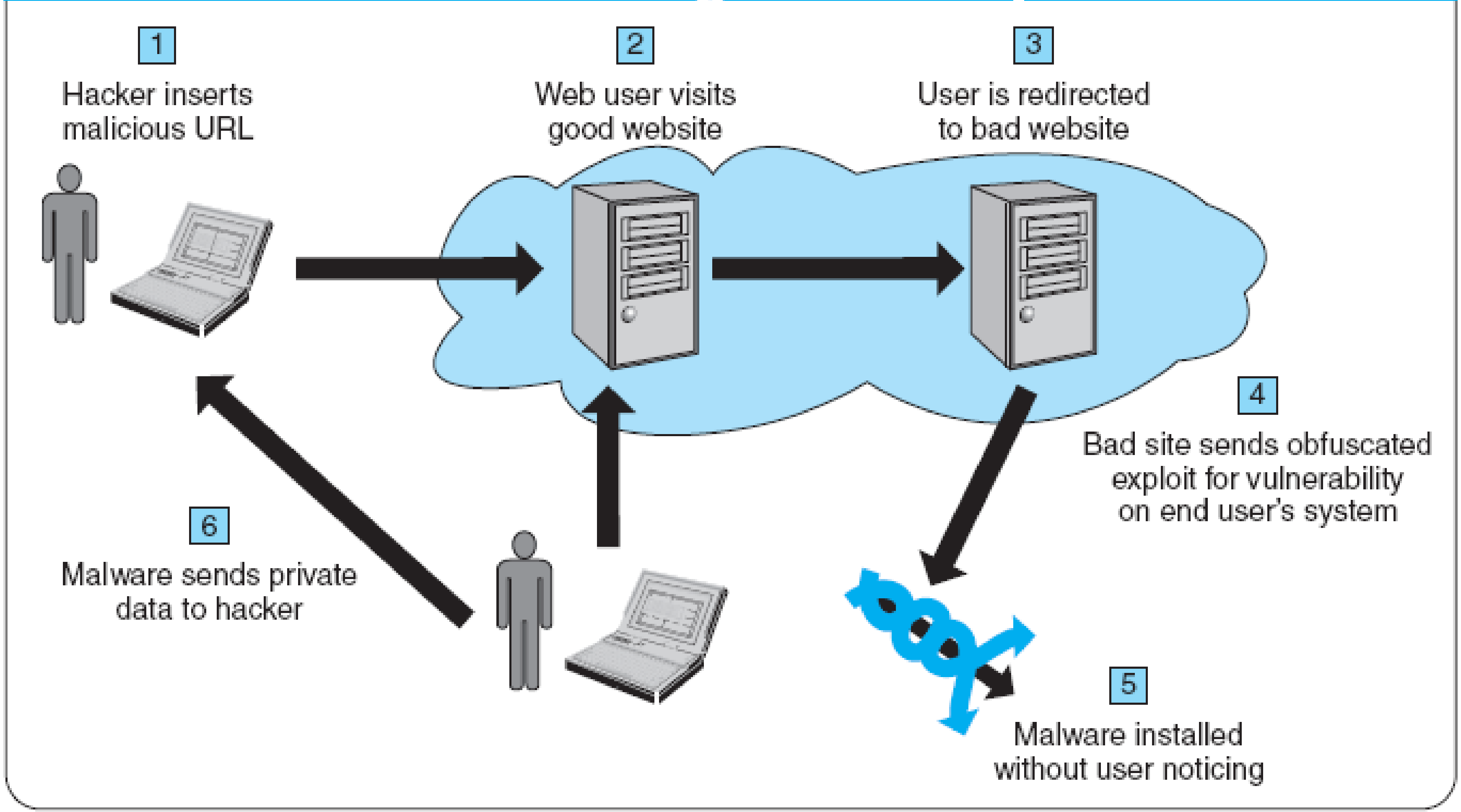
Sell in Underground E-Market

Nontechnical Methods: From Phishing To Spam

- **SOCIAL PHISHING**
  - **Sophisticated Phishing Methods**
- **FRAUD ON THE INTERNET**
  - **Examples of Typical Online Fraud Attacks**
  - **Identity Theft and Identify Fraud**
    - **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

EXHIBIT 9.6 **How Phishing Is Accomplished**



1 Hacker inserts malicious URL

2 Web user visits good website

3 User is redirected to bad website

4 Bad site sends obfuscated exploit for vulnerability on end user's system

5 Malware installed without user noticing

6 Malware sends private data to hacker

Nontechnical Methods: From Phishing To Spam

- **CYBER BANK ROBBERIES**
  - **Other Financial Fraud**
- **SPAM AND SPYWARE ATTACKS**
  - **e-mail spam**

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

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

Nontechnical Methods: From Phishing To Spam

- **SOCIAL NETWORKING MAKES SOCIAL ENGINEERING EASY**
  - **How Hackers Are Attacking Social Networks**
  - **Spam in Social Networks and in the Web 2.0 Environment**

Nontechnical Methods: From Phishing To 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

Nontechnical Methods: From Phishing To Spam

- **data breach**

  A security incident in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so

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

  - **confidentiality**

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

The Information Assurance Model and Defense Strategy

- **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 website, or other EC data service is timely, available, reliable, and restricted to authorized users

The Information Assurance Model and Defense Strategy

- **AUTHENTICATION, AUTHORIZATION, AND NONREPUDIATION**
- **E-COMMERCE SECURITY STRATEGY**
  - **The Objective of Security Defense**
  - **Security Spending Versus Needs Gap**
  - **Assessing Security Needs**
    - **vulnerability assessment**

      The process of identifying, quantifying, and prioritizing the vulnerabilities in a system

