E-Commerce Security and Fraud Issues and Protections

10

Contents

Learning Objectives

Upon completion of this chapter, you will be able to:

1. Understand the importance and scope of security of information systems for EC.
2. Describe the major concepts and terminology of EC security.
3. Understand 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.
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. Discuss enterprisewide implementation issues for EC security.
11. Understand why it is so difficult to stop computer crimes.

Electronic supplementary material The online version of this chapter (doi: 10.1007/978-3-319-10091-3_10) contains supplementary material, which is available to authorized users

E. Turban et al., *Electronic Commerce: A Managerial and Social Networks Perspective*, Springer Texts in Business and Economics, DOI 10.1007/978-3-319-10091-3_10,

OPENING CASE: HOW STATE UNIVERSITY OF NEW YORK COLLEGE AT OLD WESTBURY CONTROLS ITS INTERNET USE

The State University of New York (SUNY) College at Old Westbury (**oldwestbury.edu**) is a relatively small U.S. university located in Long Island, New York. The college has 3,300 students and 122 full-time faculty. Internet access is essential for both faculty and students.

The Problem

The College does not regulate the types of devices people use in its network, such as laptops, tablets, and smartphones, nor the purposes for which the devices are used. Thus, students, faculty, and networks are vulnerable to a variety of security issues, many of which originate from social media websites such as Facebook and YouTube. The College encourages the use of social media as a collaborative, sharing, and learning environment.

Social media is also a leading target for malware writers. With the large number of downloads, social media has become an ideal place for cybercriminals to insert viruses and hack into systems. Phishers use social engineering techniques to deceive users into clicking on, or downloading, malware.

Because of the various devices used by the students and faculty, the College's attempts to manage network security were unsuccessful. Specifically, the attempt to use intelligent agents (which some students objected to having on their computers) as guards failed.

The College had computer-use policies in place, but these were established in the past for older computing environments. Since the old policies were not effective, the university decided to transform its old usage policy to meet the needs of current technology.

Bandwidth usage was a problem due to the extensive downloading of videos by faculty and students. The high level usage for non educational related activities sometimes interfered with classroom or research needs.

The Solution

All students, faculty, and staff received a user ID for computer utilization. Next, a new usage policy was implemented. This policy was communicated to all users and was enforced by monitoring the usage for each ID, watching network traffic, and performing behavioral analysis.

The policy covered all users, all devices, and all types of usage, including mobile devices and the Internet. According to SUNY College at Old Westbury (2014), the policy states that users should not expect full privacy when it comes to their e-mail messages or other online private information, including Internet usage records and sets forth what information is collected by the university. Given that the IDs identify the type of users (e.g., student or faculty), management was able to set priorities in allocating bandwidth.

Old Westbury is not alone in utilizing a policy to control Internet usage. Social Media Governance (**socialmediagovernance.com**) is a website that provides tools and instructions regarding the control of computing resources where social media is concerned.

The Results

The new system monitors performance and automatically sends alerts to management when deviations from the policy occur (e.g., excessive usage). Also, it conducts behavioral analysis and reports behavioral changes of users.

The users are contacted via e-mail and alerted to the problem. The system may even block the user's access. In such an event, the user can go to the student computer lab for problem resolution.

Bandwidth is controlled only when classes are in session.

Sources: Based on Goodchild (2011), SUNY (2014), and **oldwestbury.edu** (accessed May 2014).

LESSONS LEARNED FROM THE CASE

This case demonstrates two problems: possible malware attacks and insufficient bandwidth. Both problems can reduce the effectiveness of SUNY's computerized system, interfering with students' learning and faculty teaching and research. The solution, in which the university can monitor when users are on the university network, look for any unusual activity, and take appropriate action if needed, demonstrates one of the defense mechanisms used by an organization. The new polices conflict with student privacy – a typical situation in security systems: the tighter the security, the less privacy and flexibility people have. In this chapter, we introduce the broad battlefield between attacks on information systems and the defense of those systems. We also present the issues of fraud in e-commerce and strategies and policies available to organizations for deploying security measures.

10.1 THE INFORMATION SECURITY PROBLEM

Information security refers to a variety of activities and methods that protect information systems, data, and procedures from any action designed to destroy, modify, or degrade the systems and their operations. In this chapter, we provide an overview of the generic information security problems and solutions as they relate to EC and IT. In this section, we look at the nature of the security problems, the magnitude of the problems, and introduce some essential terminology of information security.

What Is EC Security?

Computer security in general refers to the protection of data, networks, computer programs, computer power, and other elements of computerized information systems. It is a very broad field due to the many methods of attack as well as the many modes of defense. The attacks on and defenses for computers can affect individuals, organizations, countries, or the entire Web. Computer security aims to prevent, or at least minimize, the attacks. We classify computer security into two categories: *generic topics*, relating to any information system (e.g., encryption), and *EC-related issues*, such as buyers' protection. Attacks on EC websites, *identify theft* of both individuals and organizations, and a large variety of fraud schemes, such as phishing, are described in this chapter.

Information security has been ranked consistently as one of the top management concerns in the United States and many other countries. Figure 10.1 illustrates the major topics cited in various studies as being the most important in information security.

The Status of Computer Security in the United States

Several private and government organizations try to assess the status of computer security in the United States annually. Notable is the annual CSI report, which is described next.

No one really knows the true impact of online security breaches because, according to the Computer Security Institute (CSI; **gocsi.com**), 2010/2011 Computer Crime and Security Survey, only 27.5% of businesses report computer intrusions to legal authorities. The survey is available at **scadahacker.com/library/Documents/Insider_Threats/CSI%20-%202010-2011%20Computer%20Crime%20and%20Security%20Survey.pdf**. Comprehensive annual security surveys are published periodically by IBM, Symantec, and other organizations.

In addition to organizational security issues, there is also the issue of personal security.

Personal Security

Fraud on the Web is aimed mostly at individuals. In addition, loose security may mean danger of personal safety due to sex offenders who find their victims on the Internet.

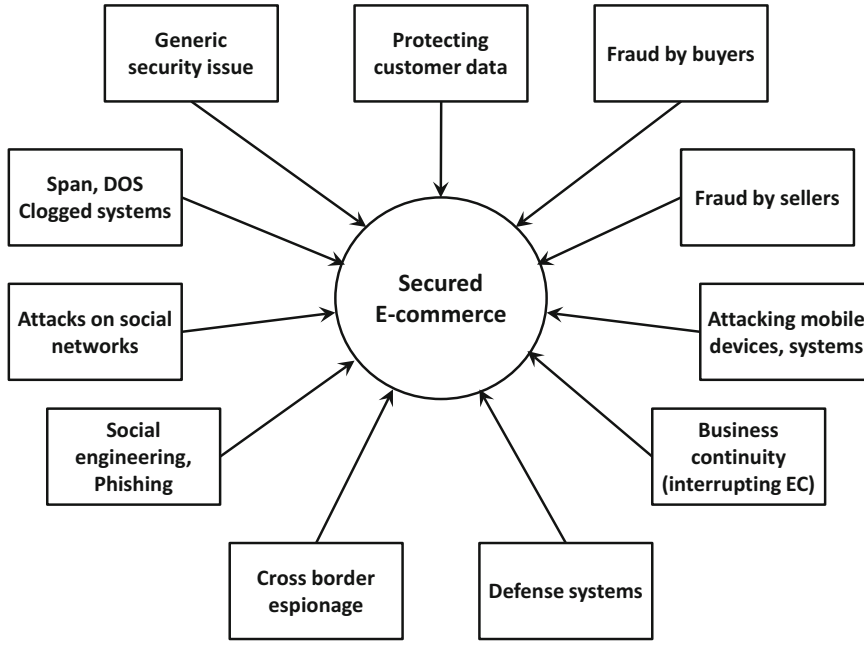

Figure 10.1 Major EC security management concerns for 2011

National Security

Protection of U.S. computer networks is handled by the Department of Homeland Security (DHS). It includes the following programs:

- **Cyber Security Preparedness and the National Cyber Alert System.** Computer users can stay up-to-date on cyberthreats through this program.
- **United States Computer Emergency Readiness Team (U.S.-CERT Operations).** Provides information about vulnerabilities and threats, proactively manages cyber risks to the nation, and operates a database to provide technical descriptions of vulnerabilities.
- **National Cyber Response Coordination Group (NCRCG).** Comprised of representatives from 13 federal agencies, it reviews threat assessments and recommends actions to incidents, including allocation of federal resources.
- **CyberCop Portal.** A portal designed for law enforcement and government officials to use the Internet to collaborate and share sensitive information with one another in a secure environment.

According to Goldman (2013), hackers are increasingly attacking the most critical infrastructures of the U.S. (e.g., power, nuclear, and water facilities). In 2012, a group of unidentified hackers broke into the corporate systems of some natural gas pipeline companies and stole data on how their control systems work. Goldman also states that according to industry researchers, many companies choose not to report cyberattacks.

On February 17, 2013, President Obama issued an executive order for combatting cyberwars. This order gave "federal agencies greater authority to share 'cyber threat' information with the public sector."

Security Risks for 2014 and 2015

According to IBM (2014) and EMC/RSA (2014), and security vendors, the major security risks for the near future are:

- Cyberespionage and cyberwars (discussed below) are growing threats.
- Attacks are now also against mobile assets, including on smartphones, tablets, and other mobile devices. Enterprise mobile devices are a particular target.
- Attacks on social networks and social software tools. User-generated content is a major source of malware.
- Attacks on BYOD ("Bring Your Own Device").
- Identity theft is exploding, increasing the criminal use of the stolen identities.
- Profit motive – as long as cybercriminals can make money, security threats and phishing attacks, will continue to grow.
- Social engineering tools such as phishing via e-mail are growing rapidly.
- Cybergang consolidation – underground groups are multiplying and getting bigger, especially in Internet fraud and cyberwars.
- Business-oriented spam (including image-based spam).
- Attacks using spyware (e.g., using Denial-of-Service method).
- Attacks on new technologies such as cloud computing and virtualization.
- Attacks on Web and mobile applications (apps).

We cover all the major topics on the above list in the rest of this chapter. According to Lawinski (2012), the major attacks on corporations are on executives (25%), shared mailboxes (23%) and sales (12%). While most of the attacks are against large enterprises (50%), hackers attack medium (32%) and small companies (48%) as well. Additionally, 93% of companies affected are in the health care or IT industries. We assume the 2014 to 2015 data will be similar.

For more information, see **sans.org**, **baselinemag.com/security**, **enisa.europa.eu/activities/risk-management**, and the Information Systems Security Certification Consortium (isc2.org).

Security Risks in Mobile Devices

According to Davis (2012b), the major mobile devices security concerns are: loss of devices that include sensitive information (66%); mobile devices infected by malware (60%); theft of data from the device (44%); users downloading malicious apps (33%); identity theft; and other user personal loss (30%).

Cyberwars and Cyberespionage Across Borders

Using computers as a tool to attack information systems and computers is growing rapidly and becoming more and more dangerous.

Cyberwarefare

According to the UN Crime and Justice Research Institute (Unicri), *Cyberwarefare* or (*Cyberwar*) refers to any action by a nation-state or international organization to penetrate another nation's computer networks for the purpose of causing damage or disruption. However, broader definitions claim that cyberwarfare also includes acts of 'cyberhooliganism,' cybervandalism or cyberterrorism. The attack usually is done through viruses, DoS, or botnets.

- Cyberwarfare, which is an illegal activity in most countries, includes the following major threats: Online acts of espionage and security breaches – which are done to obtain national material and information of a sensitive or classified nature through the exploitation of the Internet (e.g., exploitation of network flaws through malicious software).
- Sabotage – the use of the Internet to disrupt online communications with the intent to cause damage.
- Attacks on SCADA (Supervisory Control and Data Acquisition) network and NCIs (National Computational Infrastructure).

Cyberespionage

Cyberespionage refers to unauthorized spying using a computer system. Espionage involves obtaining secrets without the permission of the holder of the information (individual, group, or organization). Cyberespionage is an illegal activity in most countries.

Attacking Information Systems

The GhostNet attack cited earlier was not an isolated case of cross-border cyber attacks. In February 2011, the U.S. security firm McAfee, Inc. reported that Chinese hackers had stolen sensitive data from oil companies in the United States and several other countries. These attacks started in November 2009, and, as of 2011, are continuing. The attacks are done via e-mails containing a virus sent to tens of thousands of people (see **csmonitor.com/USA/2011/0210/Report-Chinese-hackers-targeted-big-oil-companies-stole-data**). The U.S. Congress is working on legislation to protect the country from what some call the 'Cyber Pearl Harbor' attack (however, others say it will not happen), or a digital 9/11 (Cowley 2012). In May 2014, the U.S. government named five military people in China as responsible for stealing data and spying on several thousand companies in the U.S. stealing trade secrets (Kravets 2014).

Types of Attacks

Cyber attacks can be classified into two major interrelated categories:

1. **Corporate espionage.** Many attacks target energy-related companies because their inside information is valuable (see McAfee 2011). According to a 2010 report by McAfee (as reported by News24 2011), almost half of all power plants and other infrastructures surveyed have been infiltrated by "sophisticated adversaries," with extortion being a common motive. For example, Nakashima (2011) reported that in November 2011, foreign hackers targeted a water plant control system in Illinois, causing the pump to fail. The attackers also gained unauthorized access to the system database. The Internet address used was tracked back to Russia. According to the *Wall Street Journal* of April 23, 2012, there were suspected cyber attacks against Iranian oil production and refineries. Cyber attackers hacked into 30,000 of Saudi Aramco's computers in 2012, and crippled the national oil company's networks, but failed to disrupt gas or oil output (Constantin 2012).

   Finally, in 2013, documents leaked from the whistleblower Edward Snowden revealed that Belgacom, a Belgian telecom company, was hacked into by a British spy agency (see **spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html**).

   According to Esposito and Ferran (2011), in 2011, cyber thieves (known as the "Rove group") based in Eastern Europe hijacked at least four million computers in more than 100 countries before they were caught. The attackers used malware and rerouted Internet traffic illegally. The cyber thieves stole $14 million before they were captured. The hackers also attacked U.S. government agencies and large corporations.

   The Chinese cyber attacking network not only installed malware to send and receive classified data from the compromised computers, but also gave them the ability to spy on people by using installed audio and video devices to monitor the rooms where the computers were located (however, investigators could not confirm whether the audio/visual had been used). In 2013, Chinese hackers allegedly attacked the *New York Times*' computers to intimidate the American news media into not reporting on China's negative image and the journalists' sources of this information.
2. **Political espionage and warfare.** Political espionage and cyberwars are increasing in magnitude. Sometimes, these are related to corporate espionage. In 2014, U.S. hackers in Illinois used DDoS malware to attack the official website of the Crimean referendum. A few days later, major Russian government Web resources and state media websites were also attacked by DDoS malware. For information about the Crimean website cyber attack, see **rt.com/news/crimea-referendum-attack-website-194**.

Example 1

In December 2010, the Iranian nuclear program was attacked via computer programs rumored to have been created by the United States and Israel. The attack was successful, causing major physical damage to the nuclear program, delaying it by months or possibly even years. The

attack was perpetrated using a sophisticated computer worm named Stuxnet. This is an example of a weapon created by a country to achieve a goal that otherwise may have been achieved only by physical weapons. In apparent retaliation, Iranians and pro-Palestinian hackers attacked El-Al (Israel's national airline) and the country's stock exchange. Iran is believed to have been behind a November 2012 attack on U.S. banks (see Goldman 2012).

Example 2

A suspected cyberespionage network known as GhostNet, compromised computer systems in 103 countries, including computer systems belonging to the Dalai Lama's exile network, embassies, and foreign ministries. The attacks allegedly came from China.

Example 3

One of the most complex cyberespionage incidents that has ever occurred (2014) is the suspected Russian spyware Turla, which was used to attack hundreds of government computers in the U.S. and Western Europe (see Apps and Finkle 2014).

The above incidents illustrate the ineffectiveness of some information security systems. For an overview of how cyberwarfare works, see **forbes.com/sites/quora/2013/07/18/how-does-cyber-warfare-work**.

For the implications of such warfare, see Dickey et al. (2010). For the U.S. Senate Homeland Security Committee's concerns and proposed legislation (e.g., the Cybersecurity Act of 2012, which failed), see Reske and Bachmann (2012).

The Drivers of EC Security Problems

There are many drivers (and inhibitors) that can cause security problems to EC. Here, we describe several major ones: the *Internet's vulnerable design*, the *shift to profit-induced crimes*, the *wireless revolution*, the *Internet underground economy*, the *dynamic nature of EC systems, and the role of insiders*, and the *sophistication of the attacks.*

The Internet's Vulnerable Design

The Internet and its network protocols were never intended to protect against cybercriminals. They were designed to accommodate computer-based communications in a *trusted community*. However, the Internet is now a global place for communication, search, and trading. Furthermore, the Internet was designed for maximum efficiency without regard for security. Despite improvements, the Internet is still fundamentally insecure.

The Shift to Profit-Induced Crimes

There is a clear shift in the nature of the operation of computer criminals (see IBM Corporation 2012). In the early days of e-commerce, many hackers simply wanted to gain fame or notoriety by defacing websites. Online File W10.1 illustrates a case of a criminal who did not attack systems to make a profit. There are many more criminals today, and they are more sophisticated and technical experts. Most popular is the theft of personal information such as credit card numbers, bank accounts, Internet IDs, and passwords. According to Privacy Rights Clearinghouse (**privacyrights.org**), approximately 250 million records containing personal information were involved in security breaches between April 2005 and April 2008 (reported by Palgon 2008). Today, the number is much higher. Criminals today are even holding data for ransom and trying to extort payments from their victims. An illustrative CNN video posted on October 8, 2012 (2:30 minutes) titled "Hackers Are Holding Data for Ransom" is available at **money.cnn.com/video/technology/2012/10/08/t-ransomware-hackers.cnnmoney**. CryptoLocker is a new ransomware Trojan used for such crimes (see **usatoday.com/story/news/nation/2014/05/14/ransom-ware-computer-dark-web-criminal/8843633**).

Note that laptop computers are stolen for two reasons: selling them (e.g., to pawn shops, on eBay) and trying to find the owners' personal information (e.g., social security number, driver's license details, and so forth). In January 2014, a former Coca-Cola employee stole laptops containing information on 74,000 individuals belonging to current and past employees of the company. The company did not have a data loss prevention program

in place, nor were the laptops encrypted (see **infosecurity-magazine.com/view/36627/74000-data-records-breached-on-stolen-cocacola-laptops**).

A major driver of data theft and other crimes is the ability to profit from the theft. Today, stolen data are sold on the black market, which is described next.

The Increased Volume of Wireless Activities and the Number of Mobile Devices

Wireless networks are more difficult to protect than wireline. For example, many smartphones are equipped with near-field communication (NFC) chips, which are necessary for mobile payments. Additionally, BYOD (Chapter 6) may create security problems. Hackers can exploit the features of smartphones and related devices (e.g., Bluetooth) with relative ease; see Drew (2012) for details.

The Globalization of the Attackers

Many countries have cyberattackers (e.g., China, Russia, Nigeria and India). See Fowler and Valentino-DeVries (2013) for cyberattacks originating in India.

The Darknet and the Underground Economy

The **darknet** can be viewed as a separate Internet that can be accessed via the regular Internet and a connection to the TOR network (TOR is a network of VPNs that allows privacy and security on the Internet). The darknet has restricted access to trusted people ("friends") by using non standard protocols (IP addresses are not listed). Darknet allows anonymous surfing. For a tutorial, see Kalomni (2012). The darknet's contents are not accessible through Google or other search engines. The TOR technology is used in file sharing (e.g., see the Pirate Bay case in Chapter 15). The darknet is often used for political dissent and conducting illegal transactions, such selling drugs and pirating intellectual property via file sharing. The latter activity is known as the *Internet underground economy*.