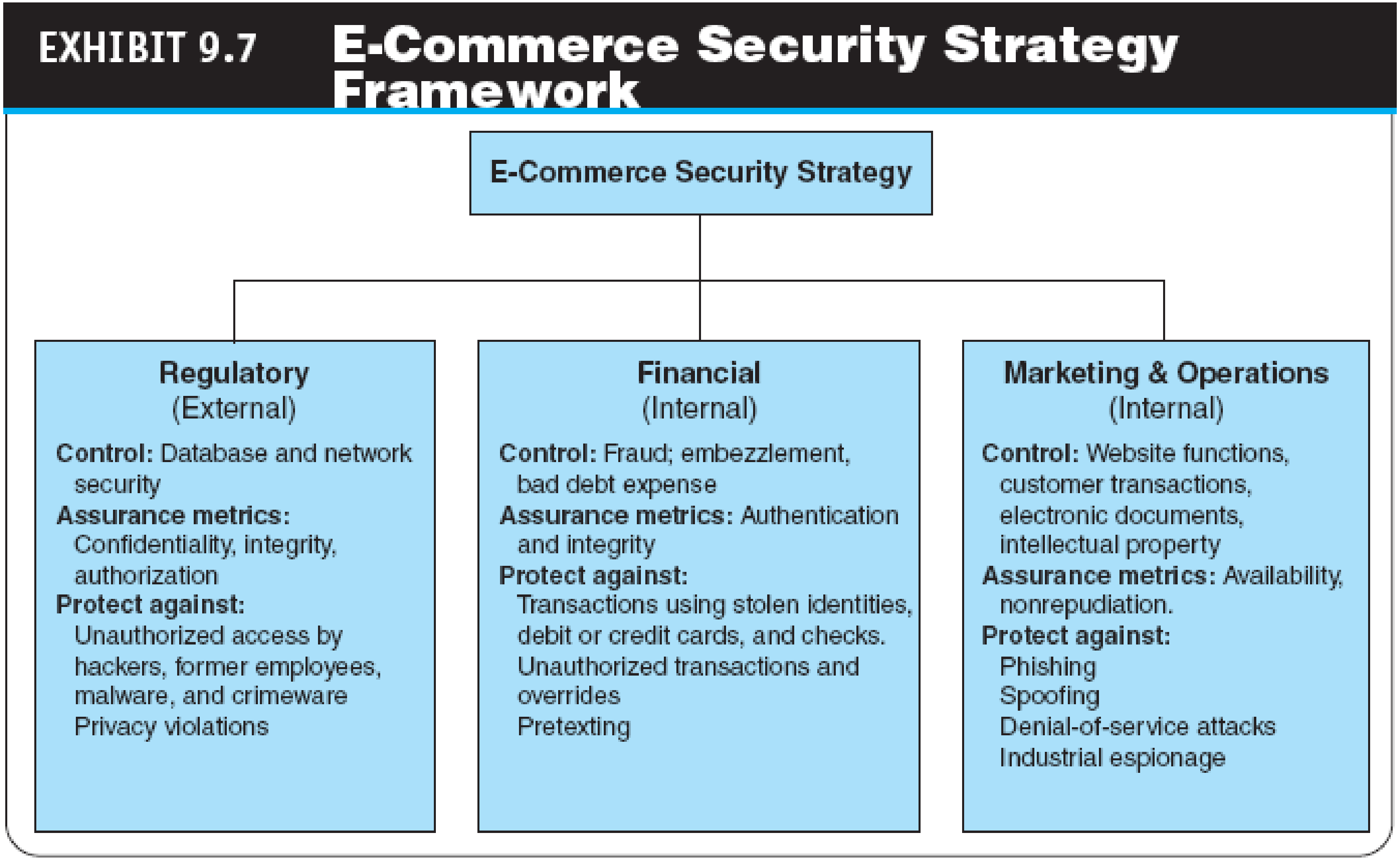


EXHIBIT 9.7

E-Commerce Security Strategy Framework

E-Commerce Security Strategy

Regulatory
(External)

Control: Database and network security

Assurance metrics: Confidentiality, integrity, authorization

Protect against:
Unauthorized access by hackers, former employees, malware, and crimeware
Privacy violations

Financial
(Internal)

Control: Fraud; embezzlement, bad debt expense

Assurance metrics: Authentication and integrity

Protect against:
Transactions using stolen identities, debit or credit cards, and checks.
Unauthorized transactions and overrides
Pretexting

Marketing & Operations
(Internal)

Control: Website functions, customer transactions, electronic documents, intellectual property

Assurance metrics: Availability, nonrepudiation.

Protect against:
Phishing
Spoofing
Denial-of-service attacks
Industrial espionage

The Information Assurance Model and Defense Strategy

- **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)

- **EC security programs**

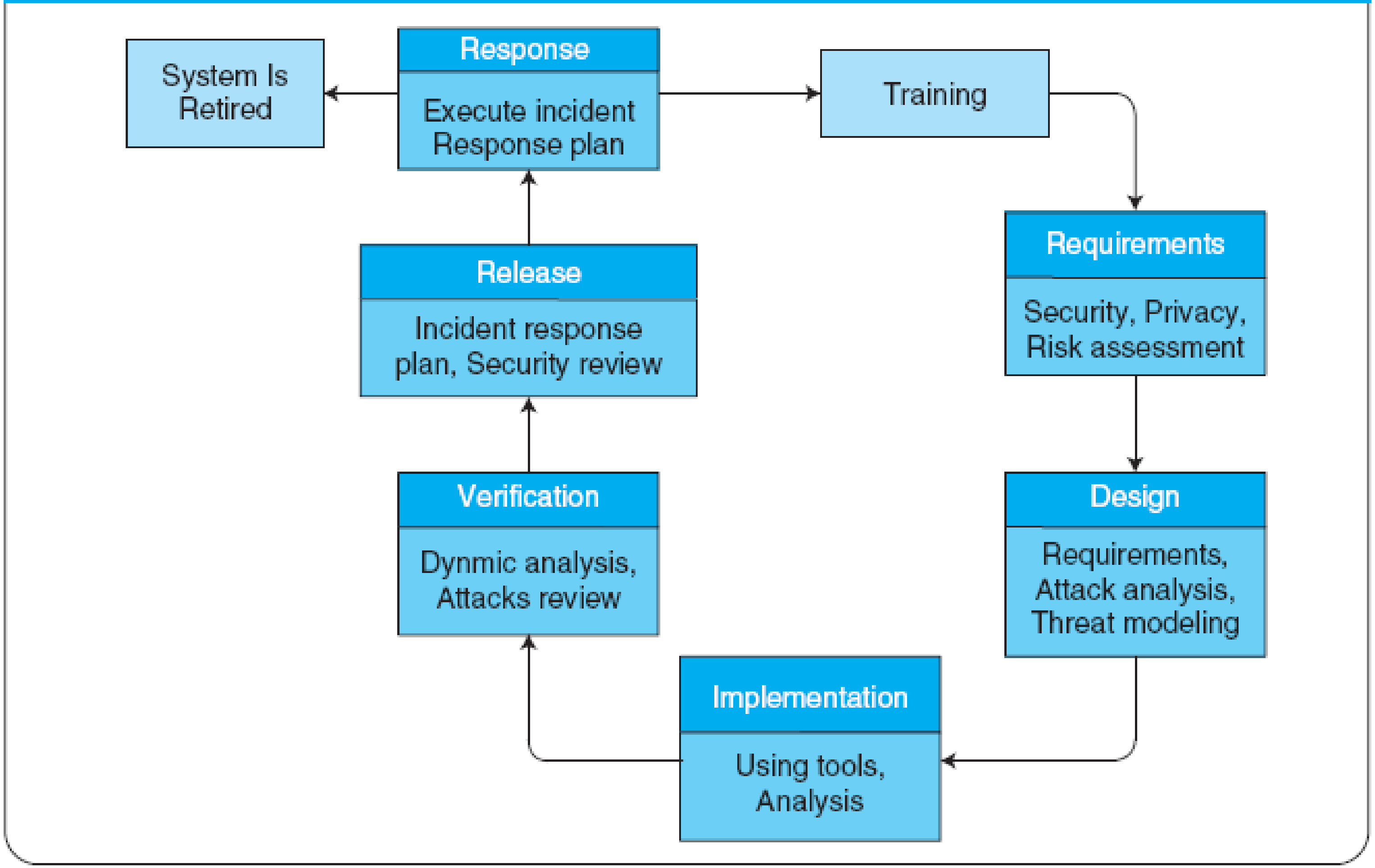
  All the policies, procedures, documents, standards, hardware, software, training, and personnel that work together to protect information, the ability to conduct business, and other assets

The Information Assurance Model and Defense Strategy

- **computer security incident management**

  The monitoring and detection of security events on a computer or computer network, and the execution of proper responses to those events. The primary purpose of incident management is the development of a well understood and predictable response to damaging events and computer intrusions.

EXHIBIT 9.8 EC Security Life Cycle Management Process



System Is Retired

Response

Execute incident Response plan

Training

Requirements

Security, Privacy, Risk assessment

Design

Requirements, Attack analysis, Threat modeling

Implementation

Using tools, Analysis

Verification

Dynmic analysis, Attacks review

Release

Incident response plan, Security review

The Information Assurance Model and Defense Strategy

- **THE DEFENSE SIDE OF EC SYSTEMS**

1. Defending access to computing systems, data flow, and EC transactions
2. Defending EC networks
3. General, administrative, and application controls
4. Protection against social engineering and fraud
5. Disaster preparation, business continuity, and risk management
6. Implementing enterprisewide security programs

The Defense I: Access Control, Encryption, and PKI

- **access control**

  Mechanism that determines who can legitimately use a network resource

  - **Authorization and Authentication**
  - **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