In November 2014, law enforcement authorities in Europe and the U.S. shut down many of TOR websites. But it seems they have not cracked TOR encryptions yet (Dalton and Grossman 2014).

The Internet Underground Economy

The **Internet underground economy** refers to the e-markets for stolen information made up of thousands of websites that sell credit card numbers, social security numbers, e-mail addresses, bank account numbers, social network IDs, passwords, and much more. For details, see the Symantec Report on the Underground Economy: July 07-June 08 (2008) and, their Fraud Activity Trends (2009–2010) at **symantec.com/threatreport/topic.jsp?id=fraud_activity_trends&aid=underground_economy_servers**. Stolen data are sold to spammers or criminals for less than a dollar a piece to several hundred dollars each. The purchasers use them to send spam or conduct illegal financial transactions such as transferring other people's money into their own accounts, or paying their credit card bills. It is estimated that about 30% of all the transactions in the underground market are made with stolen credit cards. Symantec estimates the potential worth of just the credit cards and banking information for sale was $7 billion. Forty-one percent of the underground economy is in the United States, while 13% is in Romania. The Symantec report also covers the issue of software piracy, which is estimated to be more than $100 million annually. Criminals use several methods to steal the information they sell. One popular method is *keystroke logging.*

The Internet Silk Road

This is one of the underground sites where hundreds of drug dealers and other 'black market' merchants conduct their business. In October 2013, law enforcement authorities in the U.S. shut down the site and arrested its founder. However, shortly thereafter, Silk Road was "resurrected" as Silk Road 2.0.

Transactions on Silk Road are paid only by *bitcoins* (Chapter 11). In February 2014, hackers stole over 4,400 bitcoins that were held in escrow (between buyers and sellers); over $2.7 million

value of bitcoins are gone forever (see Pagliery 2014). The owner of the Silk Road site declared bankruptcy. However, by May 2014 the site was back in business.

Keystroke Logging in the Underground Economy

Keystroke logging (keylogging) is the process of using a device or software program that tracks and records the activity of a user in real time (without the user's knowledge or consent) by the keyboard keys they press. Since personal information such as passwords and user names are entered on a keyboard, the keylogger can use the keystrokes to obtain them. A keylogger can also be a malware Trojan installed to infect the user's computer with viruses and steal confidential information. Keylogging methods and their tutorials are available free on the Web. For more information, see **pctools.com/security-news/what-is-a-keylogger**. The more sophisticated the underground economy is, the more criminals will use keylogging to obtain users' personal information to sell in underground marketplaces.

The Explosion of Social Networking

The huge growth of social networking and the proliferation of platforms and tools make it difficult to protect against hackers. Social networks are easy targets for phishing and other social engineering attacks.

The Dynamic Nature of EC Systems and the Acts of Insiders

EC systems are changing all the time due to a stream of innovations. Security problems often accompany change. In recent years, we have experienced many security problems in the new areas of social networks and wireless systems (some will be explored later in this book). Note that insiders (people who work for the attacked organizations) are responsible for almost half of the security problems. New employees are being added frequently to organizations, and they may bring security threats with them.

The Sophistication of the Attacks

Cybercriminals are sharpening their weapons continuously, using technological innovations. In addition, criminals are getting organized in very powerful groups, such as LulzSec and Anonymous. According to IBM Corporation (2012), cybercriminals change their tactics because of improved security in a certain area (i.e., they are adapting quickly to a changing environment). See Acohido (2011).

The Cost of Cyber Crime

It is not clear how much cybercrime costs. Many companies do not disclose their losses. However, HP Enterprise Security's "2013 Cost of Cyber Crime Study: Global Report" (independently conducted by Ponemon Institute) found that the average annualized cost of cybercrime per company surveyed was $7.2 million per year, which is an increase of 30% from the previous year's global cyber cost study. Data breaches can be very costly to organizations (see Kirk 2013). For how organizations can be devastated by cyberattacks, see Kavilanz (2013b).

SECTION 10.1 REVIEW QUESTIONS

1. Define computer security.
2. List the major findings of the CSI 2010/2011 survey.
3. Describe the vulnerable design of the Internet.
4. Describe some profit-induced computer crimes.
5. Describe the Internet underground economy and the darknet.
6. Describe the dynamic nature of EC systems.
7. Relate security issues to social networks and mobile computing.

10.2 BASIC E-COMMERCE SECURITY ISSUES AND LANDSCAPE

In order to understand security problems better, we need to understand some basic concepts in EC and IT security. We begin with some basic terminology frequently related to security issues.

Basic Security Terminology

In Section 10.1, we introduced some key concepts and security terms. We begin this section by introducing alphabetically the major terms needed to understand EC security issues:

Business continuity plan
Cybercrime
Cybercriminal
Exposure
Fraud
Malware (malicious software)
Phishing
Risk
Social engineering
Spam
Vulnerability
Zombie

Definitions of these terms are provided later in the chapter glossary and at **webopedia.com/TERM**.

The EC Security Battleground

The essence of EC security can be viewed as a battleground between attackers and defenders and the defenders' security requirements. This battleground includes the following components, as shown in Figure 10.2:

- The attacks, the attackers, and their strategies
- The assets that are being attacked (the targets) in vulnerable areas
- The security defense, the defenders, and their methods and strategy

The Threats, Attacks, and Attackers

Information systems, including EC, are vulnerable to both unintentional and intentional threats. (For a discussion, see IBM Corporation 2012).

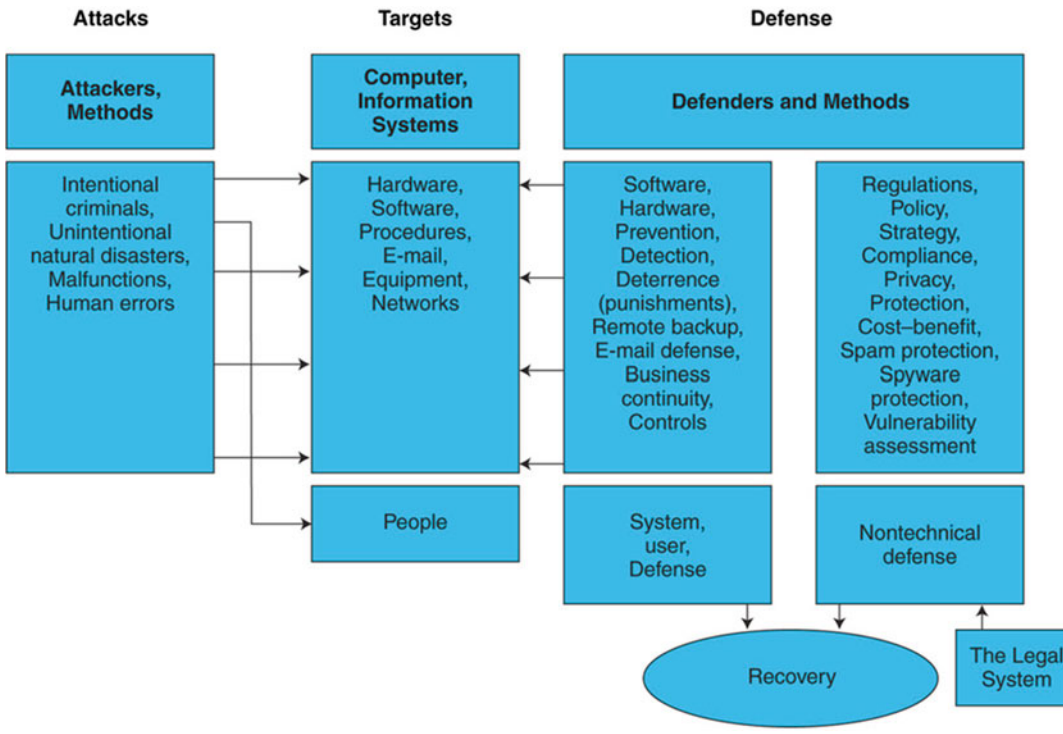

Figure 10.2 The EC security battleground

Unintentional Threats

Unintentional threats fall into three major categories: human error, environmental hazards, and malfunctions in the computer system.

Human Error

Human errors can occur in the design of the hardware, software, or information systems. It can also occur in programming (e.g., forgetting to factor in leap year), testing, data collection, data entry, authorization, and instructions. Errors can occur because of negligence, outdated security procedures or inadequate employee training, or because passwords are not changed or are shared with others. According to the 2013 *Cost of Breach Study: Global Analysis* by Symantec and Ponemon Institute, human error accounted for over half of data breaches in 2012 (see HP Enterprise Security 2013).

Environmental Hazards

These include natural disasters and other environmental conditions outside of human control (e.g., Acts of God, large scale acts of nature and accidents such as earthquakes, severe storms, hurricanes, blizzards, or sand storms), floods, power failures or strong fluctuations, fires (the most common hazard), explosions, radioactive fallout, and water-cooling system failures. Computer resources also can be damaged by side effects such as smoke and water. Damages during wars or property vandalism are a special kind of environmental hazards.

Malfunctions in the Computer System

Defects can be the result of poor manufacturing, defective materials, memory leaks, and outdated or poorly maintained networks. Unintentional malfunctions can also happen for other causes, ranging from lack of user experience to inadequate testing. For example, in March 2012, a computer glitch (related to United Airlines switching over to the computer system used by Continental Airlines after their merger) overloaded United Airlines' phone lines and caused flight delays, causing frustration for customers, and the problem continutes. According to the *Sydney Morning Herald Traveller* (January 13, 2014), United Airlines "is still struggling to integrate Continental Airlines more than three years after their merger" (see **smh.com.au/travel/travel-essentials/travel-news/united-airlines-computer-glitch-strands-pilots-20140113-30q4d.html**). In the early part of 2014, United was still having problems with their computer system, with hundreds of flights being cancelled and thousands being delayed. United's computer problems extended to printing boarding passes, checking in passengers, and getting baggage tags. According to United, most of the problems were due to the computer glitches. (For the problems United is facing due to computer glitches in 2014, see **dailymail.co.uk/wires/ap/article-2562268/Flight-delays-soar-winter-storm-United-glitch.html**.)

Another example is Amazon's Cloud (EC2), which hosts many major websites (e.g., Reddit, Airbnb, Foursqure). In June and October 2012, the cloud hosting service crashed due to problems with the company's data centers. The system also crashed in July 2012, taking down Netflix, Foursquare, Dropbox, Instagram, and Pinterest due to severe weather hitting the North Virginia data center.

Intentional Attacks and Crimes

Intentional attacks are committed by cybercriminals. Types of intentional attacks include theft of data; inappropriate use of data (e.g., changing it or presenting it for fraudulent purposes); theft of laptops and other devices and equipment and/or

computer programs to steal data; vandalism or sabotage directed toward the computer or its information system; damaging computer resources; losses from malware attacks; creating and distributing viruses; and causing monetary losses due to Internet fraud. Most of these are described in Sections 10.3 and 10.4.

For a 2013 state of the art study including all threats, see Suby (2013).

The Criminals and Methods

Intentional crimes carried out using computers and the Internet are called *cybercrimes*, which are done by *cybercriminals* (*criminals* for short), that includes *hackers and crackers.* A **hacker** describes someone who gains unauthorized access to a computer system. A **cracker**, (also known as a *"black hat" hacker*), is a *malicious hacker* with extensive computer experience who may be more damaging. According to PC Tools, "hackers build things while crackers break things. Cracker is the name given to hackers who break into computers for criminal gain…Crackers' motivations can range from profit, a cause they believe in, general maliciousness or just because they like the challenge. They may steal credit card numbers, leave viruses, destroy files or collect personal information to sell." (See **pctools.com/security-news/crackers-and-hackers** for the differences between crackers and hackers.) Some hacker groups (such as the international group Anonymous) are considered unstoppable in penetrating organizations of all kinds (many U.S. government agencies, including the U.S. Army and the Department of Energy). The danger is that some companies may not take even minimal precautions to protect their customer information if they can place the blame for the attacks on the cybercriminals (see Murray 2011).

Unlike "black hat" hackers, "white hat" hackers can be Internet security experts who are hired by companies to find vulnerabilities in their computer systems.

Criminals use a variety of methods for the attacks. Some use computers as a weapon; some attack computing assets depending on the targets. For a short history of hacking (with an infographic) see **i-programmer.info/news/149-security/3972-a-short-history-of-hacking.html**.

Hackers and crackers may recruit unsuspecting people, including company insiders, to assist in their crimes. For example, according to Malware Bytes Unpacked, a "money mule" is a person who is local to the compromised account, who can receive money transfers with a lesser chance of alerting the banking authorities.

"These money mules retrieve the funds and then transfer them to the cyber criminal." Since the mules are used to transfer stolen money, they can face criminal charges and become victims of identity theft. Notorious hacker Kevin Mitnick, who served jail time for hacking, used social engineering as his primary method to gain access to computer systems.

For 10 tips to keeping your EC website protected against hacking and fraud, see **tweakyourbiz.com/technology/2014/01/20/10-tips-to-protect-an-ecommerce-website-against-hacking-and-fraud**.

The Targets of the Attacks in Vulnerable Areas

As seen in Figure 10.2, the targets can be people, computers, or information systems. Fraud usually aims to steal money or other assets such as real estate. Computers are also used to harass people (e.g., cyberbullying), damage their reputation, violate their privacy, and so forth.

Vulnerable Areas Are Being Attacked

Any part of an information system can be attacked. PCs, tablets, or smartphones can easily be stolen or attacked by viruses and/or malware. Users can become victims of a variety of fraudulent actions. Databases can be attacked by unauthorized intruders, and data are very vulnerable in many places in a computerized system. For example, data can be copied, altered, or stolen. Networks can be attacked, and information flow can be stopped or altered. Computer terminals, printers, and any other pieces of equipment can be damaged in different ways. Software programs can be manipulated. Procedures and policies may be altered, and much more. *Vulnerable* areas are frequently attacked.

Vulnerability Information

A *vulnerability* is where an attacker finds a weakness in the system and then exploits that weakness. Vulnerability creates opportunities for attackers to damage information systems. MITRE Corporation publishes a dictionary of publicly known security vulnerabilities called *common vulnerabilities and exposures (CVE)* (**cve.mitre.org**). In a December 27, 2006 article in *SC Magazine*, MITRE reported that four of the top five reported vulnerabilities were within Web applications. *Exposure* can result when a cybercriminal exploits a vulnerability. See also Microsoft's guide to threats and vulnerabilities at **technet.microsoft.com/en-us/library/dd159785.aspx**.

Attacking E-Mail

One of the easiest places to attack is a user's e-mail, since it travels via the unsecured Internet. One example is the ease of former candidate for U.S. Vice President Sarah Palin's e-mail that was hacked in March 2008.

Attacking Smartphones and Wireless Systems

Since mobile devices are more vulnerable than wired systems, attacking smartphones and wireless systems is becoming popular due to the explosive growth of mobile computing.

The Vulnerability of RFID Chips

These chips are embedded everywhere, including in credit cards and U.S. passports. Cards are designed to be read from some distance (contactless), which also creates a vulnerability. When you carry a credit card in your wallet or pocket, anyone with a RFID reader that gets close enough to you may be able to read the RFID information on your card. For a presentation, watch the video "How to Hack RFID-Enabled Credit Cards for $8 (BBtv)" at **youtube.com/watch?v=vmajlKJlT3U**.

The Vulnerabilities in Business IT and EC Systems

Sullivan (2009) divided the vulnerabilities into *technical weaknesses* (e.g., unencrypted communications; insufficient use of security programs and firewalls) and *organizational weaknesses* (e.g., lack of user training and security awareness, and an insider who steals data and engages in inappropriate use of business computers).

Many areas can be vulnerable, some of which we do not even think about (e.g., RFID). A related topic is that of intellectual property piracy.

Pirated Videos, Music, and Other Copyrighted Material

It is relatively easy to illegally download, copy, or distribute music, videos, books, software, and other intellectual property when it is on the Web. Online piracy occurs when illegal software is downloaded from a peer-to-peer network. An example is the pirating of live sports events. At stake are millions of dollars in lost revenue to sports leagues and media companies. These institutions are joining forces in lobbying for stronger copyright legislation and by filing lawsuits against violators (see Chapter 15 for details). For a comprehensive discussion, see Stone (2011). For facts and statistics about online piracy, see **articles.latimes.com/2013/sep/17/business/la-fi-ct-piracy-bandwith-20130917**.

EC Security Requirements

Good security is a key success factor in EC.

The following set of security requirements are used to assure success and to minimize EC transaction risks:

- **Authentication. Authentication** is a process used to verify (assure) the real identity of an EC entity, which could be an individual, software agent, computer program, or EC website. For electronic messages, authentication verifies that the sender/receiver of the message is who the person or organization claims to be. (The ability to detect the identity of a person/entity with whom you are doing business.)
- **Authorization. Authorization** is the provision of permission to an authenticated

person to access systems and perform certain operations in those specific systems.

- **Auditing.** When a person or program accesses a website or queries a database, various pieces of information are recorded or logged into a file. The process of maintaining or revisiting the sequence of events during the transaction, when, and by whom, is known as *auditing*.
- **Availability.** Assuring that systems and information are available to the user when needed and that the site continues to function. Appropriate hardware, software, and procedures ensure availability.
- **Nonrepudiation.** Closely associated with authentication is **nonrepudiation**, which is the assurance that online customers or trading partners will not be able to falsely deny (repudiate) their purchase, transaction, sale, or other obligation. Nonrepudiation involves several assurances, including providing proof of delivery from the sender and proof of sender and recipient identities and the identity of the delivery company.

Authentication and non-repudiation are potential defenses against phishing and identity theft. To protect and ensure trust in EC transactions, *digital signatures*, or *digital certificates*, are often added to validate the senders and the times of the transactions so buyers are not able to deny that they authorized a transaction or that it never occurred. Section 10.6 provides a technical overview of digital signatures and certificates and how they provide verification in EC. Unfortunately, phishers and spammers have devised ways to compromise certain types of digital signatures.

The Defense: Defenders, Strategy, and Methods

Everybody should be concerned about security. However, in a company, the information systems department and security vendors provide the technical side, while management provides the administrative aspects. Such activities are done via security and strategy procedures that users need to follow.

EC Defense Programs and Strategy

An **EC security strategy** consists of multiple layers of defense that includes several methods. This defense aims to deter, prevent, and detect unauthorized entry into an organization's computer and information systems. **Deterrent methods** are countermeasures that make criminals abandon their idea of attacking a specific system (e.g., a possible deterrent is a realistic expectation of being caught and punished). **Prevention measures** help stop unauthorized people from accessing the EC system (e.g., by using authentication devices and firewalls or by using *intrusion prevention* which is, according to TechTarget "a preemptive approach to network security used to identify potential threats and respond to them swiftly"). **Detection measures** help find security breaches in computer systems. Usually this means to find out whether intruders are attempting (or have attempted) to break into the EC system, whether they were successful, whether they are still damaging the system, and what damage they may have done. This needs to be done as early as possible after a criminal attempt is made and can be done with an *intrusion detecting system*.

Information Assurance

Making sure that a customer is safe and secure while shopping online is a crucial part of improving the online buyer's experience. **Information assurance (IA)** is measures taken to protect information systems and their processes against all risks. In other words assure the systems' availability when needed. The assurance includes all tools and defense methods.