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

The Defense I: Access Control, Encryption, and PKI

- **encryption algorithm**

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

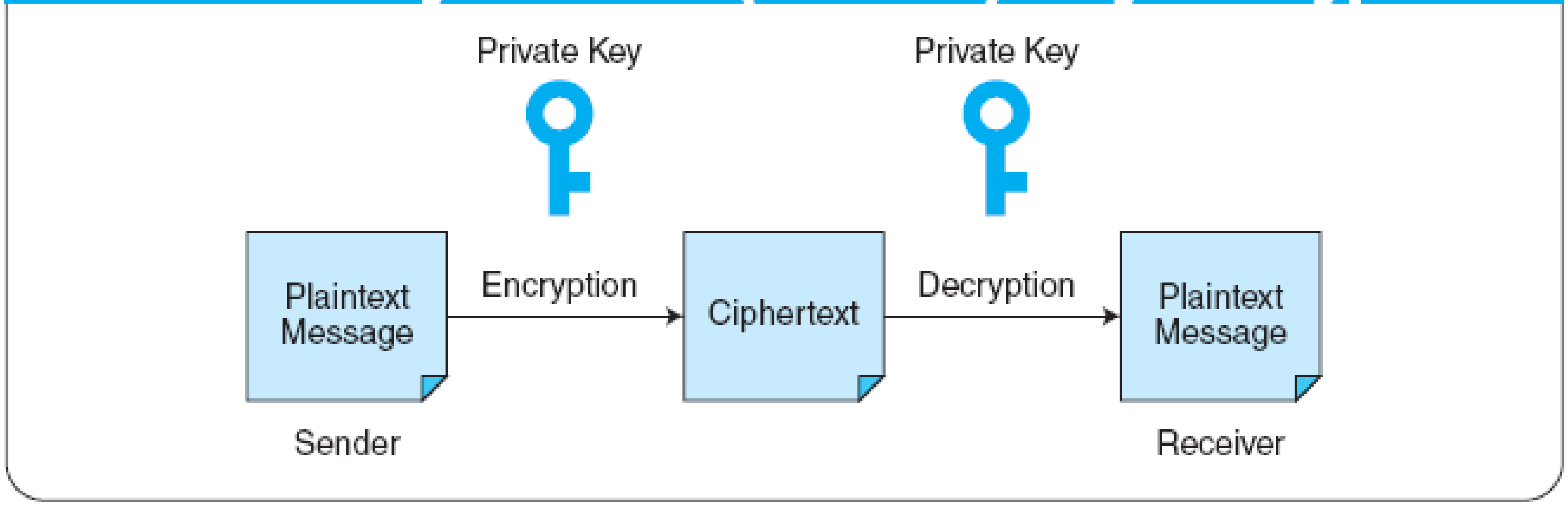
- **key (key value)**

  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

EXHIBIT 9.10 Symmetric (Private) Key Encryption



The Defense I: Access Control, Encryption, and PKI

- **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

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

The Defense I: Access Control, Encryption, and PKI

- **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

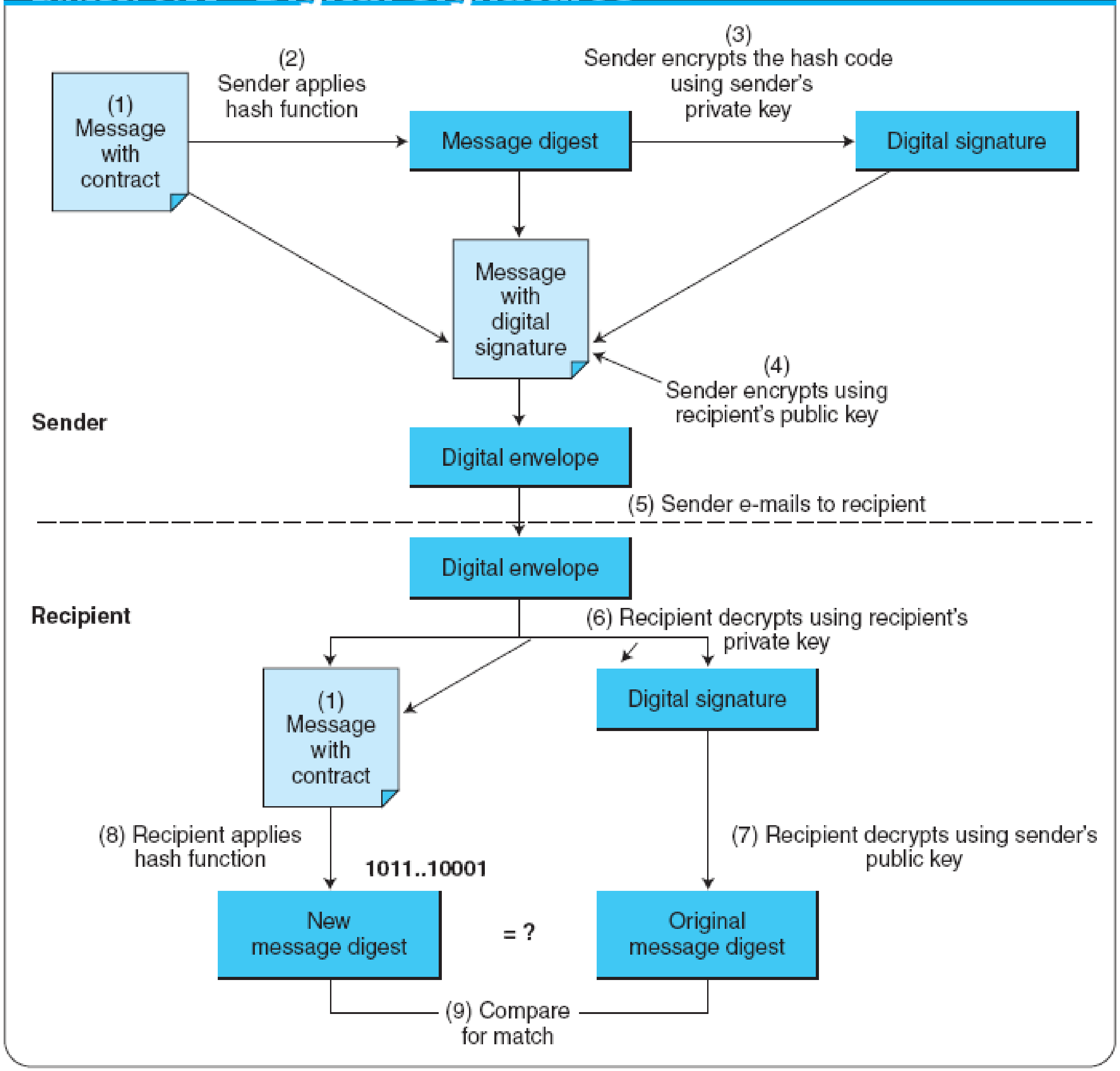
- **hash function**

  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

EXHIBIT 9.11 **Digital Signatures**


(1) Message with contract
(2) Sender applies hash function
Message digest
(3) Sender encrypts the hash code using sender's private key
Digital signature
Message with digital signature
(4) Sender encrypts using recipient's public key
Sender
Digital envelope
(5) Sender e-mails to recipient
Digital envelope
Recipient
(6) Recipient decrypts using recipient's private key
(1) Message with contract
Digital signature
(8) Recipient applies hash function
1011..10001
(7) Recipient decrypts using sender's public key
New message digest
= ?
Original message digest
(9) Compare for match

The Defense I: Access Control, Encryption, and PKI

- **digital envelope**

  The combination of the encrypted original message and the digital signature, using the recipient's public key
- **certificate authorities (CAs)**