Possible Punishment

A part of the defense is to deter criminals by punishing them heavily if they are caught. Judges now are giving more and harsher punishments than a decade ago. For example, in March 2010, a federal judge sentenced 28 year old TJX hacker Albert Gonzalez to 20 years in prison for his role in stealing millions of credit and debit card num-

bers and selling them. Such severe sentences send a powerful message to hackers and help the defense. Unfortunately, in many cases the punishment is too light to deter the cybercriminals (see Jones and Bartlett Learning LLC 2012).

Defense Methods and Technologies

There are hundreds of security defense methods, technologies, and vendors and these can be classified in different ways so their analyses and selection may be difficult. We introduce only some of them in Sections 10.5, 10.6, 10.7, 10.8, and 10.9.

Recovery

In security battles, there are winners and losers in each security episode, but it is difficult to win the security war. As we will discuss in Section 10.9, there are many reasons for this. On the other hand, organizations and individuals usually recover after a security breach. Recovery is especially critical in cases of a disaster or a major attack, and it must be speedy. Organizations need to continue their business until the information systems are fully restored, and they need to restore them fast. This is accomplished by activating *business continuity and disaster recovery plans.*

Because of the complexity of EC and network security, comprehensive coverage requires an entire book, or even several books. Here we cover only selected topics. Those readers interested in a more comprehensive discussion should see the *Pearson/Prentice Hall Security Series* of security books and also conduct a Google search.

SECTION 10.2 REVIEW QUESTIONS

1. List five major EC security terms.
2. Describe the major unintentional security hazards.
3. List five examples of intentional EC security crimes.
4. Describe the security battleground, who participates, and how. What are the possible results?
5. Define hacker and cracker.
6. List all security requirements and define authentication and authorization requirements.
7. What is non-repudiation?
8. Describe vulnerability and provide some examples of potential attacks.
9. Describe deterring, preventing, and detecting in EC security systems.
10. What is a security strategy, and why it is needed?

10.3 TECHNICAL MALWARE ATTACK METHODS: FROM VIRUSES TO DENIAL OF SERVICE

There are many ways criminals attack information systems and users (see Suby 2013 for a survey). Here, we cover some major representative methods.

It is helpful to distinguish between two common types of attacks – *technical* (which we discuss in this section) and *nontechnical* (or *organizational*), which we discuss in Section 10.4.

Technical and Nontechnical Attacks: An Overview

Software and systems knowledge are used to perpetrate *technical attacks.* Insufficient use of antivirus and personal firewalls and unencrypted communication are the major reasons for technical vulnerabilities.

Organizational attacks are those where the security of a network or the computer is compromised (e.g., lack of proper security awareness training). According to Sullivan (2009), "Organizational vulnerability is the improper use of computers and network services." We consider *financial fraud*, *spam*, *social engineering,* that includes *phishing,* and other fraud methods as nontechnical. The goals of social engineering are to gain unauthorized access to systems or information by persuading unsuspected people to disclose personal information that is used by criminals to conduct fraud and other crimes. The major nontechnical methods are described in Section 10.4.

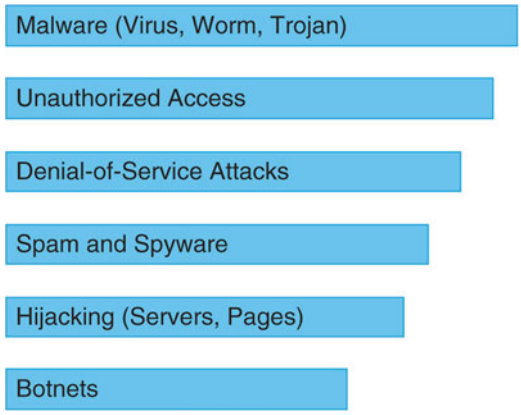

Figure 10.3 The major technical security attack methods (in descending order of importance)

The Major Technical Attack Methods

Hackers often use several software tools (which unfortunately are readily and freely available over the Internet together with tutorials on how to use them) in order to learn about vulnerabilities as well as attack procedures. The major technical attack methods are illustrated in Figure 10.3 and are briefly described next. Note that there are many other methods such as "Mass SQL Injection" attacks that can be very damaging.

Malware (Malicious Code): Viruses, Worms, and Trojan Horses

Malware (or *malicious software*) is software code, that when spread, is designed to infect, alter, damage, delete, or replace data or an information system without the owner's knowledge or consent. Malware is a comprehensive term that describes any malicious code or software (e.g., a virus is a "subset" of malware). According to Lawinski (2011), malware attacks are the most frequent security breaches, affecting 22% of companies. Computer systems infected by malware take orders from the criminals and do things such as send spam or steal the user's stored passwords.

Malware includes computer viruses, worms, botnets, Trojan horses, phishing tools, spyware tools, and other malicious and unwanted software. For an overview, see "malware and the malicious web" at IBM Corporation (2012).

Viruses

A **virus** is programmed software inserted by criminals into a computer to damage the system; running the infected host program activates the virus. A virus has two basic capabilities. First, it has a mechanism by which it spreads. Second, it can carry out damaging activities the once it is activated. Sometimes a particular event triggers the virus's execution. For instance, Michelangelo's birth date triggered the infamous Michelangelo virus. On April 1, 2009, the entire world was waiting for a virus named Conficker (see Brooks 2009). In 2014, a virus by the name of "Pony" infected hundreds of thousands of computers to steal bitcoins and other currencies (see Finkle 2014). Finally, Finkle reports that a virus named Agent BTZ attacked over 400,000 computers in Russia, the U.S., and Europe. The big attack was not successful, but viruses continue to spread all the time. For how computer viruses work, see **computer.howstuffworks.com/virus.htm**. Some viruses simply infect and spread, causing only minor damage. Others do substantial damage (e.g., deleting files or corrupting the hard drive).

According to Kaspersky Lab (a major Russian Internet crime fighting company), malware-based crime is growing very rapidly.

Web-based malware is very popular today. Virus attacks are the most frequent computer attacks. The process of a virus attack is illustrated in Figure 10.4.

Viruses are dangerous, especially for small companies. In 2013, the CryptoLocker virus was used to blackmail companies after seizing their computer files and threatening to erase their content.

For tutorials on, and information about, viruses, see Scott (2014) and Dawn Ontario (undated). For symptoms of, and diagnosis tips for PC

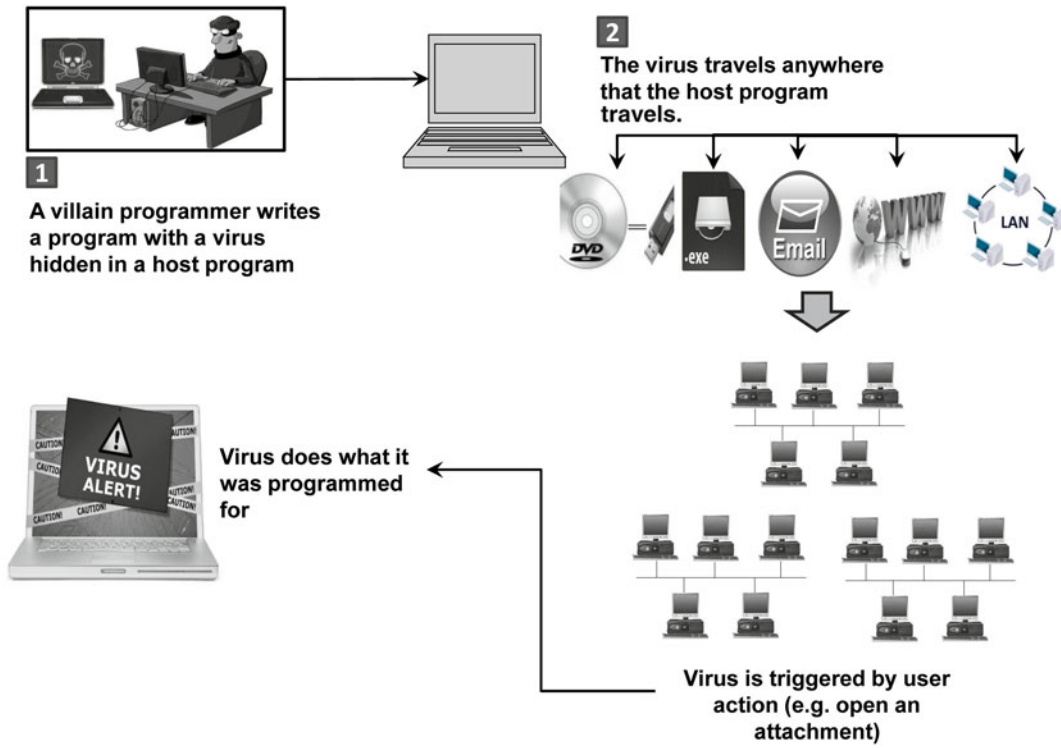

Figure 10.4 How a computer virus can spread

viruses, see Worley (2012). Note that in Microsoft tutorials, you will learn how to identify a computer virus, how to know if you are infected, and how to protect yourself against viruses (see the Microsoft Safety and Security Center at **microsoft.com/security/default.aspx**). Computer programs that are very similar to viruses are worms and Trojan horses.

Worms

Unlike a virus, a **worm** can replicate itself automatically (as a "standalone" – without any host or human activation). Worms use networks to propagate and infect a computer or handheld device and can even spread via instant messages or e-mail. In addition, unlike viruses that generally are confined within a target computer, a worm can infect many devices in a network as well as degrade the network's performance. According to Cisco, "worms either exploit a vulnerability on the target system or use some kind of social engineering to trick users into executing them." Because worms spread much more rapidly than viruses, they may be more dangerous.

Macro Viruses and Microworms

A **macro virus (macro worm)** is a malware code that is attached to a data file rather than to an executable program (e.g., a Word file). According to Microsoft, macro viruses can attack Word files as well as any other application that uses a programming language. When the document is opened or closed, the virus can spread to other documents on the computer's system. For information about Word macro viruses, see Microsoft Support at **support.microsoft.com/kb/187243/en**.

Trojan Horse

A **Trojan horse** is a program that seems to be harmless or even looks useful but actually contains a hidden malicious code. Users are tricked into executing an infected file, where it attacks the host, anywhere from inserting pop-up windows to

damaging the host by deleting files, spreading malware, and so forth. The name is derived from the Trojan horse in Greek mythology. Legend has it that during the Trojan War, the city of Troy was presented with a large wooden horse as a gift to the goddess Athena. The Trojans hauled the horse inside the city gates. During the night, Greek soldiers who were hiding in the hollow horse opened the gates of Troy and let in the Greek army. The army was able to take the city and win the war.

Trojans spread only by user interaction (e.g., such as opening an under the guise of an e-mail allegedly sent by Verizon), and there are many variants of Trojans (e.g., Zeus, W32) that will be discussed later.

Example 1: Trojan-Phisher-Rebery

In 2006, a variant of a Trojan horse program named *Trojan-Phisher-Rebery* was used to steal tens of thousands of identities from people in 125 different countries. The Rebery malicious software is an example of a **banking Trojan**, which is programmed to create damage when users visit certain online banking or e-commerce sites. For an infographic describing the state of financial Trojans see Symantec (2014).

Example 2: The DDOS Attacks on WordPress

In March 2014, hackers used a botnet to attack more than 162,000 WordPress sites. Given that WordPress powers about 17% of the world's blogging websites, any attack can be devastating (see BBC News Technology 2013).

Some Recent Security Bugs: Heartbleed and Crytolocker

Two dangerous computer bugs were discovered in 2013 and 2014.

Heartbleed

According to Russel (2014) "Heartbleed is a flaw in OpenSSL, the open-source encryption standard used by the majority of websites that need to transmit the data that users want to keep secure. It basically gives you a secure line when you're sending an e-mail or chatting on IM."

Encryption works by making it so that the data sent looks like nonsense to anyone but the intended recipient. Occasionally, one computer might want to check that there's still a computer at the end of its secure connection, and it will send out what's known as a heartbreak, a small packet of data that asks for a response.

Because of a programming error in the implementation of OpenSSL, researchers found that it was possible to send a well-disguised packet of data that looked like one of these heartbeats to trick the computer at the other end into sending data stored in its memory.

The potential damage may be large. In theory, any data kept in the active memory can be pulled out by the bug. Hackers can even steal encryption keys that enable them to read encrypted messages. About 650 million websites may be affected. The only advice provided by experts is to change the online passwords. The Mashable Team (2014) provides a list of popular websites that are affected.

Cryptolocker

Discovered in September 2013, Cryptolocker is a ransomware Trojan bug. This malware can come from many sources including e-mail attachments, can encrypt files on your computer, so that you cannot read these files. The malware owner then offers to decrypt the data in exchange for a Bitcoin or similar untraceable payment system.

For information on what to do if you are being blackmailed and how to protect yourself see Cannell (2013).

Denial of Service

According to Incapsula, Inc., a **denial-of-service (DoS) attack** is "a malicious attempt to make a server or network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet." This causes the system to crash or become unable to respond in time, so the site becomes unavailable. One of the most popular types of DoS attacks occurs when a hacker "floods" the system by overloading the system with "useless traffic" so a user is prevented from accessing their e-mail, websites, etc.

Note: A DoS attack is a malicious attack caused by one computer and one Internet connection as opposed to a DDos attack, which involves many devices and multiple Internet connections

(to be discussed later). An attacker can also use spam e-mail messages to launch a similar attack on your e-mail account. A common method of launching DoS attacks is by using *zombie (hijacked) computers*, which enable the hijacked computer to be controlled remotely by a hacker without the knowledge of the computer's owner. The zombie computer (also known as a 'botnet') launches an overwhelming number of requests toward an attacked website, creating the DoS. For example, DoS attackers target social networks, especially Facebook and Twitter. An example of such an attack is described in Online File W10.1.

DoS attacks can be difficult to stop. Fortunately, the security community has developed tools for combating them. For comprehensive coverage, see **us-cert.gov/ncas/tips/ST04-015**.

Web Server and Web Page Hijacking

Page hijacking, *or pagejacking*, is illegally copying website content so that a user is misdirected to a different website. Social media accounts are sometimes hijacked for the purpose of stealing the account holder's personal information. For example, Justin Bieber's 50 million followers fell victim to this when Bieber's Twitter account was hijacked in March 2014 (see Lyne 2014). The account was embedded with a malicious link to an application that was used to hijack accounts and retweeted to their friends.

Botnets

According to the Microsoft Safety and Security Center, a **botnet** (also known as "zombie army"), is malicious software that criminals distribute to infect a large number of hijacked Internet connected computers controlled by hackers. These infected computers then form a "botnet," causing the personal computer to "perform unauthorized attacks over the Internet" without the user's knowledge. Unauthorized tasks include sending spam and e-mail messages, attacking computers and servers, and committing other kinds of fraud, causing the user's computer to slow down (**microsoft.com/security/resources/botnet-whatis.aspx**).

Each attacking computer is considered *computer robot.* According to Prince (2010a), a botnet made up of 75,000 systems infected with the Zeus Trojan contaminated computers within 2,500 companies worldwide in 2010. Among its targets were the login credentials for Facebook, Yahoo!, and other popular sites, including financial and e-mail systems.

For the six most dangerous cyberattacks, including the Timthumb attack, see Kavilanz (2013a). Botnets are used in scams, spams, frauds, or just to damage systems (as in the hospital case described in Online File W10.1). Botnets appear in different forms and can include worms or viruses. Famous botnets include Zeus, Srizbi, Pushdo/Cutwail, Torpig, and Conficker.

Example

Rustock was a botnet made up of about one million hijacked PCs, which evaded discovery for years. The botnet, which sent out up to 30 billion spam messages per day, placed "booby trapped" advertisements and links on websites visited by the victims. The spammers camouflaged the updates to PCs to look like comments in discussion boards, which made them hard to find by security software. In March 2011, Microsoft was one of the companies that helped shut down Rustock (reported by BBC News Technology 2011). In 2013, Microsoft and the FBI "disrupted" over 1,000 botnets used to steal banking information and identities. Both Microsoft and the FBI had been trying to take down the malware "Citadel," which affected millions of people located in more than 90 countries, since early 2012 (see Albanesius 2013). For an analysis of malicious botnet attacks, see Katz (2014).

Home Appliance "Botnet"

The Internet of Things (IoT) can also be hacked. Since participating home appliances have a connection to the Internet, they can become computers that can be hacked and controlled. The first home attack, which involved television sets and at least one refrigerator, occurred between December 2013 and January 2014, and was referred to as "the first home appliance 'botnet' and the first cyberattack from the Internet of Things." Hackers broke into more than 100,000 home appliances and used them to send over 750,000 malicious e-mails to enterprises and individuals worldwide (see Bort 2014; Kaiser 2014).

Malvertising

According to Techopedia, *malvertising* is "a malicious form of Internet advertising used to spread malware." Malvertising is accomplished by hiding malicious code within relatively safe online advertisements (see **techopedia.com/definition/4016/malvertising**).

Note that hackers are targeting ads at accelerating rates. For example, in 2013, Google disabled ads from over 400,000 sites that were hiding malware (see Yadron 2014). A final word: If you get an e-mail that congratulates you on winning a large amount of money and asks you to "Please view the attachment," don't!

SECTION 10.3 REVIEW QUESTIONS

1. Describe the difference between a nontechnical and a technical cyber attack.
2. What are the major forms of malicious code?
3. What factors account for the increase in malicious code?
4. Define a virus and explain how it works.
5. Define worm and Trojan horse.
6. Define DoS. How are DoS attacks perpetrated?
7. Define server and page hijacking.
8. Describe botnet attacks.

10.4 NONTECHNICAL METHODS: FROM PHISHING TO SPAM AND FRAUD

As discussed in Section 10.1, there has been a shift to profit-related Internet crimes. These crimes are conducted with the help of both technical methods, such as malicious code that can access confidential information that may be used to steal money from your online bank account, and nontechnical methods, such as social engineering.

Social Engineering and Fraud

As stated earlier, *social engineering* refers to a collection of methods where criminals use human psychology to persuade or manipulate people into revealing their confidential information so they can collect information for illegal activities. The hacker may also attempt to get access to the user's computer in order to install malicious software that will give them control over the person's computer. The major social engineering attacks are: phishing (several submethods; typically, a phisher sends an e-mail that appears to come from a legitimate source), pretexting (e.g., an e-mail allegedly sent from a friend asking for money), and diversion theft (when a social engineer convinces a courier company that he is the real recipient of the package but it should be "rerouted" to another address, whereupon the social engineer accepts the package). Once information is obtained from a victim (e.g., via phishing), it is used for committing crimes, mostly for financial gain, as shown in Figure 10.5. The growth rate of unpatched vulnerabilities and the volume of e-mail scam/phishing activities are increasing rapidly.

As you can see in the figure, phishers (or other criminals) obtain confidential information by using methods ranging from social engineering to physical theft. The stolen information (e.g., credit card numbers, users' identity) is used by the thieves to commit fraud for financial gain, or it is sold in the underground Internet marketplace to another set of criminals, who then use the information to conduct financial crimes themselves. For details see Goodchild (2012). In this section, we will describe how phishing, which is a subset of social engineering, is used.