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

The Defense II: Securing E-Commerce Networks

- **firewall**

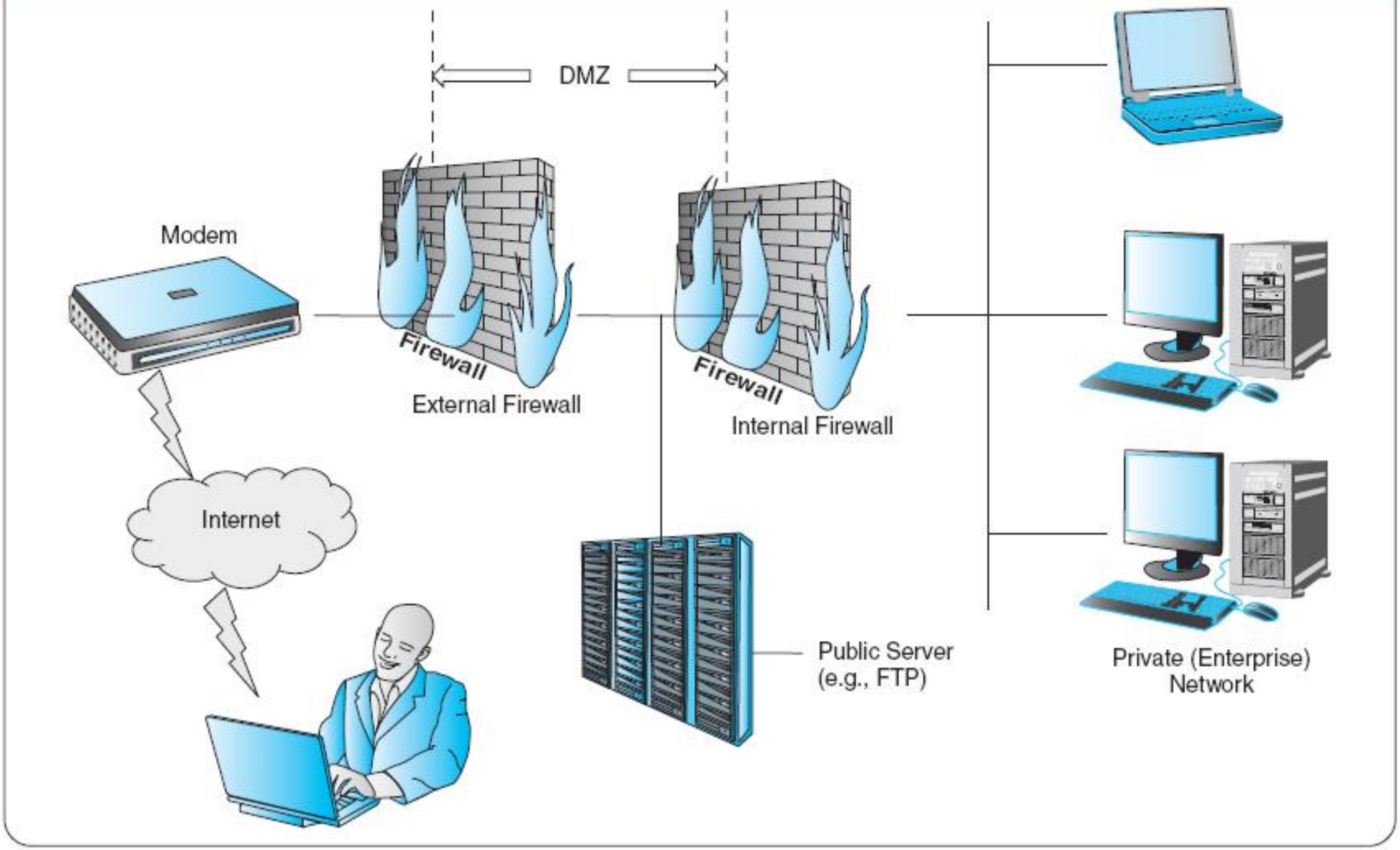
  A single point between two or more networks where all traffic must pass (choke point); the device authenticates, controls, and logs all traffic

  - **packet**

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

  - **The Dual Firewall Architecture: The DMZ**

EXHIBIT 9.12 The Two Firewalls: DMZ Architecture



The Defense II: Securing E-Commerce Networks

- **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

- **Additional Virus, Malware, and Botnet Protection**

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**

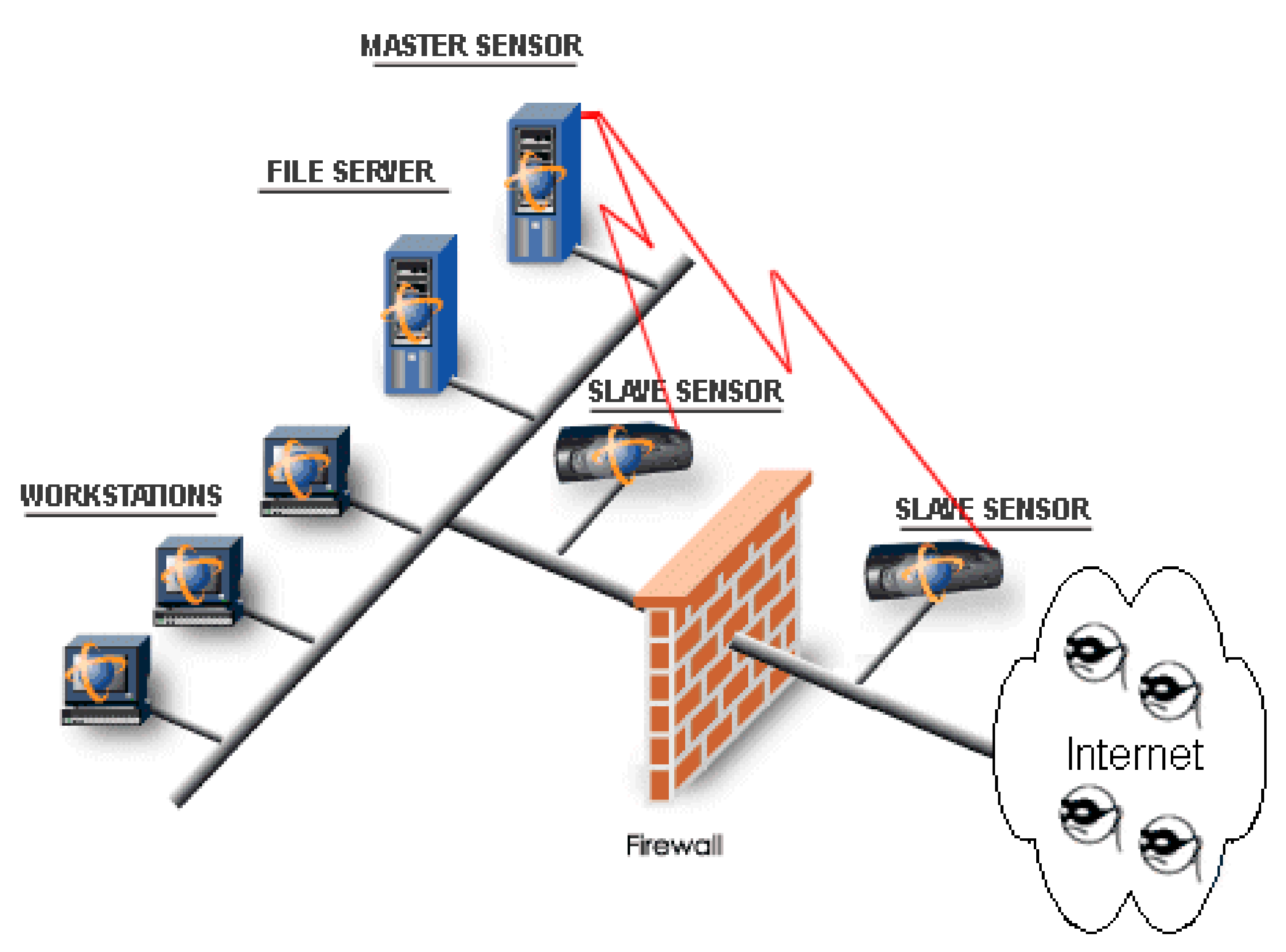
    Method used to ensure confidentiality and integrity of data transmitted over the Internet by encrypting data packets, sending them in packets across the Internet, and decrypting them at the destination address

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

  - **Dealing with DoS Attacks**
    - Cloud Computing Prevents DoS Attacks


MASTER SENSOR
FILE SERVER
SLAVE SENSOR
WORKSTATIONS
SLAVE SENSOR
Internet
Firewall

The Defense II: Securing E-Commerce Networks

- **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

  - **E-Mail Security**

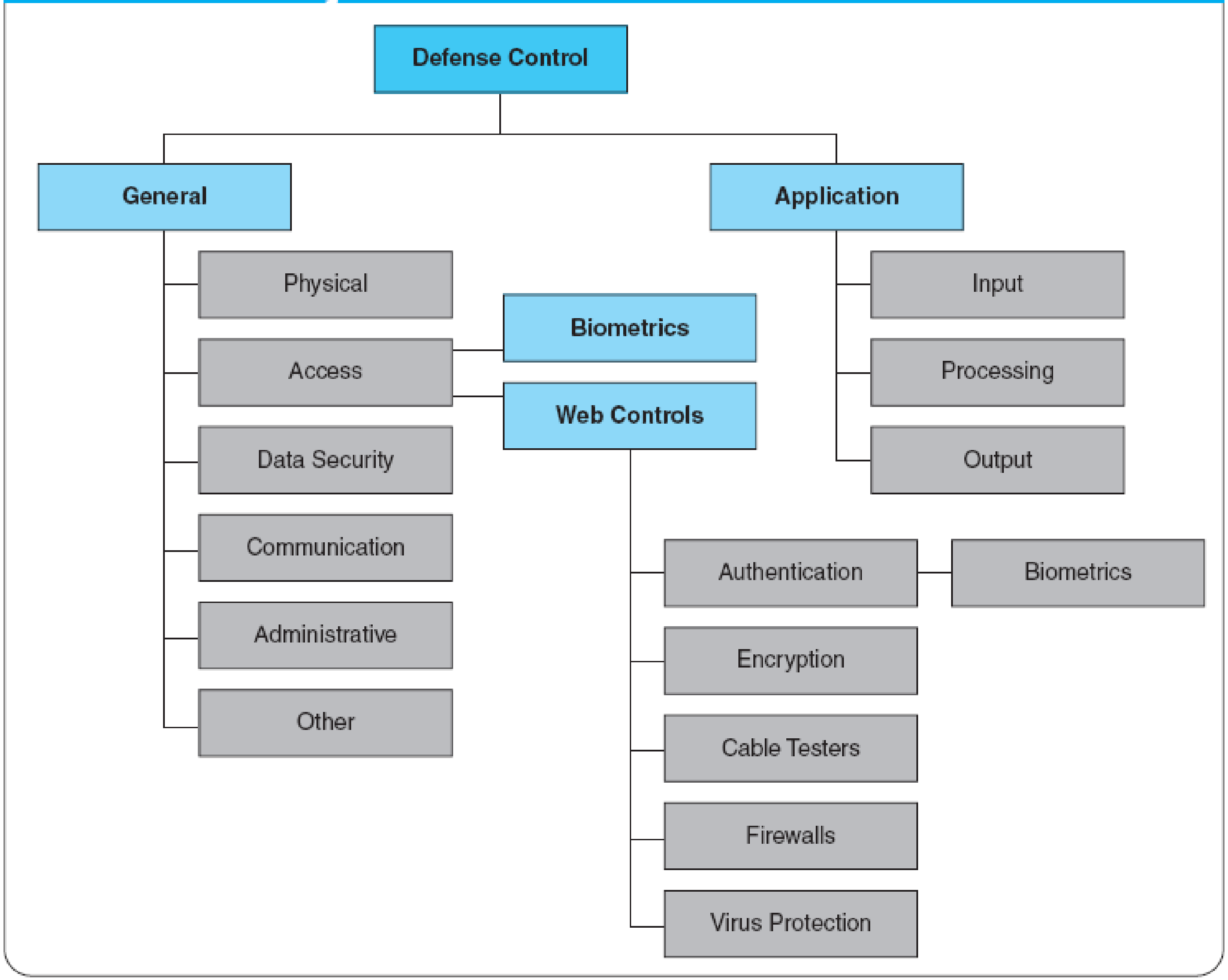
The Defense III: General Controls, Internal Controls, Compliance, and Other Defense Mechanisms