Social Phishing

In the field of computer security, **phishing** is a fraudulent process of acquiring confidential information, such as credit card or banking details, from unsuspecting computer users. According to Teller (2012), "a phisher sends an e-mail, IM, comment, or text message that appears to come from a legitimate, popular company, bank, school, or institution." Once the user enters the corrupted website, he or she may be tricked into submitting confidential information (e.g., being asked to "update" information). Sometimes phishers install malware to facilitate the extraction of information. For an interesting novel that "cries out an alarm about cyber security," read

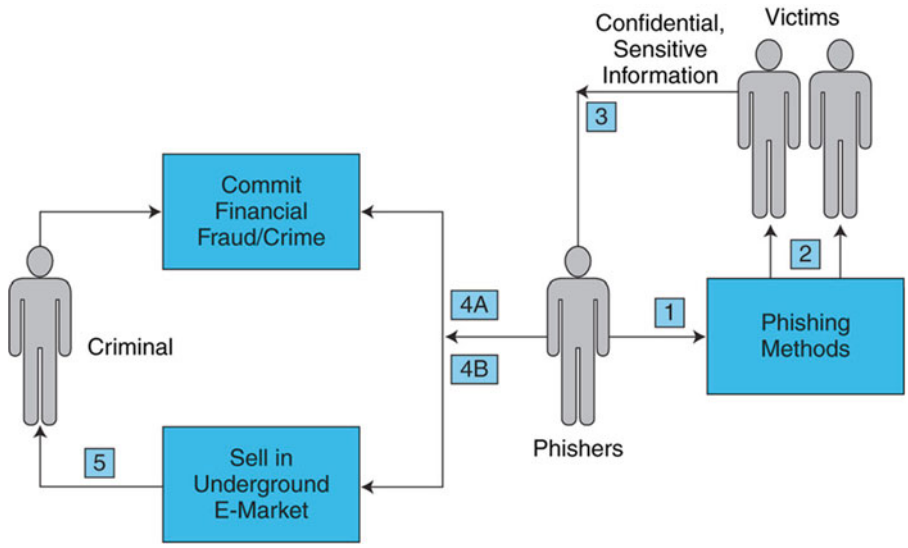

Figure 10.5 Social engineering: from phishing to financial fraud and crime

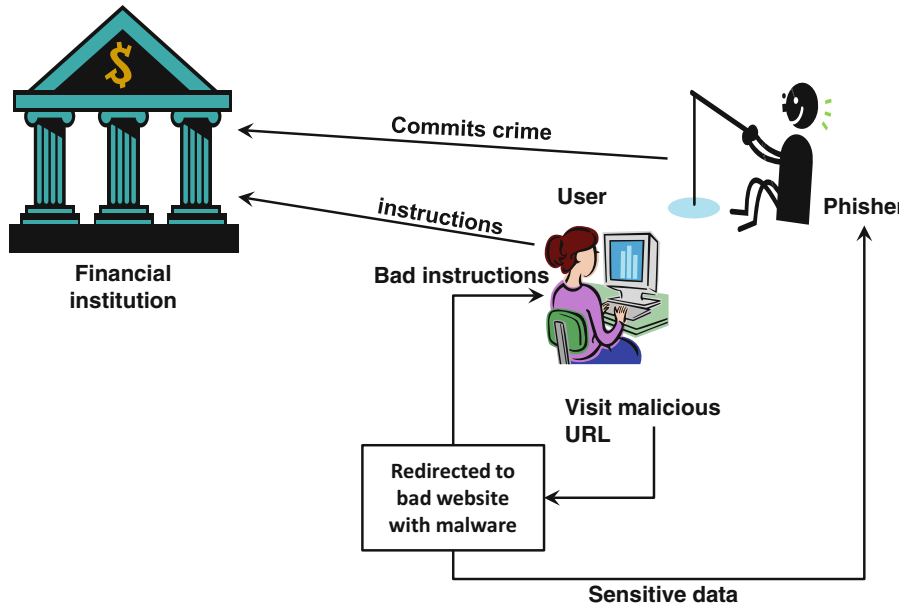

Figure 10.6 How phishing is accomplished

"*Marlins Cry A Phishing Story*" by Swann (2012). The process of Web-based phishing is illustrated in Figure 10.6.

For a discussion of what phishing is and how to recognize it, see **ehow.com/how_7350964_recognize-phishing.html**. EMC/RSA (2014) provides a comprehensive coverage of phishing with statistics and forecasts. Casti (2014a) describes a phishing scam on Netflix where users were tricked into contacting phony customer service representatives and handing over personal account data. Scammers have now targeted other

companies, such as AT&T and Comcast, by drawing users to fake websites via phony sponsored ads (Casti 2014b).

Selling stolen information, like selling any stolen goods, can be profitable and unstoppable. Unfortunately, potential e-commerce customers list "the potential risk of fraud," and "the mistrust of online merchants that you do not know" as their primary reasons for not shopping online.

Notes that as companies try to expand their e-businesses in countries where the legal systems are underdeveloped, opportunities for fraud expand, making it difficult to conduct EC.

There are several different kinds of phishing. *Spear phishing* is when attackers target specific individuals by gaining personal data about them through information they share on the Internet, such as on social networks. Spear phishing is more dangerous than regular phishing because the e-mails are targeting specific people or organizations, rather than to millions of unknown recipients.

Example: The Target Security Breach

The Target Corp. 2013 security breach, where millions of customers had their debit and credit card data stolen, started as a phishing attack (see Schwartz 2014). Hackers used the credentials of an employee of one of Target's vendors to gain access to Target's security system and install malware for the purpose of accessing the data of every card used. A Target employee would swipe the customer's card and the installed malware would "capture the shopper's credit card number, and store it on a server commandeered by the hackers" (see Riley et al. 2014). Once the hackers gained access to the data, they were able to steal 40 million credit and debit card numbers – and 70 million addresses, phone numbers, and other pieces of personal information. To see an infographic of how the hackers broke in, and how Target could have prevented the hack, see Smith (2014).

For an overview of phishing, its process, techniques, and the damage it can cause, see Mandalia (2011), and the *Symantec Monthly Intelligence Report* at **symantec.com**.

Pharming

Similarly to phishing, **pharming** is a scam where malicious code is installed on a computer and used to redirect victims to a bogus websites without their knowledge or consent. Pharming can be more dangerous than phishing since users have no idea that they are have been redirected to a fake website. Pharming is directed towards large groups of people at one time via *domain spoofing*. Pharming can be used for identity theft scams (discussed later in this section). For details, see Pattison (2012) and **en.wikipedia.org/wiki/Pharming**.

Fraud and Scams on the Internet

Phishing is the first step that leads to many fraud schemes. The EC environment where buyers and sellers cannot see each other facilitates fraud. There are many types of fraud on the Internet (see CyberSource 2012 and **fbi.gov/scams-safety/fraud/internet_fraud**). Fraud is a problem for online retailers and customers alike. Fortunately, even though actual losses per incident increase, there are fewer incidents; and thus the total monetary damage may be declining. Note that online merchants reject roughly 4% of submitted credit card-based shopping orders because of suspicion of fraud. Yet, only an estimated 1% of accepted online orders turn out to be fraudulent.

Internet fraud has grown very rapidly since 2005. The following examples demonstrate the scope of the problem. In addition, visit **dmoz.org/Society/Issues/Fraud/Internet** for a comprehensive collection of fraud resources.

Examples of Typical Online Fraud Attacks

The following are some characteristic fraud attacks perpetrated on the Internet.

- In March 2011, Google removed over 50 apps from its Android marketplace due to malware infections. Users who downloaded the infected apps, which contained

malware called "DroidDream" may have had their data compromised. The infected apps included Spider Man, Photo Editor, and other popular apps. Luckily, Google was quickly able to remove the infected apps from the market.

- When one of the authors of this book advertised online that he had a house to rent, several "doctors" and "nurses" pretending to be from the United Kingdom and South America applied. They agreed to pay a premium price for a short-term lease and said they would pay with a cashier's check. They asked if the author would accept a check from $6,000 to $10,000 and send them back the balance of $4,000 to $8,000. When advised that this would be fine, but that the difference would be returned only after their check had cleared, none of the would-be renters followed up.
- Extortion rings in the United Kingdom and Russia have extorted hundreds of thousands of dollars from online sports betting websites. Any site refusing to pay "protection fees" has been threatened with DoS attacks.

For a video titled "How Hackers Can Invade Your Home" (2:26 minutes) showing how hackers can invade your home, see **money.cnn.com/video/technology/2013/08/14/t-hack-my-baby-monitor-and-house.cnnmoney**. For a comprehensive discussion of fraud, see CyberSource (2013).

More examples of Internet fraud and typical scams are provided by Pattison (2012) and in **voices.washingtonpost.com/securityfix/web_fraud_20**. For a discussion on social engineering, phishing, and other methods of fraudulently obtaining confidential information online, see Pontrioli (2013).

Types of Scams

The following are some representative types of current scams (per Spamlaws see **spamlaws.com/scams.html**): Literary scams, jury duty scams, banking scams, e-mail scams, lottery scams, Nigerian scams (or "419" fraud), credit cards scams (several types), work at/from home scams, IRS e-mail scams, and free vacation scams. Many more can be found at fbi.gov (see **fbi.gov/scams-safety/fraud/internet_fraud**).

E-Mail Scams

E-mail scams are the most popular type of scam since they are so easy to commit. Dog Breed Info Center (**dogbreedinfo.com**; undated) posts common examples at (**dogbreedinfo.com/internet-fraud/scamemailexamples.htm**). The examples are both educational and entertaining. The most dangerous are e-mails scams that look like they come from well-known organizations (banks, telecommunication companies) that tell you that you must provide information in order to keep your account active. An example of an e-mail purportedly sent by Yahoo! is provided below.

Yahoo Account
Verification Alert!!!
(KMM69467VL55834KM)
Dear Valued Member,
Due to the congestion in all Yahoo Accounts, Yahoo would be shutting down all unused Accounts. You will have to confirm your E-mail by filling out your Login Information below after clicking the reply button, or your account will be suspended within 24 hours for security reasons.

Yahoo! ID Card
Name: . . . . . .
Yahoo! ID: . . . . . .
Yahoo! Mail Address: . . . . . .
Password: . . . . . .
Member Information
Gender: . . . . . .
Birth Date: . . . . . .
Occupation: . . . . . .
Country: . . . . . .

If you are a Yahoo! Account Premium subscriber, we will refund the unused por-

tion of your Premium subscription. The refund will appear as a credit via the billing method we have on file for you. So please make sure that your billing information is correct and up-to-date. For more information, please visit billing.yahoo. com.

After following the instruction on this sheet your account will not be interrupted and will continue as normal.

We appreciate your being a Yahoo! Account user.

Sincerely,

Yahoo! Customer Support

Any e-mail you receive asking for personal details is most likely a scam or phishing attempt since a legitimate organization will already have all your personal information. For tips from Yahoo! on how to protect yourself online, see Yahoo! Safely (**safely.yahoo.com/safety-tips**).

Everyone can be a victim of e-mail scams, as shown in Case 10.1.

CASE 10.1: ANYONE CAN BE A VICTIM (FROM STUDENTS TO LAWYERS TO TEXTBOOK AUTHORS)

How a scammer attacked an author of this book:

Example

The "Stranded Traveler" scam is still going strong. How it works: An individual receives an e-mail purportedly sent from a real friend that goes something like this (these come in variations of countries, amounts of currency needed, etc.):

> I'm writing this e-mail with tears in my eyes, I came down to London for a program unfortunately, I was mugged at the park of the hotel where I stayed, all cash, credit, and cell were stolen off me but luckily for me I still have my passport with me, I have no access to my account. I have been to the embassy and the police here but they are not helping issue at all and my flight leaves tomorrow night but I am having problems settling the hotel bills and the hotel manager won't let me leave until I settle the bills. I'm freaked out at the moment. I need about £2,250 or any amount you can lend me to sort-out the bills, I will repay you as soon as I get back home.

How it happened: Hackers hacked into your e-mail accounts, finding who your contacts are and their e-mail addresses. They then sent out an e-mail to you from people on the list.

Alternatively, hackers get into your friend's e-mail account and find that you are one of their contacts. Then they send you the request for help.

LESSONS LEARNED FROM THE CASE

1. In general, make sure you log off of your e-mail account when you are away from home. Change your password often, especially after travelling, and have a complex password.
2. Have an additional (secondary) password to communicate with e-mail servers (e.g., Yahoo! Gmail) to advise them of the security breach.
3. Remember, many scammers are smart and experienced. Read examples given by the Dog Breed Info Center and the FTC.

Questions

1. Find information on the different methods scammers can use to hijack e-mail account and what a possible defense may be.
2. What is the process used by the scammer?
3. It looks as if this attack method is very popular. Why it is used so frequently, and why are so many e-mail accounts being hijacked?

Top 10 Attacks and Remedies

IT security site Secpoint.com provides a list of the top 10 security-related attacks on the following topics: Top viruses, spyware, spam, worms, phishing, hacker attacks, and hackers and social engineering tactics. In addition, the site provides related pages on IT security resources such as the top 10 top hackers; top 10 security tips and tools; pages relating to Anti phishing, Anti DOS, Anti spam, and more. For SecPoint IT resources for top 10 spam attacks, see **secpoint.com/Top-10-Spam-Attacks.html**.

Identity Theft and Identify Fraud

Identity theft, according to the United States Department of Justice website, is a crime. It refers to wrongfully obtaining and using the identity of another person in some way to commit crimes that involve fraud or deception (e.g., for economic gain). Victims can suffer serious damages. In many countries, it is a crime to assume another person's identity. According to the U.S. Federal Trade Commission (**ftc.gov**), identity theft is one of the major concerns of EC shoppers. According to the FTC statistics, identity theft affects over 12 million Americans each year, for a loss of over $55 billion, and is growing about 20% annually. For an entertaining comedy, see the 2013 movie "Identity Thief."

Identity Fraud

Identity fraud refers to assuming the identity of another person or creating a fictitious person and then unlawfully using that identity to commit a crime. Typical activities include:

- Opening a credit card account in the victim's name
- Making a purchase using a false identity (e.g., using another's identity to buy goods)
- Business identity theft is using another's business name to obtain credit or to get into a partnership
- Posing as another to commit a crime
- Conducting money laundering (e.g., organized crime) using a fake identity

For additional information, see Nuerm (2012). For information and protection, see **idtheftcenter.org** and **fdic.gov/consumers/theft**.

Cyber Bank Robberies

Cyberattacks can happen to individuals and organizations, including banks.

Example

According to Perez (2010), a global computer gang stole about $70 million (possibly up to $220 million) from bank accounts of businesses, municipalities, and churches, mostly in the U.S. In October 2010, over 100 people in four countries were detained or charged. According to the FBI, the hacking ring included computer-code writers who were located in the Ukraine. A network of "mules" (people recruited to move stolen funds via bank accounts opened with fake names) were located in several countries.

The thieves used different versions of Zeus malware, a popular tool of cyber bank robbers (a variant Trojan horse). The thieves concentrated on small and medium businesses, because those usually have technologically limited computer security systems.

In 2011, criminals combined old-fashioned "con artistry" with "newfangled technology" to rob banks in London. Two cases where the thieves entered the bank posing as IT technicians are reported by Nugent (2013).

In addition to stealing bank accounts, criminals commit check fraud as well.

Example

Secureworks.com uncovered the following check fraud operations (per Prince 2010b): Russian cybercriminals used "money mules" (people who thought they were signing up for a legitimate job), 2,000 computers, and sophisticated hacking methods to steal archived check images from five companies, and wire the collected money overseas.

Next, the scammers printed counterfeit checks, which the money mules deposited in their own accounts. Then, the mules were ordered to wire (transfer) the money to a bank in Russia. The "mules," as usual, were innocent people who were hired and paid to do the transfer. Some of the mules became suspicious and reported the scam to the authorities.

Spam Attacks

E-mail spam, also known as *junk e-mail* or just *spam,* occurs when almost identical messages are e-mailed to many recipients in bulk (sometimes millions of unsolicited e-mails). According to Symantec (as reported by McMillan 2009), in April 2009, over 90% of messages on corporate networks were e-mail spam. Nearly 58% of spam came from botnets, the worst called *Dotnet*. The situation is better today (2014) due to improved filtering of junk mail. Spammers can purchase

millions of e-mail addresses, and then using a program such as MS Word, format the addresses, cut and paste the messages and press "send." Mass e-mail software that generates, sends, and automates spam e-mail sending is called *Ratware*. The messages can be advertisements (to buy a product), fraud-based, or just annoying viruses. For current statistics on spam, see **securelist.com/en/analysis/spam?topic=199380272**. Securelist is a comprehensive site that also provides descriptions of spam and viruses, a glossary, and information on threats. See Gudkova (2013) for the evolution of spam in 2013. Spam annoys e-mail users and therefore legislators are attempting to control it (see discussion of the CAN-Spam Act in Chapter 15). More than 130 billion spam e-mails are sent each day as of 2013, but this growth rate has stabilized. Note that approximately 80% of all spam is sent by fewer than 200 spammers. These spammers are using spyware and other tools mostly for sending unsolicited advertising. The spammers are getting more and more sophisticated. (e.g., see Kaiser 2014).

An example of how spam is used for stock market fraud is provided in Case 10.2.

CASE 10.2: INTERNET STOCK FRAUD AIDED BY SPAM

A study reported by Lerer (2007) concluded that stock market spam could influence stock prices. The results show that on average, the investors influenced by the spam lost about 5.5%, while the spammers made a 5.79% return. Spammers send out a massive amount of e-mails telling the recipients that a certain stock is "too good to miss," and if many people are influenced into buying it, the shares rise and the spammers can sell at a big profit.

In March 2007, the federal government cracked down on dozens of such stock sites. The success of *Operation Spamalot*, conducted by the Securities and Exchange Commission (SEC), helped, but did not eliminate this kind of fraud. By 2014, the practice spread all over the Internet (see Gandel 2014).

There are two reasons that such spam will not go away: It *works* and it is *profitable*. However, unlucky spammers may end up in jail. For example, Ralsky and Bradley advertised Chinese penny stocks via e-mail and then, when the demand drove the share price up, sold them at a profit. Both people, together with their accomplices, were sentenced to several years in prison.

Sources: Based on Lerer (2007) and Gandel (2014).

Questions

1. Why might people buy the penny stocks promoted in an e-mail message from an unknown source?
2. Use Google or Bing to find out what can be done to better filter spam.

Secure Computing Corporation saw a 50% increase in spam. In 2012, spam accounted for nearly 90% of all e-mail. The amount of image spam, which today accounts for 30% of all spam, tripled between 2010 and 2011. According to Gudkova (2013), the percentage of spam sent in 2013 was 73.26, while the percentage of spam in Q 1 of 2014 was approximately 66%.

Typical Examples of Spamming

Each month Symantec provides a report titled "The State of Spam: A Monthly Report." The report provides examples of current popular scams, categories of spam, originating countries, volume, and much more.

Spyware

Spyware is tracking software that is installed by criminals or advertisers, without the user's consent, in order to gather information about the user and direct it to advertisers or other third parties. Once installed the spyware program tracks and records the user's movements on the Internet. Spyware may contain malicious code redirecting Web browser activity. Spyware can also slow surfing speeds and damage a program's functionality. Spyware usually is installed when you download freeware or shareware. For more on

spyware, see Harkins (2011) and Gil (2013). For news and a video titled "Ethiopian Government Spying on U.S.-Based Journalists" (2:23 minutes) of how some regimes use spyware against journalists, see Timberg (2014).

Social Networking Makes Social Engineering Easy

Social networking sites are a vulnerable and fertile area for hackers and con artists to gain a user's trust, according to a study by Danish-owned IT security company CSIS.

The CSIS Security Group Research (csis.dk)

Dennis Rand, a security and malware researcher at CSIS designed the following experiment:

1. Under the fake name of John Smith, he created a profile on LinkedIn.com.
2. He selected thousands of people at random, inviting them to join his network.
3. He targeted several companies and posed on their enterprise social network as an ex-employee.
4. Many existing employees of these companies, who were included in the randomly selected sample, accepted the invitation, creating a network of over a thousand trusted members for Rand.
5. Rand communicated with the members, thus collecting their e-mail addresses. He harvested confidential data from some of the members. He also sent links (e.g., recommendations for videos), and some were clicked on by the receivers.

The objective of the experiment was to study the potential security risks in using social networks. For example, messages may include links to malware and these attachments may be opened since they come from trusted friends. Some networks do not even encourage users to select strong passwords and to change them periodically. At the end of the experiment, Rand sent an e-mail to all participating members, explaining the purpose of the experiment. Then he closed the "John Smith" network. See Rand (2007).

How Hackers Are Attacking Social Networks

Hackers are exploiting the trusted environment of social networks that contain personal information (especially Facebook) to launch different social engineering attacks. Unfortunately, many social network sites have poor track records for security controls. There is a growing trend to use social networking sites as platforms for stealing users' personal data.

Examples

Here are some examples of security problems in social networking:

- Users may unknowingly insert malicious code into their profile page, or even their list of friends.
- Most anti-spam solutions cannot differentiate between real and criminal requests to connect to a network. This enables criminals to obtain personal information about the members in a network.
- Facebook and other popular social networking sites offer free, useful, attractive applications. These applications may have been built by developers who used weak security.
- Scammers may create a fake profile and use it in a phishing scam.

Spam in Social Networks and in the Web 2.0 Environment

Social networks attract spammers due to the large number of potential recipients and the less secure Internet and social network platforms. Spammers like to attack Facebook in particular. Another problem area is blog spam.

Automated Blog Spam

Bloggers are spammed by automatically generated commercials (some real and some fake) for items ranging from herbal Viagra to gambling vendors. Blog writers can use tools to ensure that a human, and not an automated system, posts comments on their blogs.

Search Engine Spam and Splogs

Search engine spam, is technology that enables the creation of pages called **spam sites** that trick search engines into offering biased search results so that the ranking of certain pages is inflated. A similar tactic involves the use of **splogs** (short for *spam blog sites*), which are blogs created by spammers solely for advertising. The spammer creates many splogs and links them to the sites of those that pay him (her) to increase certain page ranking. As you may recall from Chapter 9, companies are looking for search engine optimization (SEO), which is conducted unethically by the above techniques.

Sploggers assume that some Web surfers who land on their site will click on one or more linked advertisements. Each of these clicks earns a few cents for the splogger, and because any one splogger can create millions of splogs, this kind of spam can be very profitable.

Examples

Some examples of spam attacks in social networks (social spam) are:

- In January 2009, Twitter became a target for a hacker who hijacked the accounts of 33 high-profile users (including President Obama), sending out fake messages.
- Instant messaging in social networks is frequently vulnerable to spam attacks.
- Cluley (2014) describes how Twitter users are attacked by phishing attacks and spammers.

Data Breach (Leak)

A **data breach** (also known as *data leak* or *data loss*) is a security incident in which data are obtained illegally and then published or processed. For an overview, see Thomson (2012). There are many purposes for data breaches. Data leaks received considerable publicity between 2010 and 2012. For instance, one person in the U.S. military used a USB to download classified information and then posted the stolen information on the Internet. For drivers of data breaches and how to protect yourself, see Goldman (2014) and Section 10.7.

The discussion so far has concentrated on attacks. Defense mechanisms, including those related to spam and other cybercrimes, are provided in Sections 10.6, 10.7, 10.8, and 10.9. First, let us examine what is involved in assuring information security.

SECTION 10.4 REVIEW QUESTIONS

1. Define phishing.
2. Describe the relationship of phishing to financial fraud.
3. Briefly describe some phishing tactics.
4. Define pharming.
5. Describe spam and its methods.
6. Define splogs and explain how sploggers make money.
7. Why and how are social networks being attacked?
8. Describe data breaches (data leaks).

10.5 THE INFORMATION ASSURANCE MODEL AND DEFENSE STRATEGY

The *Information Assurance (IA) model,* known as the **CIA security triad**, is a point of reference used to identify problem areas and evaluate the information security of an organization. The use of the model includes three necessary attributes: *confidentiality*, *integrity*, and *availability.* This model is described next. (For a discussion, see **whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA**.)

Note. The assurance model can be adapted to several EC applications. For example, securing the supply chain is critical.

Confidentiality, Integrity, and Availability

The success and security of EC can be measured by these attributes:

1. **Confidentiality** is the assurance of data secrecy and privacy. Namely, the data is disclosed only to authorized people. Confidentiality is achieved by using several methods, such as encryption and passwords, which are described in Sections 10.6, 10.7, 10.8, and 10.9.
2. **Integrity** is the assurance that data are accurate and that they cannot be altered. The integrity attribute needs to be able to detect and prevent the unauthorized creation, modification, or deletion of data or messages in transit.
3. **Availability** is the assurance that access to any relevant data, information websites, or other EC services and their use is available in real time, whenever and wherever needed. The information must be reliable.

Authentication, Authorization, and Nonrepudiation

Three concepts are related to the IA model: *authentication, authorization*, and *nonrepudiation.* These important concepts are:

- *Authentication* is a security measure making sure that data information, ECD participants and transactions, and all other EC related objects, are valid. *Authentication* requires verification. For example, a person can be authenticated by something he knows (e.g., a password), something he possesses (e.g., an entry token), or something unique to that person (e.g., a fingerprint).
- *Authorization* requires comparing information provided by a person or a program during a login with stored information associated with the access requested.
- *Nonrepudiation* is the concept of ensuring that a party in an EC transaction cannot repudiate (or refute) the validity of an EC contract and that she or he will fulfill their obligation in the transactions. According to the National Information Systems Security (INFOSEC)'s glossary, Nonrepudiation is the "[a]ssurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so that neither can later deny having processed the data."

Note: See the list of Key Terms in Section 10.2. Some sources list more concepts (e.g., Techopedia).

To assure these attributes, e-commerce applies technologies such as encryption, digital signature, and certification (Section 10.6). For example, the use of a *digital signature* makes it difficult for people to deny their involvement in an EC transaction.

In e-commerce, new or improved methods to ensure the confidentiality of credit card numbers, the integrity of transaction-related messages, the authentication of buyers and sellers, and nonrepudiation of transactions need to be constantly updated as older methods become obsolete.

E-Commerce Security Strategy

EC security needs to address the IA model and its components. In Figure 10.7, an EC security framework that defines the high-level categories of assurance and their controls is presented. The major categories are regulatory, financial, and marketing operations. Only the key areas are listed in the figure.

The Phases of Security Defense

The security defense process includes the following phases:

1. **Prevention and deterrence (preparation)**. Good controls may prevent criminal activities as well as human error from occurring.

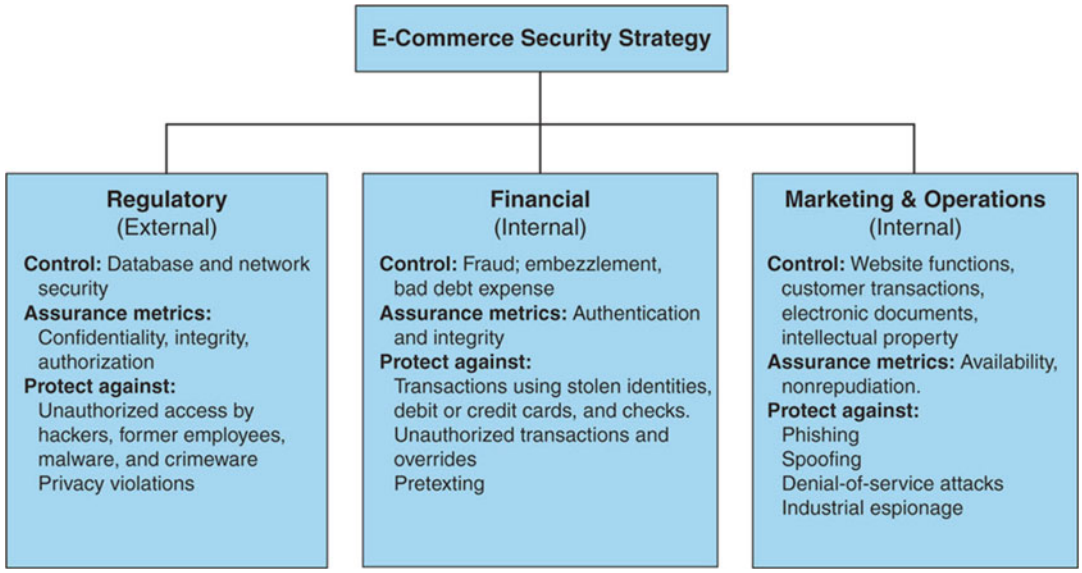

Figure 10.7 E-commerce security strategy framework

Controls can also deter criminals from attacking computerized systems and deny access to unauthorized human intruders. Also, necessary tools need to be acquired.

2. **Initial Response**. The first thing to do is to verify if there is an attack. If so, determine how the intruder gained access to the system and which systems and data are infected or corrupted.
3. **Detection.** The earlier an attack is detected, the easier it is to fix the problem, and the smaller amount of damage is done. Detection can be executed by using inexpensive or free intrusion detecting software.
4. **Containment (contain the damage).** This objective is to minimize or limit losses once a malfunction has occurred. It is also called *damage control*. Damage control can be done, for example, by using *fault-tolerant* hardware and software that enable operation in a satisfactory, but not optimal, mode until full recovery is made.
5. **Eradication.** Remove the malware from infected hosts.
6. **Recovery.** Recovery needs to be planned for to assure quick return to normal operations at a reasonable cost. One option is to replace parts rather than to repair them. Functionality of data should also be restored.
7. **Correction.** Finding the causes of damaged systems and fixing them will prevent future occurrences.
8. **Awareness and compliance.** All organization members must be educated about possible hazards and must comply with the security rules and regulations.

Security Spending Versus Needs Gap

A major concern in information security management is how to match the security defense efforts (money, labor, time) against the major security threats. This is a difficult task since the EC threat landscape is constantly changing. Therefore, in any defense strategy one should explore the following issues (examples of each are available in Chickowski 2008):

1. What are the most critical current data security issues?
2. Where are the greatest risks of exposure?
3. Where do you spend the money? How is spending matched with risk exposure?

4. What are the benefits (including intangible) that you can derive from money spent on security project tools?
5. What are the losses due to security incidents (in your organization and in general)?
6. What are the major security technologies that reduce security losses (e.g., firewall, encryption, and antiviruses are usually at the top)?
7. What guidelines will be used for the upcoming security budget?

The Defense Side EC Systems

We organize the defense into seven categories:

1. **Defending access to computing systems, data flow, and EC transactions.** In Section 10.6, we present three topics: Access control (including biometrics), encryption of contents, and public key infrastructure (PKI).

   This line of defense provides comprehensive protection when applied together. Intruders that circumvent the access control will face encrypted material even if they pass a firewall.
2. **Defending EC networks.** In Section 10.7, we recognize the protection provided by firewalls. The firewall isolates the corporate network and computing devices from the Internet that are poorly secured. To make the Internet more secure, we can use virtual private networks. In addition to these measures, it is wise to use intrusion-detecting systems. A protected network means securing the incoming e-mail, which is usually unencrypted. It is also necessary to protect against viruses and other malware that are transmitted via the networks.
3. **General, administrative, and application controls.** These are a variety of safeguards that are intended to protect computing assets by establishing guidelines, checking procedures, and so forth. They are discussed in Section 10.8.
4. **Protection against social engineering and fraud.** In Section 10.8, we describe defense methods against spam, phishing, and spyware.
5. **Disaster preparation, business continuity, and risk management.** These topics are managerial issues that are supported by software and described in Section 10.9.
6. **Implementing enterprisewide security programs.** To deploy the previously mentioned defense methods, one needs to use appropriate implementation strategy, as described in Section 10.9.
7. **Conduct a vulnerability assessment and a penetration test.** (See the following text.)

For a comprehensive coverage of all aspects of information protection, see Rhodes-Ousley (2013).

To implement the above defense, first conduct some assessment and then plan and execute. Two possible activities are *vulnerability assessments* and *penetration tests*. For the concepts of information systems security fundamentals as applied to an IT infrastructure, see Jones and Bartlett Learning LLC (2012).

Assessing Vulnerabilities and Security Needs

A key task in security strategy is to find the weaknesses and strengths of the existing security strategies and solutions. This is part of a risk assessment and can be accomplished in different ways. Here are two representative suggestions:

1. Conduct a vulnerability assessment of your EC systems. A **vulnerability assessment** is a process of identifying and evaluating problem areas that are vulnerable to attack on a computerized system. The assessment can also predict the potential effectiveness of implemented countermeasures and evaluate their effectiveness after they are applied. The EC system includes online ordering,

communication networks, payment gates, product database, fraud protection, and so forth. The most critical vulnerabilities are those that can interrupt or shut down the business. For example, a DoS can prevent order taking; a virus attack can prevent communication. The assessment will determine the need for, and priority of, the defense mechanisms. For an overview of vulnerability assessment including the process, see **searchmidmarket-security.techtarget.com/definition/vulnerability-analysis**. For a method of conducting Web vulnerability analysis at a reasonable cost, see Symantec (2011).

2. Conduct *penetration (pen) tests* (possibly implemented by hiring ex-hackers) to find the vulnerabilities and security weaknesses of a system. These tests are designed to simulate outside (external) attacks. This is also called "black-box" testing. In contrast, software development companies conduct intensive "white-hat" testing, which involves a careful inspection of the system – both hardware and software. Other types of pen testing include targeted texting, blind testing, and double blind testing.

For more information, see Talabis and Martin (2013) and **searchsoftwarequality.techtarget.com/definition/penetration-testing**.

Penetration Test

A **penetration test (pen test)** is a method of assessing the vulnerability of a computer system. It can be done manually, by allowing experts to act as hackers to simulate malicious attacks. The process checks the weak (vulnerable) points that an attacker may find and exploit. Any weakness that is discovered is presented to management, together with the potential impact and a proposed solution. A pen test can be one step in a comprehensive security audit.

Several methods can be used to execute pen tests (e.g., automated process). In addition, many software tools are available for this purpose. For a review and a tutorial, see **pen-tests.com** and **coresecurity.com/penetration-testing-overview**.

SECTION 10.5 REVIEW QUESTIONS

1. What is Information Assurance? List its major components.
2. Define confidentiality, integrity, and availability.
3. Define authentication, authorization, and nonrepudiation.
4. List the objectives of EC strategy.
5. List the seven categories of defense in EC systems.
6. Describe vulnerability assessment.
7. What is a penetration test?

10.6 THE DEFENSE I: ACCESS CONTROL, ENCRYPTION, AND PKI

In this section, we describe several popular methods that deal with protection of EC information assets inside organizations, from both outside and inside attacks. For new malware mitigation tools and techniques, see Snyder (2014), who also discusses firewalls, sandboxing, and reputation services.

Access Control

Access control determines who (person, program, or machine) can legitimately use the organization's computing resources (which resources, when, and how). A resource refers to hardware, software, Web pages, text files, databases, applications, servers, printers, or any other information source or network component. Typically, access control defines the rights that specific users with access may have with respect to those resources (i.e., read, view, write, print, copy, delete, execute, modify, or move).

Authorization and Authentication

Access control involves *authorization* (having the right to access) and *authentication*, which is also called *user identification* (user ID), i.e., proving that the user is who he or she claims to be. Each user has a distinctive identification that differentiates it from other users. Typically, user identification is used together with a password.

Authentication

After a user has been *identified*, the user must be *authenticated. Authentication* is the process of verifying the user's identity and access rights. Verification of the user's identity usually is based on one or more characteristics that distinguish one individual from another.

Traditionally, authentication has been based only on passwords. Passwords by themselves may be ineffective because people have a habit of writing them down and putting them where they can be easily found, choosing values that are guessed easily (e.g. "password"), and sharing their passwords with others.

Two-Factor Authentication

This type of authentication system is a security process that requires two different types of identification (more than just your password). For example, one mechanism is physical (something a person *has*), such as a token card, and the other is something that a person *knows* (usually a password or an answer to a security question, or a combination of variations of both). Companies use RSA's Security ID to manage systems that require high security. However, in 2011 hackers breached the RSA code. Therefore, companies must enforce password discipline, which will protect the system even when the RSA code is hacked.

Biometric Systems

A **biometric authentication** is a technology that measures and analyzes the identity of people based on measurable biological or behavioral characteristics or physiological signals.

Biometric systems can *identify* a previously registered person by searching through a database for a possible *match* based on the person's observed physical, biological, or behavioral traits, or the system can *verify* a person's identity by matching an individual's measured biometric traits against a previously stored version.

Examples of biometric features include fingerprints, facial recognition, DNA, palm print, hand geometry, iris recognition, and even odor/scent. Behavioral traits include voice ID, typing rhythm (keystroke dynamics), and signature verification. A brief description of some of these follows:

- **Thumbprint or fingerprint.** A thumb- or fingerprint (finger scan) of users requesting access is matched against a template containing the fingerprints of authorized people.
- **Retinal scan.** A match is sought between the patterns of the blood vessels in the retina of the access seekers against the retinal images of authorized people stored in a source database.
- **Voice ID (voice authentication).** A match is sought between the voice pattern of the access seekers and the stored voice patterns of the authorized people.
- **Facial recognition.** Computer software that views an image or video of a person and compares it to an image stored in a database.
- **Signature recognition.** Signatures of access seekers are matched against stored authentic signatures.

Other biometrics types are: thermal infrared face recognition, hand geometry, and hand veins. For details, comparisons with regard to human characteristics, and cost–benefit analyses, see **findbiometrics.com/solutions** and Rubens (2012).

To implement a biometric authentication system, the physiological or behavioral characteristics of a participant must be scanned repeatedly under different settings. The scans are then used to produce a biometric template, or identifier. The template is encrypted and stored in a database. When a person enters a biometric system, a live scan is conducted, and the scan is converted to the encrypted template and compared to the stored one. Biometric methods are improving, but they have not yet replaced passwords (see Duncan 2013). In addition, for stronger security you need to use encryption.

Encryption and the One-Key (Symmetric) System

Encryption is the process of encoding data into a form (called a *ciphertext*) that will be difficult, expensive, or time-consuming for an unauthorized person to understand. All encryption methods have five basic components: *plaintext, ciphertext*, an *encryption algorithm*, the *key,* and *key space.* **Plaintext** is a human-readable text or message. **Ciphertext** is an encrypted plaintext. The **encryption algorithm** is the set of procedures or mathematical algorithms used to encrypt or decrypt a message. Typically, the algorithm is not the secret piece of the encryption process. The **key (key value)** is the secret piece used with the algorithm to encrypt (or decrypt) the message. The **key space** is the total universe of possible key values that can be created by a specific encryption algorithm. Today, both encryption and trying to break the encryption codes (i.e., decrypting the messages) are done by powerful computers. However, it may be difficult to decide which data to encrypt, how best to manage encryption, and how to make the process as transparent as possible. For how encryption works, see **computer.howstuffworks.com/encryption.htm**.

According to Davis (2012a), encryption is more important today than ever, especially when cloud computing and other methods are being added to the defense system. Many databases are still unprotected, and very few companies encrypt information on company mobile devices. This is because of the attributes and benefits of encryption.