- **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

EXHIBIT 9.13 Major Defense Controls

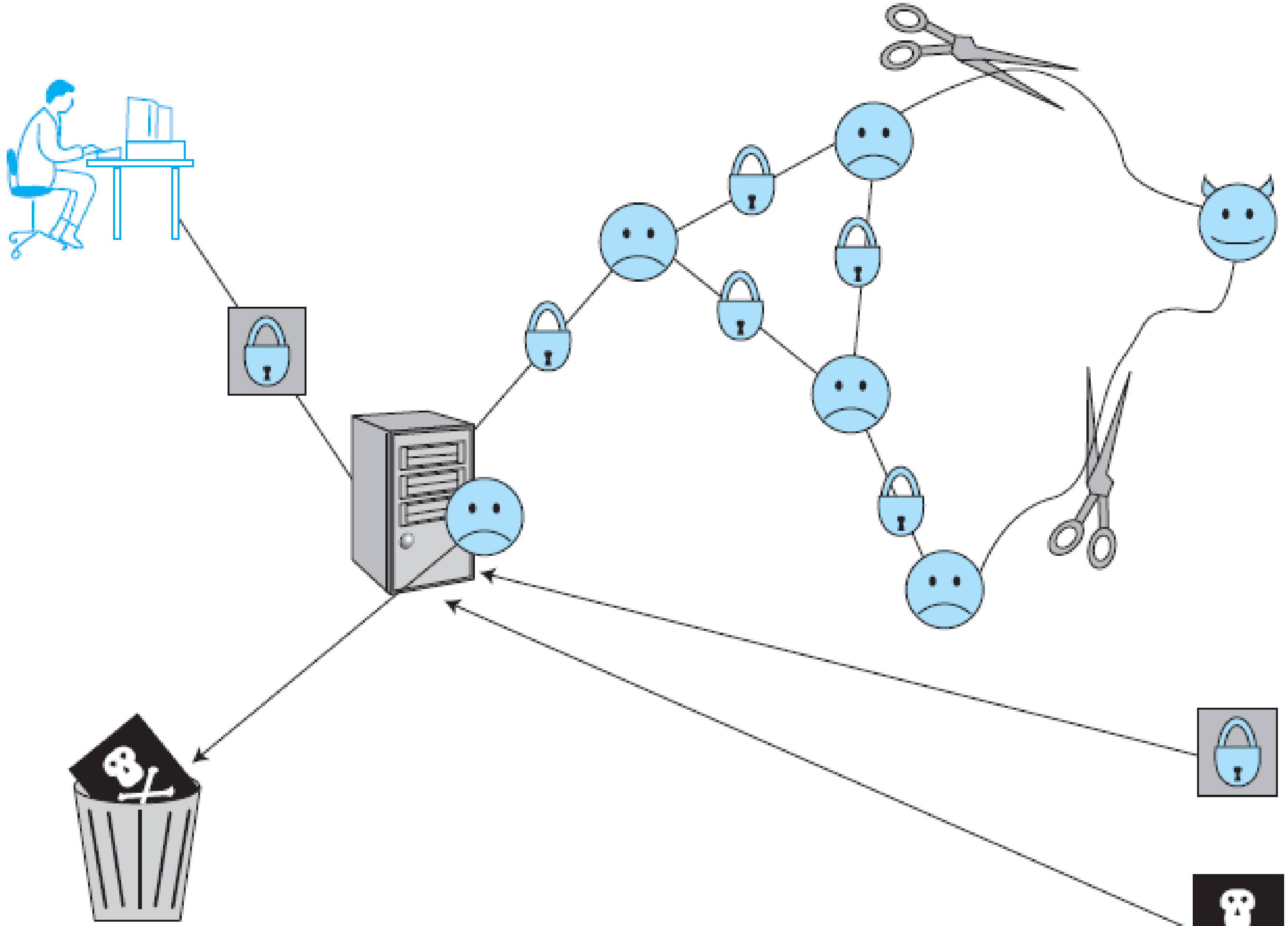


The Defense III: General Controls, Internal Controls, Compliance, and Other Defense Mechanisms

- **GENERAL, ADMINISTRATIVE, AND OTHER CONTROLS**
  - **Physical Controls**
  - **Administrative Controls**
- **APPLICATION CONTROLS AND INTELLIGENT AGENTS**
  - **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

EXHIBIT 9.15 **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.

The Defense III: General Controls, Internal Controls, Compliance, 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

The Defense III: General Controls, Internal Controls, Compliance, and Other Defense Mechanisms