The major benefits of encryption are:

- Allows users to carry data on their laptops, mobile devices, and storage devices (e.g., USB flash drives).
- Protects backup media while people and data are offsite.
- Allows for highly secure virtual private networks (VPNs; see Section 10.7).
- Enforces policies regarding who is authorized to handle specific corporate data.
- Ensures compliance with privacy laws and government regulations, and reduces the risk of lawsuits.
- Protects the organization's reputation and secrets.

For the top 10 benefits of encryption, including how to safeguard data stored in the cloud, see Pate (2013).

Encryption has two basic options: he *symmetric system*, with one secret key, and the *asymmetric system*, with two keys.

Symmetric (Private) Key Encryption

In a **symmetric (private) key encryption**, the same key is used to encrypt and decrypt the plaintext (see Figure 10.8). The sender and receiver of the text must share the same key without revealing it to anyone else – making it a so-called *private* system. For a symmetric encryption to succeed, it needs a strong key. The strength is measured by bits used. For example, a 4-bit key will have only 16 combinations (i.e., 2 raised to the fourth power). However, a 64-bit encryption key has 2 raised to the 64th power combinations, which would take even a powerful computer years to enumerate.

A strong key is only one requirement. Transferring the key between individuals and organizations may make it insecure. Therefore, in EC, a PKI system is used.

Public Key Infrastructure

A **public key infrastructure (PKI)** is a comprehensive framework for securing data flow and information exchange that overcomes some of the shortcomings of the one-key system. For example, the symmetric one-key encryption requires the writer of a message to reveal the key to the message's recipient. A person that is sending a message (e.g., vendor) may need to distribute the key to thousands of recipients (e.g., buyers), and then the key probably would not

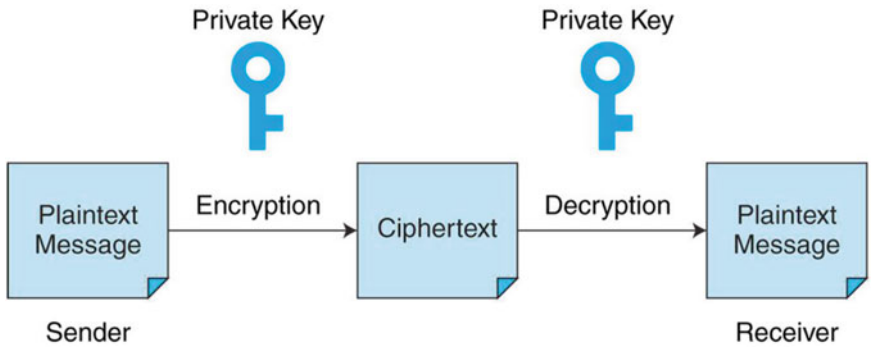

Figure 10.8 Symmetric (private) key encryption

remain secret for long unless the vendor has a different key for each buyer. If the electronic transfer of the key is intercepted, the key may be stolen or changed. The PKI solution overcomes this problem by using two keys, public and private, as well as additional features that create a highly secured system. In addition to the keys, PKI includes digital signatures, hash digests (function), and digital certificates. Let us see how the system works.

Public (Asymmetric) Key Encryption

Public (asymmetric) key encryption uses two keys – a **public key** that is known to all and a **private key** that only its owner knows. The two keys must be used together. If a message is encrypted with a public key, then only the associated private key can decrypt the message (and vice versa). If, for example, a person wants to send a purchase order to a vendor and have the contents remain private, the sender encrypts the message with the buyer's public key. When the vendor, who is the *only one able* to read the purchase order, receives the order, the vendor decrypts it with the associated private key.

The most common public key encryption algorithm is RSA (sold by RSA Security acquired by EMC Corporation; **emc.com**). The RSA algorithm uses keys ranging in length from 1,024 bits to 4,096 bits. The main problem with public key encryption is speed. Symmetrical algorithms are significantly faster than asymmetrical key algorithms. Therefore, public key encryption cannot be used effectively to encrypt and decrypt large amounts of data. In theory, a combination of symmetric and asymmetric encryption should be used to encrypt messages. Public key encryption is supplemented by *digital signatures* and *certificate authority*.

The PKI Process: Digital Signatures and Certificate Authorities

Digital signatures are the electronic equivalent of personal signatures on paper. They are difficult to forge since they authenticate the identity of the sender that uses the public key. According to the U.S. Federal Electronic Signatures in Global and National Commerce Act of 2000, digital signatures are legally treated as signatures on paper. To see how a digital signature works, go to **searchsecurity.techtarget.com/definition/digital-signature**.

Figure 10.9 illustrates how the PKI process works. Suppose a person wants to send a financial contract to a vendor (the recipient) via e-mail. The sender wants to assure the vendor that the content is secure. To do so, the sender takes the following steps:

1. The sender creates the e-mail message that includes the contract in plain language.

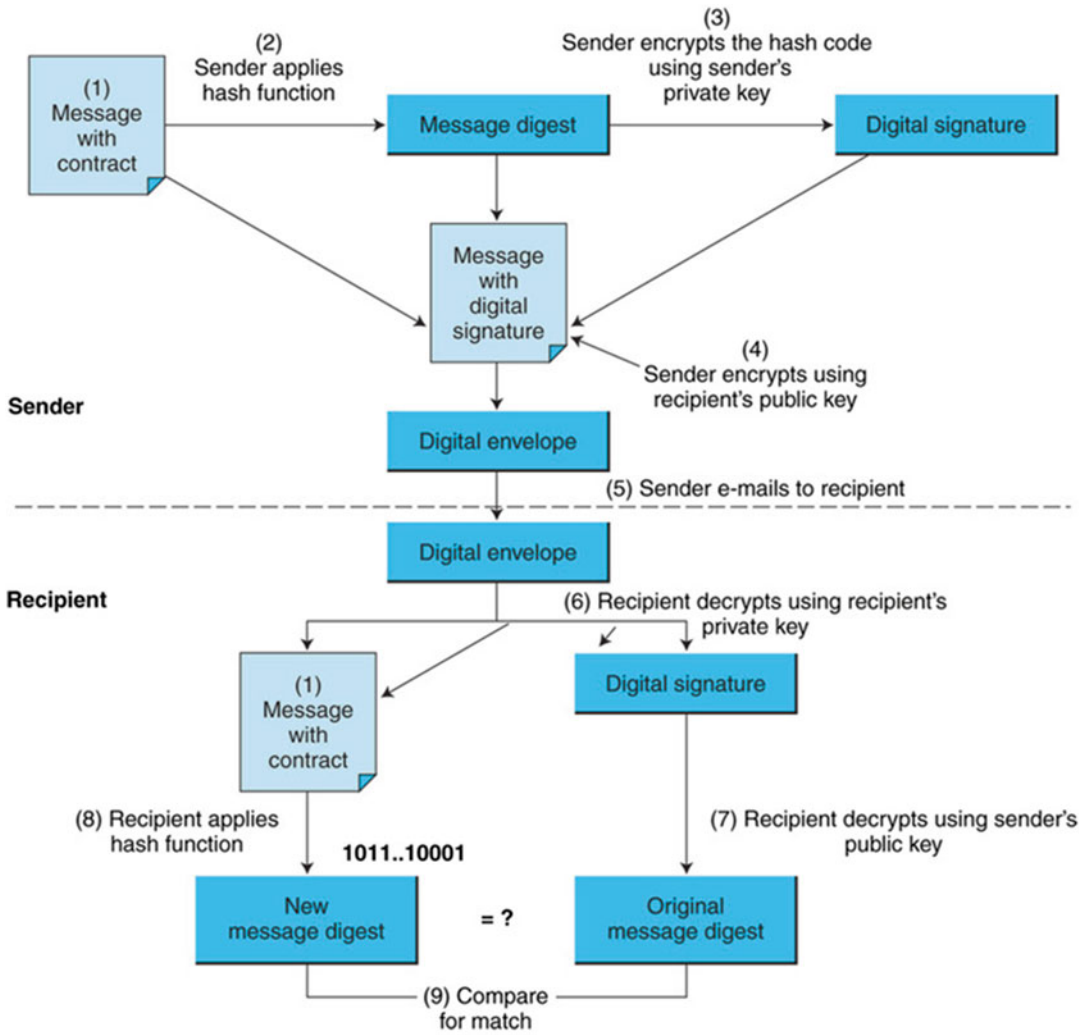

Figure 10.9 Digital signature

2. Using special software, a secured mathematical algorithm called a **hash function** is applied to the message, which results in a special summary of the message converted into a string of digits that is called a **message digest**.
3. The sender uses his or her private key to encrypt the hash. This is the sender's *digital signature*. No one else can replicate the sender's digital signature because it is based on the sender's private key, which no one else knows.
4. The sender encrypts with the recipients' public key, both the original message and the digital signature. This pair together form a **digital envelope**.
5. The sender e-mails the digital envelope to the vendor.
6. Upon receipt, the vendor uses his or her private key to decrypt the contents

of the digital envelope. This produces a copy of the message and the sender's digital signature. No one else can do it since there is only one copy of the of the vendor's private key.
7. The vendor uses the sender's public key for decrypting the content of the digital signature, resulting in a copy of the original message digest.
8. Using the same hash function employed in step 2, the vendor then creates a message digest from the decrypted message.
9. The vendor then compares this digest with the original message digest.
10. If the two digests match, then the vendor can conclude that the message is authentic.

Thus, the receiver is assured that the sender really sent the e-mail, because the sender is the only one with access to his private key. The receiver knows that the message has not been tampered with because if it had been, the two hashes would not have matched.

Certificate Authority

Independent agencies called **certificate authorities (CAs)** issue digital certificates or SSL certificates, which are electronic files that uniquely identify individuals and websites and enable encrypted communication. The certificate contains personal information and other information related to the public key and the encryption method, as well as a signed hash of the certificate data. There are different types of certificates. The major types are: *site certificates*, *personal certificates*, and *software publisher certificates*.

There are several third-party CAs. VeriSign (a Symantec company) is the most well-known of the CAs (see **verisign.com**).

Secure Socket Layer (SSL)

PKI systems are further secured with SSL – a protocol for e-commerce. The PKI with SSL make e-commerce very secure but cumbersome for users. Fortunately, Web browsers and Web servers handle many of the PKI's activities in a transparent fashion. Given that different companies, financial institutions, and governments in many countries are involved in e-commerce, it is necessary to have generally accepted protocols for securing e-commerce transactions. One of the major protocols in use today is Secure Socket Layer (SSL). SSL has been succeeded by Transport Layer Security (TLS), which is based on SSL. For further details, see **searchsecurity.techtarget.com/definition/Transport-Layer-Security-TLS**.

Other Topics and Methods of Defense

There are many other methods to combat malware and improve computer security in general.

- Use of antivirus tools. Hundreds of these are marketed by Internet security companies (e.g., Norton from Symantec and virus removing tools from Kaspersky Inc.).
- The U.S. Federal government has a website that provides information on how to avoid, detect, and eliminate malware (see **onguardonline.gov/articles/0011-malware**). The site provides a list of resources about combating spyware, spam, viruses, adware, and more. See also Wang (2013).
- Cloud-based security is advocated by many as a successful method to fight cybercriminals (e.g., Fisher 2014 and Kaplan et al. 2013). Cloud computing security includes a broad set of technologies, controls, and policies deployed to protect computer resources (see Fisher 2014).
- Integrated suites of tools. Some vendors provide an integrated set of tools in one package. This combination can be especially useful for a small company. An example is Symantec's *Endpoint Protection Small Business Edition* (**symantec.com/endpoint-protection-small-business-edition**). This integrated suite includes most of the products discussed in Sections. 10.6 and 10.7.

- Innovation. The more new methods are used by cyber criminals, the more innovative defense methods need to be developed (e.g., see Kontzer 2011).

In the next section, the focus is on the company's digital perimeters – the networks.

SECTION 10.6 REVIEW QUESTIONS

1. Define access control.
2. What are the basic elements of an authentication system?
3. Define biometric systems and list five of their methods.
4. Define a symmetric (one-key) encryption.
5. List some of the disadvantages of the symmetric system.
6. What are the key components of PKI?
7. Describe the PKI process.
8. How does a digital signature work?
9. Describe digital certification.

10.7 THE DEFENSE II: SECURING E-COMMERCE NETWORKS

Several technologies exist that ensure that an organization's network boundaries are secure from cyber attack or intrusion, and that if the organization's boundaries are compromised, the intrusion is detected quickly and combated. Different types of cyber attacks (e.g., viruses and other malware, DoS, and other botnet attacks) can arrive via the organization's communication networks. Companies need to detect intrusions as quickly as possible, diagnose the specific type of attack, and fix the problem. The major tools for protecting against attacks that arrive via the networks are described next.

Firewalls

Firewalls are barriers between an internal trusted network (or a PC) and the untrustworthy Internet. A firewall is designed to prevent unauthorized access to and from private networks, such as intranets. Technically, a firewall is composed of hardware and a software package that separates a private computer network (e.g., your LAN) from a public network (the Internet). On the Internet, the data and information exchanged between computers are broken into segments called **packets**. Each packet contains the Internet address of the computer sending the data, as well as the Internet address of the computer receiving the data. A firewall examines all data packets that pass through it and then takes appropriate action based on its diagnosis – to allow or not to allow the data to enter the computer. Firewalls are designed mainly to protect against any remote login, access by intruders via backdoors, spam, and different types of malware (e.g., viruses or macros). Firewalls come in several shapes and formats (search Google Images for 'firewalls'). A popular defense system is a DMZ. The DMZ can be designed in two different ways, using a single firewall or with dual firewalls. The one that includes two firewalls is illustrated in Figure 10.10.

The Dual Firewall Architecture: The DMZ

In the simplest case, there is one firewall between the Internet and the internal users. In the DMZ architecture (DMZ stands for demilitarized zone), there are two firewalls between the Internet and the internal users. One firewall is between the Internet and the DMZ (border firewall) and another one is between the DMZ and the internal network. All public servers are placed in the DMZ (i.e., between the two firewalls). With this setup, it is possible to have firewall rules that allow trusted partners access to the public servers, but the interior firewall can restrict all incoming connections. Using internal firewalls at various intranet boundaries also can limit damage from *threats* that have managed to penetrate the border firewalls.

Personal Firewalls

The number of users with high-speed broadband (cable modem or digital subscriber lines; DSL) has increased the number of Internet connections to homes or small businesses. The connections that are always "on" are much more vulnerable to attack than simple dial-up connections.

Personal firewalls protect desktop systems by monitoring all incoming traffic to your computer.

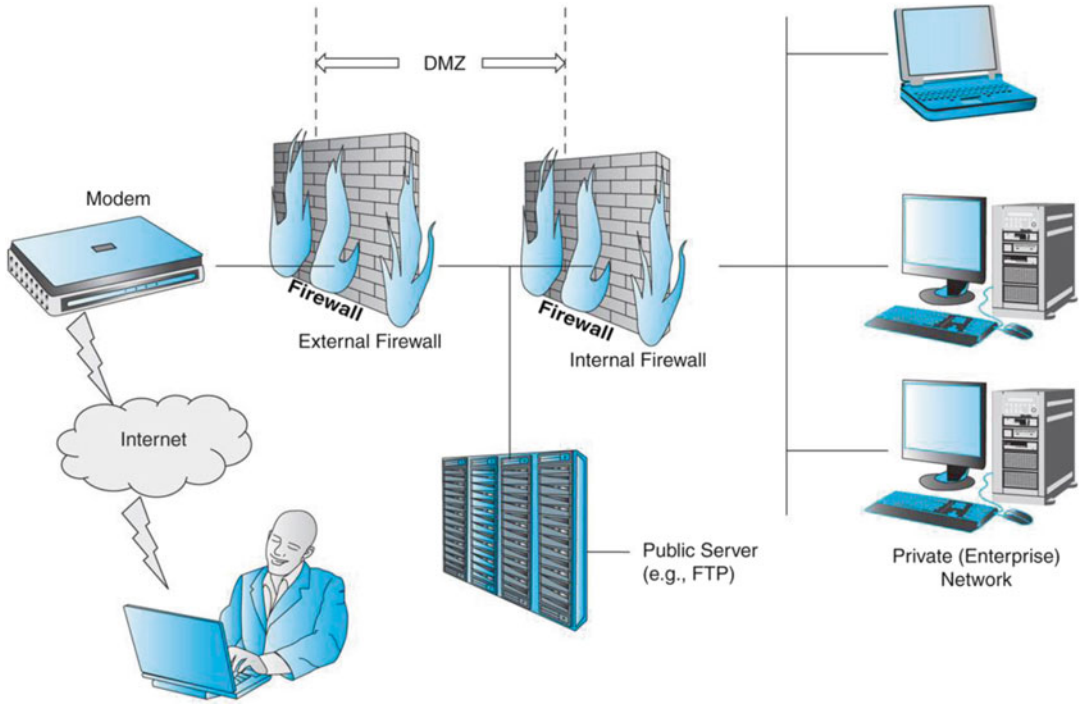

Figure 10.10 The two firewalls: DMZ architecture

Virtual Private Networks (VPNs)

Suppose a company wants to establish a B2B application, providing suppliers, partners, and others access not only to data residing on its internal website, but also to data contained in other files (e.g., Word documents) or in legacy systems (e.g., large relational databases). Traditionally, communications with the company would have taken place over a secure but expensive *value-added private leased line* or through a dial up line connected to modems or a remote access server (RAS). Unfortunately, using the Internet instead, which is free, may not be secure. A more secure use of the Internet is provided by using a VPN.

A **virtual private network (VPN)** refers to the use of the Internet to transfer information, but in a more secure manner. A VPN behaves like a private network by using encryption and other security features to keep the information secure. For example, a VPN verifies the identity of anyone using the network.

VPNs can reduce communication costs dramatically. The costs are lower because VPN equipment is cheaper than other communication solutions; private leased lines are not needed to support remote access; and a single access line can be used to support multiple purposes.

To ensure the confidentiality, integrity, and availability of the data transmitted, a VPN uses *protocol tunneling*. With **protocol tunneling**, data packets are first encrypted and then encapsulated into packets that can be transmitted across the Internet. Cisco Systems, Inc. (**cisco.com**) provides several types of VPNs. For details on VPNs, see **searchenterprisewan.techtarget.com/definition/virtual-private-network.**

Intrusion Detection Systems (IDS)

No matter how protected an organization is, it still can be a target for attempted security attacks. For example, most organizations have antivirus software, yet they are subjected to virus attacks by new viruses. This is why an organization must continually monitor for attempted, as well as

actual, security breaches. The monitoring can be done by using intrusion detectors.

An **intrusion detection system (IDS)** is a device composed of software and/or hardware designed to monitor the activities of computer networks and computer systems in order to detect and define unauthorized and malicious attempts to access, manipulate, and/or disable these networks and systems. An IDS inspects all inbound and outbound flows of information and is used for detecting specific types of malicious activities (e.g. viruses, DoS) that have already occurred. For example, the IDS checks files on a regular basis to see if the current digital signatures match the previous signatures. If the signatures do not match, security personnel are alerted. For details, the technology, benefits, and limitations, see **searchsecurity.techtarget.com/guidesIntroduction-to-IDS-IPS-Network-intrusion-detection-system-basics**.

Dealing with DoS Attacks

DoS attacks, as described earlier, are designed to bombard websites with all types of useless information, which clogs the sites. The faster a DoS attack is discovered, the easier is the defense. DoS attacks grow rapidly. Therefore, detecting an intrusion early can help. Since there are several types of DoS attacks (e.g., DDoS), there are several defense methods. For examples, see **learn-networking.com/network-security/how-to-prevent-denial-of-service-attacks**. Intrusion detecting software also identifies the DoS type, which makes the defense easier and faster.

Cloud Computing Prevents DoS Attacks

In 2011, it was demonstrated that cloud computing was effective against distributed denial-of-service (DDoS). For examples, see Fisher (2014).

Honeynets and Honeypots

Honeynets are another technology that can detect and analyze intrusions. A **honeynet** is a network of *honeypots* designed to attract hackers, just as bees are attracted to honey. In this case, the **honeypots** are simulated information system components such as EC servers, payments gates, routers, database servers, and even firewalls, that look like real working systems. When intruders enter the honeypot, their activities are monitored. Security experts then analyze why and how the hackers attack, and what they do during and after the system is compromised.

Project Honeypot consists of thousands of security professionals from around the world (see **projecthoneypot.org**). The project runs its own honeynet traps, but also helps others with running theirs. Honeynet's volunteers investigate the latest attacks and help create new tools to improve Internet security.

E-Mail Security

E-mail exhibits several of the security problems discussed in Sections 10.3 and 10.4. To begin with, we get viruses from e-mail attachments and software downloads. Spam and social engineering attacks arrive via e-mail. Unfortunately, firewalls may not be effective in protecting e-mail, and therefore one should use an antivirus program as well as anti-spam software (available from dozens of vendors). E-mail encryption is advisable and available from many vendors. Finally, a technique called *outbound filtering* may be used. A brief description of each of these methods follows:

- **Antivirus and antispam.** Detects and quarantines messages that contain viruses, worms, spam, phishing attacks, or other unwanted content.
- **E-mail encryption.** Scrambles sensitive data in messages and attachments so they can be read only by intended recipients.
- **Outbound filtering.** Scans for unauthorized content, such as a user's Social Security number, included in outgoing e-mail or other communications.

Cloud Computing May Help

As of 2008, there has been increased interest in using cloud computing to improve e-mail security. Furthermore, this can be done by cutting

costs 50 to 80% (per Habal 2010). One reason is that there are dozens of vendors that offer cloud solutions, ranging from Oracle and Microsoft to small vendors.

SECTION 10.7 REVIEW QUESTIONS

1. List the basic types of firewalls and briefly describe each.
2. What is a personal firewall? What is DMZ architecture?
3. How does a VPN work and how does it benefit users?
4. Briefly describe the major types of IDSs.
5. What is a honeynet? What is a honeypot?
6. Describe e-mail security.

10.8 THE DEFENSE III: GENERAL CONTROLS, SPAM, POP UPS, FRAUD, AND SOCIAL ENGINEERING CONTROLS

The objective of IT security management practices is to defend information systems. A defense strategy requires several *controls*, as shown in Figure 10.11.

The major types of controls are: (1) **General controls**, which are designed to protect all system applications. (2) **Application controls** guard applications. In this and the following sections, we discuss representative types of these two groups of

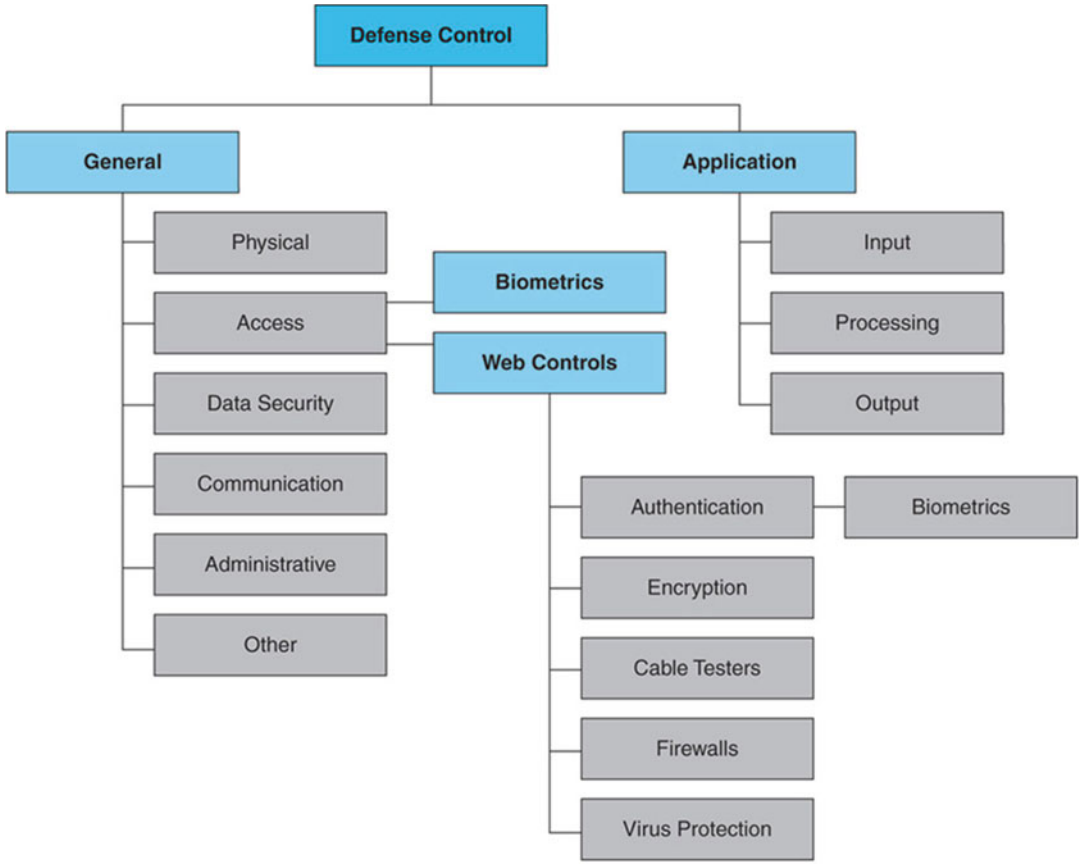

Figure 10.11 Major defense controls

information system controls. Later in the section, we cover spam and fraud mitigation.

General, Administrative, and Other Controls

The major categories of general controls are physical controls, administrative controls, and other controls. A brief description of general controls is provided next.

Physical Controls

Physical controls protect computer facilities and resources, including the physical area where computing facilities are located. The controls provide protection against natural hazards, criminal attacks, and some human error. Typical physical controls could include:

- A properly designed data center. For example, the site should be air conditioned, noncombustible, and waterproof.
- Protection against electromagnetic fields (e.g., against lightning).
- Comprehensive fire management (i.e., fire prevention, detection, containment, and extinguishment).
- Emergency (back up) power generators and automatic shut off power devices, if needed.
- Motion detectors that can detect physical intrusion and activate alarms.

Network access control software is offered by all major security vendors (e.g., see **symantec.com/endpoint-protection**).

Administrative Controls

Administrative controls are defined by management and cover guidelines and compliance issuing and monitoring. Table 10.1 gives examples of such controls.

Table 10.1 Representative administrative controls

• Appropriately selecting, training, and supervising employees, especially in accounting and information systems
• Fostering company loyalty
• Immediately revoking access privileges of dismissed, resigned, or transferred employees
• Requiring periodic modification of access controls (such as passwords)
• Developing programming and documentation standards (to make auditing easier and to use the standards as guides for employees)
• Insisting on security bonds or malfeasance insurance for key employees
• Instituting separation of duties; namely, dividing sensitive computer duties among as many employees as economically feasible in order to decrease the chance of intentional or unintentional damage
• Holding periodic random audits of the system

Protecting Against Spam

Sending spam that includes a sales pitch and looks like personal, legitimate e-mail and may bypass filters, is a violation of the U.S. Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003. However, many spammers hide their identity by using hijacked PCs or spam zombies to avoid detection and identification. For protecting your system against botnet attacks, which also spread a huge volume of spam, see MessageLabs (2009).

The "Controlling the Assault of Non-Solicited Pornography and Marketing Act," **CAN-SPAM Act** makes it a crime to send commercial e-mail messages with spam. The following are other provisions of the law, extracted from the United States Federal Trade Commission (FTC) Bureau of Consumer Protection Business Center (**business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business**), which provides "The CAN-SPAM Act: A Compliance Guide for Business.

- Companies must offer an opt-out link in each message and marketing campaigns.
- Allows heavy penalties for spamming (each separate e-mail is subject to penalties of up to $16,000).

- Requires marketers to report their physical postal address in e-mail messages.
- Carries other penalties – those found guilty of certain criminal acts (e.g., accessing someone else's computer to send spam; using false information to register multiple e-mail addresses, etc.) may face up to five years in prison.
- Enables the FTC, certain other federal agencies, and state attorneys general to bring lawsuits under certain sections of the Act. Although individuals are prohibited from suing spammers, individuals may be able to sue as ISPs but this may be cost prohibitive.

In 2008, the FTC added four new provisions to the CAN-SPAM Act of 2003, intending to clarify the Act's requirements. For details, see **ftc.gov/news-events/press-releases/2008/05/ftc-approves-new-rule-provision-under-can-spam-act**.

Protecting Your Computer from Pop-Up Ads

As discussed in Chapter 9, the use of pop-ups and similar advertising methods is growing rapidly. Sometimes it is even difficult to close these ads when they appear on the screen. Some of these ads may be part of a consumer's permitted marketing agreement, but most are unsolicited. What can a user do about unsolicited pop-up ads? The following tools help minimize pop-ups.

Tools for Stopping or at Least Minimizing Pop-Ups

It is possible to install software that blocks pop-up ads. Several software packages offer pop-up stoppers. Some are free (e.g., Panicware, Inc.'s Pop-Up Stopper Free Edition **pop-up-stopper-free-edition.software.informer.com**), Softonic's Pop up Blocker (**pop-up-blocker.en.softonic.com/download**), and AdFender (**adfender.com**); others are available for a fee. For a list, see **snapfiles.com**; and for a list of blocker software for Windows, see **download.cnet.com/windows/popup-blocker-software**. Many ISPs and major browser makers (e.g., Google, Microsoft, Yahoo!, Mozilla) offer tools to stop pop-ups.

However, adware or software that is bundled with other popular applications, like person-to-person file sharing, is able to deliver the pop-up ads.

Protecting Against Other Social Engineering Attacks

With the increasing number of social engineering attacks via websites and in social networks comes the need for better protection. The open source environment and the interactive nature of the technology also create risks (see Chapter 7 and Section 10.4). Thus, EC security becomes a necessity for any successful social networking initiative.

Social networking spans many different applications and services. Therefore, many methods and tools are available to defend such systems. Many of the solutions are technical in nature and are outside the scope of this book.

For discussion on security in social media and social networking, see Sarrel (2010).

Protecting Against Phishing

Because there are many phishing methods, there are many defense methods as well. Illustrative examples are provided by Symantec (2009) and the FTC Consumer Information at **consumer.ftc.gov/articles/0003-phishing**. For risk and fraud insights, see **sas.com/en_us/insights/risk-fraud.html**.

Protecting Against Malvertising

According to TechTarget, *malvertising (malicious advertising)* "is an advertisement on the Internet that is capable of infecting the viewer's computer with malware." Microsoft combats malvertising by taking legal action against malvertisers.

Protecting Against Spyware

In response to the emergence of spyware, a large variety of antispyware software exists. Antispyware laws, available in many jurisdictions,

usually target any malicious software that is installed without the knowledge of users. The U.S. Federal Trade Commission advises consumers about spyware infections. For details and resources, see **ftc.gov/news-events/media-resources/identity-theft-and-data-security/spyware-and-malware**.

Protecting Against Cyberwars

This is a difficult task since these attacks usually come from foreign countries. The U.S. government is developing tools that will mine social media sites to predict cyber attacks. The tools will monitor all Facebook, Twitter, and other social networks sites to interpret content. The idea is to automate the process.

Fraud Protection

As we will see in Chapter 15, it is necessary to protect both the sellers and buyers (consumers) against fraud they may commit against each other. In a special annual online fraud report, CyberSource (2012, 2013) describes the issue of payment fraud committed by buyers, which cost merchants several billions of dollars annually. The reports cover the areas of detection, prevention, and management of online fraud. The report also list tools for automatic screening of credit cards.

Business Continuity, Disaster Recovery, and Risk Management

A major building block in EC security for large companies or companies where EC plays a critical role (e.g., banks, airlines, stock brokerages, e-tailers) is to prepare for natural or man-made disasters. Disasters may occur without warning. A prudent defense is to have a *business continuity plan*, mainly consisting of a *disaster recovery* plan. Such a plan describes the details of the recovery process from major disasters such as loss of all (or most) of the computing facilities. Moreover, organizations may need to have a satisfactory disaster prevention and recovery plan in order to obtain insurance for their computer systems or even for the entire business operation. The comprehensiveness of a business recovery plan is shown in Figure 10.12. The details are presented in Online File W10.2.

Risk-Management and Cost-Benefit Analysis

It is usually not economical to prepare protection against every possible threat. Therefore, an EC security program must provide a process for assessing threats and their potential damages, deciding which threats to protect against first, and which threats to ignore or provide only reduced protection. For details, see Online File W10.2.

SECTION 10.8 REVIEW QUESTIONS

1. What are general controls? List the various types.
2. What are administrative controls?
3. How does one protect against spam?
4. How does one protect against pop-ups?
5. How does one protect against phishing, spyware, and malvertising?
6. Describe protection against cyberwars.
7. Define business continuity and disaster recovery.

10.9 IMPLEMENTING ENTERPRISEWIDE E-COMMERCE SECURITY

Now that you have learned about both the threats and the defenses, we can discuss some implementation issues starting with the reasons why it is difficult, or even impossible, to stop computer crimes and the malfunction of information systems.

The Drivers of EC Security Management

The explosive growth of EC and SC, together with an increase in the ever-changing strategies of cybercriminals (Jaishankar 2011), combined with regulatory requirements and demands by insurance companies, drive the need for comprehensive EC security management. Additional drivers are:

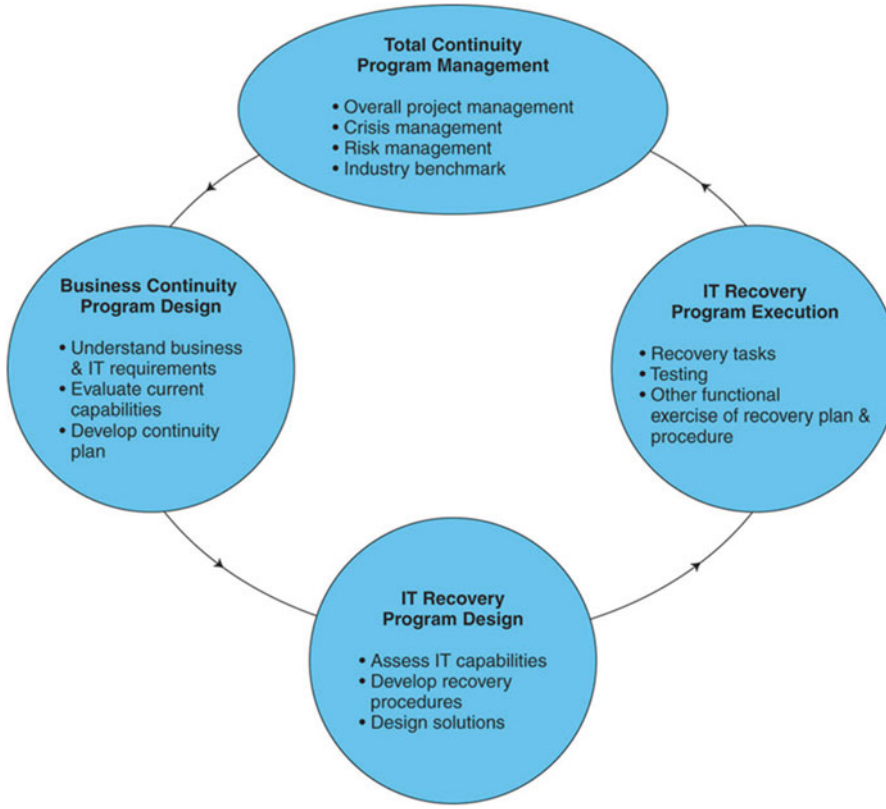

Figure 10.12 Business continuity services and IT recovery process

- The laws and regulations with which organizations must comply.
- The conduct of global EC. More protection is needed when doing business with a foreign country.
- Information assets have become critical to the operation of many businesses.
- New and faster information technologies are shared throughout organizations. Organizational collaboration is needed.
- The complexity of both the attacks and the defense require an organization-wide collaboration approach.

Senior Management Commitment and Support

The success of an EC security strategy and program depends on the commitment and involvement of senior management. Many forms of security are unpopular because they are inconvenient, restrictive, time-consuming, and expensive. Security practices may not be a top organizational priority unless they are mandated.

Therefore, an EC security and privacy model for effective enterprisewide security should begin with senior management's commitment and support, as shown in Figure 10.13. The model views EC security (as well as the broader IT security)

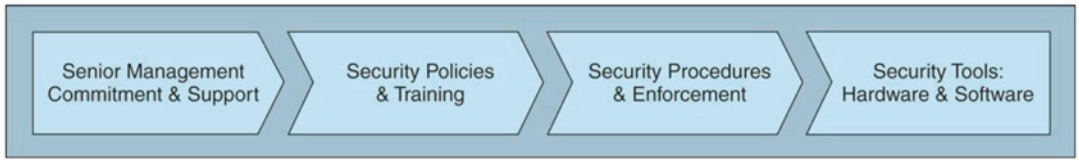

Figure 10.13 Enterprisewide EC security and privacy model

as a combination of commitment and support, policies and training, procedures and enforcement, and tools, all executed as a continuous process.

EC Security Policies and Training

An important security task is developing an organizational EC security policy, as well as procedures for specific security and EC activities such as access control and protecting customer data. These include roles, responsibilities, and enforcement. The policies need to be disseminated throughout the organization and necessary training needs to be provided (see Bailey et al. 2012). For example, to protect privacy during data collection, policies need to specify that customers should:

- Know that data is being collected, and when it is done.
- Give their permission for the data to be collected.
- Have knowledge and some control over how the data is controlled and used.
- Be informed that the information collected is not to be shared with other organizations.

Similarly, to protect against criminal use of social media, you can:

- Develop policies and procedures to exploit opportunities but provide customer protection.
- Educate employees and others about what is acceptable and what is not acceptable.

Cyber Threat Intelligence (CTI)

As part of policies and training, companies can deploy cyber intelligence. According to **sans.org**, it is an important defense tool.

EC Risk Analysis and Ethical Issues

EC security procedures require an evaluation of the digital and financial assets at risk – including cost and operational considerations. To calculate the proper level of protection, managers responsible for a digital asset need to assess its risk exposure.

A related assessment is the *business impact analysis.* **Business impact analysis (BIA)** refers to an analysis of the impact of losing the functionality of an EC activity (e.g., e-procurement, e-ordering) to an organization. Once such risks are computed, the organization should focus its defense strategy on the largest risks. This analysis may include the use of cyber-risk insurance against data breaches and other cybercrimes (see Willhite 2013).

Ethical Issues

Implementing security programs raises several ethical issues. First, some people are against the monitoring of any individual's activities. Imposing certain controls is seen by some as a violation of freedom of speech or other civil rights. A survey by the Gartner Group found that even after the terrorist attacks of September 11, 2001, only 26% of Americans approved a national ID database. Many consider using biometrics to be a violation of privacy.

Handling the privacy versus security dilemma is difficult. There are other ethical and legal obligations that may require compa-

nies to "invade the privacy" of employees and monitor their actions. In particular, IT security measures are needed to protect against loss, liability, and litigation. Losses are not just financial, but also include the loss of valuable information, customers, trading partners, brand image, and the inability to conduct business as usual due to the actions of hackers, malware, or employees.