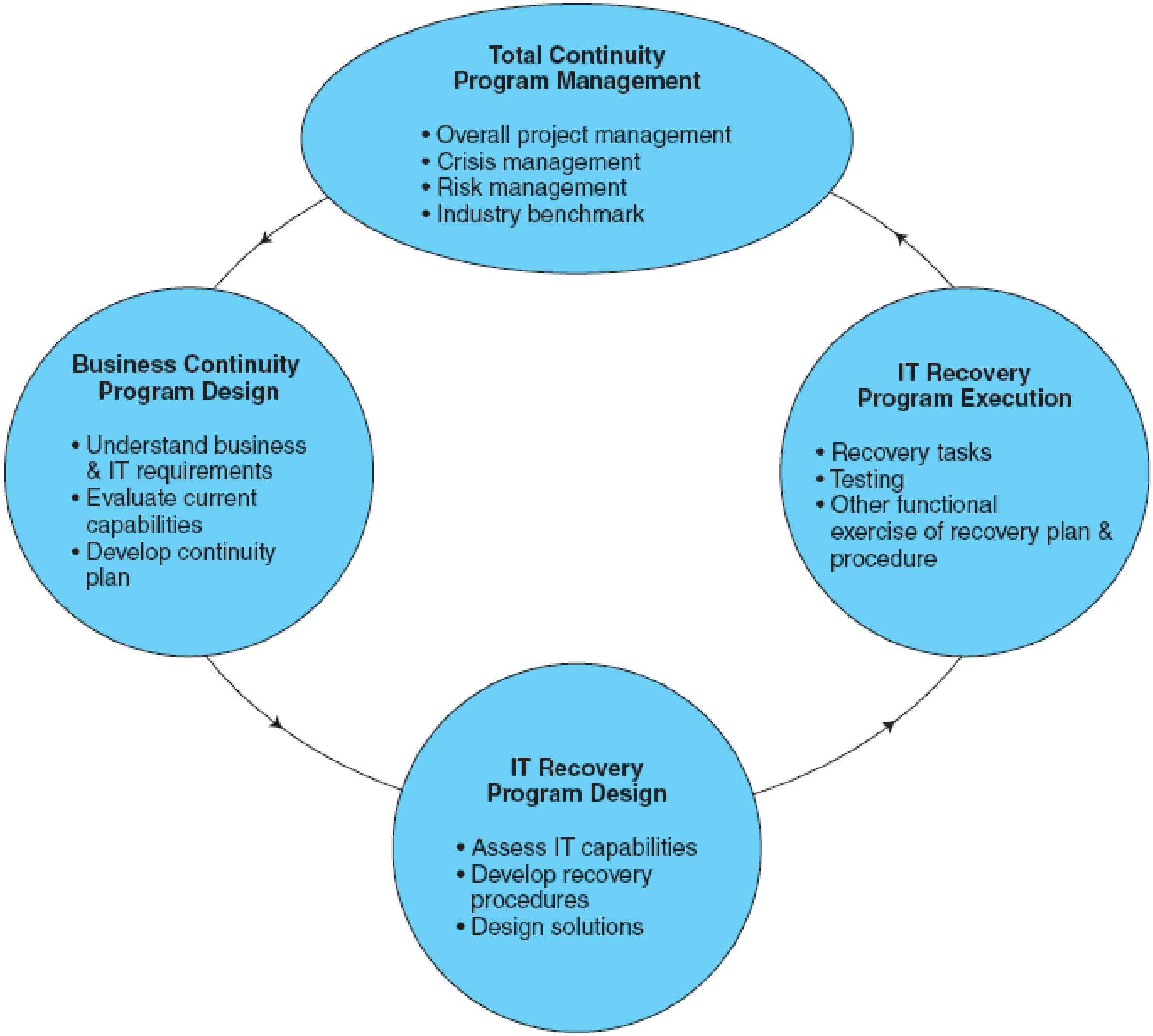
- **PROTECTING AGAINST POP-UP ADS**
- **PROTECTING AGAINST SOCIAL ENGINEERING ATTACKS**
  - **Protecting Against Phishing**
  - **Protecting Against Malvertising**
- **PROTECTING AGAINST SPYWARE**
  - **Using Policies and Training**

Business Continuity, Disaster Recovery, 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)

EXHIBIT 9.16 **Business Continuity Services and IT Recovery Process**



Total Continuity Program Management

- Overall project management
- Crisis management
- Risk management
- Industry benchmark

Business Continuity Program Design

- Understand business & IT requirements
- Evaluate current capabilities
- Develop continuity plan

IT Recovery Program Execution

- Recovery tasks
- Testing
- Other functional exercise of recovery plan & procedure

IT Recovery Program Design

- Assess IT capabilities
- Develop recovery procedures
- Design solutions

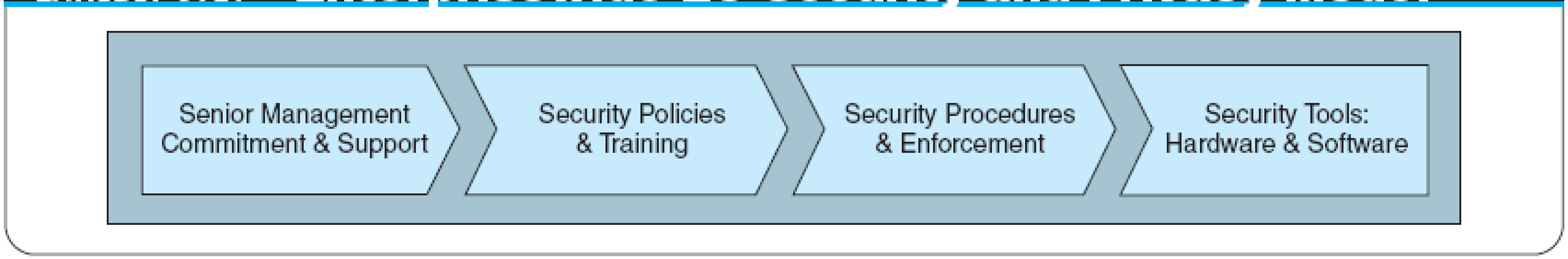
Business Continuity, Disaster Recovery, Security Auditing, and Risk Management

- **RISK-MANAGEMENT AND COST–BENEFIT ANALYSIS**
  - **Risk-Management Analysis**
  - **Calculating the Cost of a Fraud-Prevention System**
  - **Ethical Issues**

Implementing Enterprisewide E-Commerce Security

- THE DRIVERS OF EC SECURITY MANAGEMENT
- SENIOR MANAGEMENT COMMITMENT AND SUPPORT
  - Unified Front

EXHIBIT 9.17 Enterprisewide EC Security and Privacy Model


Senior Management Commitment & Support
Security Policies & Training
Security Procedures & Enforcement
Security Tools: Hardware & Software

Implementing Enterprisewide E-Commerce Security

- **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

Implementing Enterprisewide E-Commerce Security

- **WHY IS IT DIFFICULT TO STOP INTERNET CRIME?**
  - **Making Shopping Inconvenient**
  - **Lack of Cooperation from Credit Card Issuers and ISPs**
  - **Shoppers' Negligence**
  - **Ignoring EC Security Best Practices**
    - **Computing Technology Industry Association (CompTIA)**

      Nonprofit trade group providing information security research and best practices

Implementing Enterprisewide E-Commerce Security

- **Design and Architecture Issues**
- **Lack of Due Care in Business Practices**
  - **standard of due care**

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

Managerial Issues

1. What is the best EC security strategy for my company?
2. Is the budget for EC 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?

Summary

1. The key to establishing strong e-commerce security
2. Basic EC security issues and terminology
3. Threats, vulnerabilities, and technical attacks
4. Internet fraud, phishing, and spam
5. Information assurance
6. Securing EC access control and communications

Summary

7. Technologies for protecting networks.
8. The different controls and special defense mechanisms.
9. Protecting from fraud.
10. Role of business continuity and disaster recovery planning.
11. Enterprisewide EC security.
12. Why is it impossible to stop computer crimes?