Why Is It Difficult to Stop Internet Crime?

The following are the major reasons Internet crime is so difficult to stop.

Making Shopping Inconvenient

Strong EC security may make online shopping inconvenient and may slow shopping as well. Therefore, shoppers may not like some security measures.

Lack of Cooperation by Business Partners

There is a potential lack of cooperation from credit card issuers, suppliers, local and especially foreign ISPs, and other business partners. If the source ISP would cooperate and suspend the hacker's access, it would be very difficult for hackers to gain access to the systems.

Shoppers' Negligence

Many online shoppers are not taking the necessary (but inconvenient) precautions to avoid becoming victims of identity theft or fraud.

Ignoring EC Security Best Practices

Many companies do not have prudent IT security management or employee security awareness. For example, in a 2008 study, the *Computing Technology Industry Association* (CompTIA 2008) found that the most widespread threats in the United States stem from the lack of user awareness and malware attacks. The situation is somewhat better today.

Design and Architecture Issues

It is well known that preventing vulnerability during the EC design and preimplementation stage is far less expensive than mitigating problems later; unfortunately, such prevention is not always made. Even minor design errors can increase hacking. Note that, almost every element in an EC application may be subject to some sort of security threat. Designers may not consider all the elements.

Lack of Due Care in Business Practices

Another reason for the difficulty is the lack of due care in conducting many business processes (e.g., in crowdsourcing). The **standard of due care** is the minimum and customary practice that a company is reasonably expected to take to protect the company and its resources from possible risks. Managers may ignore the standard of due care (e.g., they hire criminals, outsource to fraudulent vendors), placing their EC business security at risk. For a description of the Payment Card Industry (PCI) standard and its requirements, see **pcistandard.com**. For a major survey see PWC (2013).

Protecting Mobile Devices, Networks, and Applications

With the explosive growth of mobility and m-commerce comes the task of protecting these systems from the security problems described earlier in this chapter and from some new ones. While the challenges, attacks, and defenses described earlier relate both to the wireline and wireless environments, there are certain challenges that are unique to the mobile/wireless environment.

Mobile Security Issues

Cooney (2012) lists the 10 major security issues that range from wireless transmissions not being encrypted, to lack of firewalls or passwords on mobile devices, or connecting to an unsecured WiFi network. The article offers many solutions, most of which are discussed in Sections 10.6 and 10.7 (e.g., conduct risk assessment, install firewalls).

Reisinger (2014) lists additional security issues such as data theft and unlocked jailbreaking devices. The proliferation of BYOD (Chapter 6) also brings threat to the enterprise (see Westervelt 2013 and Phneah 2013).

The Defense

To defend mobile systems it is necessary to implement tools and procedures such as those described in Sections 10.6 and 10.7, and modify them for the mobile environment. A practical checklist for reducing security risks is offered by Lenovo (2013). See also, LabTech (2012). Finally, a major problem is the theft of mobile devices. Two solutions are at work: First, automatic security that enables only the owners to use their devices and second, make a kill switch a mandatory feature in all smartphone (scheduled for 2015).

SECTION 10.9 REVIEW QUESTIONS

1. If senior management is not committed to EC security, how might that impact the e-business?
2. What is a benefit of using the risk exposure method for EC security planning?
3. Why should every company implement an acceptable use policy?
4. Why is training required?
5. List the major reasons why it is difficult to stop computer crimes.

MANAGERIAL ISSUES

Some managerial issues related to this chapter are as follows.

1. **What steps should businesses follow in establishing a security plan?** Security management is an ongoing process involving three phases: asset identification, risk assessment, and implementation. By actively monitoring existing security policies and procedures, companies can determine which of them are successful or unsuccessful and, in turn, which should be modified or eliminated. However, it also is important to monitor changes in business processes and business environments and adjust the plans accordingly. In this way, an organization can keep its security policies and measures up-to-date.
2. **Should organizations be concerned with internal security threats?** Except for malware, breaches committed by insiders are much more frequent than those done by outsiders. This is true for both B2C and B2B sites. Security policies and measures for EC sites need to address the insider threats. For a guideline, see Schwartz (2012). In addition, insiders can be victims of security crimes. Therefore, organizations need to be aware of social engineering schemes. Companies should educate employees, especially new hires, about such threats.
3. **What is the key to establishing strong e-commerce security?** Most discussions about security focus on technology, with statements like, "all messages should be encrypted." Although technologies are important, no security solution is useful unless it is adopted by the employees. Determining business requirements is the first step in creating a security solution. Business requirements, in turn, determine information requirements. Once information requirements are known, it is possible to assess their value, and then a plan can be made for how to protect the most valuable and most vulnerable information assets.

SUMMARY

In this chapter, you learned about the following EC issues as they relate to the chapter's learning objectives.

1. **The importance and scope of EC information security.** For EC to succeed, it must be secure. Unfortunately, this is not an easy task due to many unintentional and intentional hazards. Security incidents and breaches interrupt EC transactions and increase the cost of doing business online. Internet design is vulnerable, and the temptation to commit computer crime is increasing with the increased applications and volume of EC. Criminals are expanding operations, creating an underground economy of valuable information that was stolen.

A strategy is needed to handle the costly defense technology and operation, which includes training, education, project management, and the ability to enforce security policy. EC security will remain an evolving discipline because threats are changing continuously. Therefore, e-business needs to adapt. An EC security strategy is needed to optimize EC security programs for efficiency and effectiveness. There are several reasons why. EC security costs and efforts, when implemented as a reaction to crises is greater than if organizations had an EC security strategy and acts accordingly. The Internet is still a fundamentally insecure infrastructure. There are many criminals whose major motive is to profit by stealing information.

2. **Basic EC security issues.** The security issue can be viewed as a battleground between attackers and attacks and defenders and defense. There are many variations on both sides and many possible collision scenarios. Owners of EC sites need to be concerned with multiple security issues: authentication, verifying the identity of the participants in a transaction; authorization, ensuring that a person or process has access rights to particular systems or data; and auditing, being able to determine whether particular actions have been taken and by whom.
3. **Threats, vulnerabilities, and technical attacks.** EC sites are exposed to a wide range of attacks. Attacks may be nontechnical (social engineering), in which a criminal lures people into revealing sensitive personal information. Alternatively, attacks may be technical, whereby software and systems expertise are used to attack networks, databases, or programs. DoS attacks bring operations to a halt by sending a flood of data to target specific computers and websites. Malicious code attacks include viruses, worms, Trojan horses, or some combination of these. Over the past few years, new malware trends have emerged, such as Blackhole and ZeroAccess (see Wang 2013). The new trends include an increase in the speed and volume of new attack methods; and the shorter time between the discovery of a vulnerability and the release of an attack (to exploit the vulnerability). Finally, the new trends include the growing use of bots to launch attacks; an increase in attacks on mobile systems, social networks, and Web applications; and a shift to profit-motivated attacks.
4. **Internet fraud, phishing, and spam.** A large variety of Internet crimes exist. Notable are identify theft and misuse, stock market frauds, get-rich-quick scams, and phishing. Phishing attempts to obtain valuable information from people by masquerading as a trustworthy entity. Personal information is extracted from people (or stolen) and sold to criminals, who use it to commit financial crimes such as transferring money to their own accounts. A related area is the use of unsolicited advertising or sales via spam.
5. **Information assurance.** The information assurance model represents a process for managing the protection of data and computer systems by ensuring their confidentiality, integrity, and availability. Confidentiality is the assurance of data privacy. Integrity is the assurance that data is accurate or that a message has not been altered. Availability is the assurance that access to data, the website, or EC systems and applications is available, reliable, and restricted to authorized users whenever they need it.
6. **Securing EC access control and communications.** In EC, issues of communication among trading partners are paramount. In many cases, EC partners do not know their counterparts, so they need secured communication and trust building. Trust starts with the authentication of the parties involved in a transaction; that is, identifying the parties in a transaction along with the actions they are authorized to perform. Authentication can be established with something one knows (e.g., a password), something one has (e.g., an entry card), or some physical characteristic (e.g., a fingerprint). Biometric systems can confirm a person's identity. Fingerprint

scanners, iris scanners, facial recognition, and voice recognition are examples of biometric systems. A special encryption system for EC is the PKI. Public key infrastructure (PKI), which is the cornerstone of secure e-payments and communication, also can authenticate the parties in a transaction. For the average consumer and merchant, PKI is made simple by including it in Web browsers and services. Such tools are secure because security is based on SSL (or TSL) communication standards.

7. **Technologies for protecting networks.** Firewalls, VPNs, and IDSs have proven extremely useful on EC sites. A firewall is a combination of hardware and software that separates an enterprise private network from the Internet. Firewalls are of two general types – packet-filtering routers or application-level proxies. IDSs monitor activities done on a network or inside a computer system. The IDSs watch for intruders and automatically act whenever a security breach or attack occurs. In the same vein, some companies are installing honeynets and honeypots in an effort to gather information on intrusions and to analyze the types and methods of attacks being perpetrated.
8. **The different controls and special defense mechanisms.** The major controls are general (including physical, access controls, biometrics, administrative controls, application controls, and internal controls for security and compliance). Each type has several variations.
9. **Protecting against fraud.** Given the large number of ways to commit Internet fraud, it is difficult to protect against all of them. Fraud protection is done by companies, security vendors, government regulations, and perhaps most important, consumer education. Knowing the most common methods used by criminals is the first step of defense. Remember, most criminals are very experienced. They are able to invest in new and clever attack methods.
10. **Enterprisewide EC security.** EC security procedures are inconvenient, expensive, tedious, and never ending. Implementing a defensive in-depth model that views EC security as a combination of commitment, people, processes, and technology is essential. An effective program starts with senior management's commitment and budgeting support. This sets the tone that EC security is important to the organization. Other components are security policies and training. Security procedures must be clearly defined. Positive incentives for compliance can help, and negative consequences need to be enforced for violations. The last stage is the deployment of hardware and software tools based on the policies and procedures defined by the management team.
11. **Why is it so difficult to stop computer crimes?** Responsibility or blame for cybercrimes can be placed on criminals, victimized people, and organizations. Online shoppers fail to take necessary precautions to avoid becoming victims. Security system designs and architectures are still incredibly vulnerable. Organizations may fail to exercise due care in business or hiring and practices, opening the doors to security attacks. Every EC business knows that there are threats of stolen credit cards, data breaches, phishing, malware, and viruses that never end – and that these threats must be addressed comprehensively and strategically.

KEY TERMS

Access control
Application controls
Authentication
Authorization
Availability
Banking Trojan
Biometric authentication
Biometric systems
Botnet
Business continuity plan
Business impact analysis (BIA)
CAN-SPAM Act
Certificate authorities
CIA security triad (CIA triad)

Ciphertext
Confidentiality
Cracker
Cybercrime
Cybercriminal
Darknet
Data breach
Denial-of-service (DoS) attack
Detection measures
Deterring measures
Digital envelope
Digital signature
EC security strategy
E-mail spam
Encryption
Encryption algorithm
Exposure
Firewall
Fraud
General controls
Hacker
Hash function
Honeynet
Honeypot
Identity theft
Information assurance (IA)
Information security
Integrity
Internet underground economy
Intrusion detection system (IDS)
Key (key value)
Key space
Keystroke logging (keylogging)
Macro virus (macro worm)
Malware (malicious software)
Message digest (MD)
Non-repudiation
Packet
Page hijacking
Penetration test (pen test)
Personal firewall
Pharming
Phishing
Plaintext
Prevention measures
Private key
Protocol tunneling
Public key
Public key infrastructure (PKI)
Public (asymmetric) key encryption
Risk
Search engine spam
Social engineering
Spam
Spam site
Splog
Spyware
Standard of due care
Symmetric (private) key encryption
Trojan horse
Virtual private network (VPN)
Virus
Vulnerability
Vulnerability assessment
Worm
Zombies

DISCUSSION QUESTIONS

1. Consider how a hacker might trick people into divulging their user IDs and passwords to their Amazon.com accounts. What are some of the specific ways that a hacker might accomplish this? What crimes can be performed with such information?
2. B2C EC sites and social networks continue to experience DoS and DDoS attacks. How are these attacks executed? Why is it so difficult to safeguard against them? What are some of the things a site can do to mitigate such attacks?
3. How are botnets, identity theft, DoS attacks, and website hijackings perpetrated? Why are they so dangerous to e-commerce?
4. Discuss some of the difficulties of eliminating online financial fraud.
5. Enter **zvetcobiometrics.com**. Discuss the benefits of these products over other biometrics.
6. Find information about the Zeus Trojan virus. Discuss why it is so effective at stealing financial data. Why is it so difficult to protect against this Trojan? Hint: See Falliere and Chien (2009).
7. Find information about the scareware social engineering method. Why do you think it is so effective?

8. Visit the National Vulnerability Database (**nvd.nist.gov**) and review five recent CVE vulnerabilities. For each vulnerability list its published date, CVSS severity, impact type, and the operating system or software with the vulnerability.
9. Report on the status of using biometrics in mobile commerce. (Start **nxt-id.com**.)

TOPICS FOR CLASS DISCUSSION AND DEBATES

1. Read McNeal (2012) and take the multiple choice quiz there. Discuss the results.
2. A business wants to share its customer data with a trading partner, and provide its business customers with access to marketing data. What types of security components (e.g., firewalls, VPNs, etc.) could be used to ensure that the partners and customers have access to the account information while those who are unauthorized do not? What types of network administrative procedures will provide the appropriate security?
3. Why is it so difficult to fight computer criminals? What strategies can be implemented by financial institutions, airlines, and other heavy users of EC?
4. All EC sites share common security threats and vulnerabilities. Do you think that B2C websites face different threats and vulnerabilities than do B2B sites? Explain.
5. Why is phishing so difficult to control? What can be done? Discuss.
6. Debate this statement: "The best strategy is to invest very little and only in proven technologies such as encryption and firewalls."
7. Debate: Can the underground Internet marketplace be controlled? Why or why not?
8. Debate: Is taking your fingerprints or other biometrics to assure EC security a violation of your privacy?
9. Body scans at airports have created controversy. Debate both points of this issue and relate it to EC security.
10. Debate: The U.S. government has signaled that it would view a computer attack from a foreign nation as justification for military action. Do you agree or not?
11. Discuss the issue of providing credit card details on Facebook. Would you do it?
12. Examine the identity theft and identity crime topics from the FBI site **fbi.gov/about-us/investigate/cyber/identity_theft**. Report the highlights.

INTERNET EXERCISES

1. Your B2C site has been hacked with a new, innovative method. List two organizations where you would report this incident so that they can alert other sites. How do you do this and what type of information do you have to provide?
2. Determine the IP address of your computer by visiting at least two websites that provide that feature. You can use a search engine to locate websites or visit **ip-adress.com** or **whatismyipaddress.com**. What other information does the search reveal about your connections? Based on this finding, how could a hacker use that information?
3. Conduct a Google search for 'Institutional Identity Theft.' Compare institutional identity theft with personal identity theft. How can a company protect itself against identity theft? Write a report.
4. The National Strategy to Secure Cyberspace (**dhs.gov/national-strategy-secure-cyberspace**) provides a series of actions and recommendations for each of its five national priorities. Download a copy of the strategy (**us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf**). Select one of the priorities and discuss in detail the actions and recommendations for that priority.
5. The Symantec Annual Internet Security Threat Report provides details about the trends in attacks and vulnerabilities in Internet security. Obtain a copy of the latest report and summarize the major findings of the report for both attacks and vulnerabilities.
6. Conduct a Google search for examples of underground Internet activities in five different countries. Prepare a summary.

7. Enter **consumer.ftc.gov/features/feature-0014-identity-theft**, **idtheftcenter.org**, and **fbi.gov/about-us/investigate/cyber/identity_theft**. Find information about the prevention of and protection against identity theft. Also look for cases of companies that survived identity theft. Write a report.
8. Enter **verisign.com** (a Symantec company) and find information about PKI and encryption. Write a report.
9. Enter **hijackthis.com**. What is offered in the site? Write a report.
10. Enter **blackhat.com**. Find out what the site is about. Describe some of the site's activities.
11. Conduct a Google search for articles on 'Fort Disco' and other botnets used to attack WordPress. Discuss the attacks and possible defenses.

TEAM ASSIGNMENTS AND PROJECTS

1. **Assignment for the Opening Case**
   Read the opening case and answer the following questions:
   (a) Why did the college have security problems? What types of problems?
   (b) What is the security problem concerning social media applications?
   (c) Why was the automation (agent-based) solution unsuccessful?
   (d) Why were the computer-use policies ineffective?
   (e) What was the problem with the bandwidth?
   (f) Describe the new security policy. Why does it work?
   (g) Discuss the issue of privacy as it applies to this case.
2. Assign teams to report on the latest major spam and scam threats. Look at examples provided by **ftc.gov**, the latest Symantec report on the State of Spam, and white papers from IBM, VeriSign, McAfee, and other security firms.
3. Enter **symantec.com/security_response/publications/whitepapers.jsp** and find the white papers: (1) "The Risks of Social Networking" (available at **symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_risks_of_social_networking.pdf**) and (2) "The Rise of PDF Malware" (available at **symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_rise_of_pdf_malware.pdf**). Prepare a summary of both and find how they relate to each other.
4. Watch the video "Cyberattacks and Extortion" (13:55 minutes) at **searchsecurity.techtarget.com/video/Cyberattacks-and-extortion**. Answer the following questions:
   (a) Why are there more extortions online today? How are they accomplished?
   (b) What is involved in targeted e-mail attacks?
   (c) What is an SQL injection attack?
5. Data leaks can be a major problem. Find some major defense methods. Check some major security vendors (e.g., Symantec). Find white papers and Webinars on the subject. Write a report.
6. Each team is assigned one method of fighting against online fraud. Each method should involve a different type of fraud (e.g., in banking). Identify suspicious e-mails, dealing with cookies in Web browsers, credit card protection, securing wireless networks, installing anti-phishing protection for your browser with a phishing filter, and so forth.
7. Find information on the Target data breaches and other physical stores that have been affected. Identify the methods used by the hackers. What defense strategies are used?

CLOSING CASE: HOW ONE BANK STOPPED SCAMS, SPAMS, AND CYBERCRIMINALS

Some say that as many as 90% of phishers are targeting financial institutions. Let us see how one bank is protecting its customers.

BankWest of South Dakota (bankwest-sd.com)

As a privately owned entity, a bank can disregard short term profit. Instead, a bank provides the utmost in customer care and employee educational programs. However, one problem is challenging:

the increasing number of incidents of social engineering experienced by customers. A few examples of scams that were noticed by the BankWest staff reported by Kitten (2010) are:

- **Sweetheart schemes.** There may be long term online relationship between a bank's customer and an overseas user. The overseas user tries to convince the customer to wire funds, share bank account information, and open joint accounts.
- **Letters, postal service, or e-mail.** A bank customer is notified by an e-mail that he or she has won a large amount of money (e.g., a sweepstakes). Hackers ask for some processing money to release the prize money to the customer.
- **Telephone scams.** A customer is asked to provide personal information from a government check and receives repeated telephone calls, each asking for different personal information (e.g., Social Security Number). Phone scams usually target elderly customers and depend on the social engineer's ability to develop a rapport with the customer.
- **Cell phone scams.** A customer is told that his or her debit card has been compromised and the customer is asked to provide card details for replacement.

The bank now provides information about social engineering schemes on its website (see **bankwest-sd.com/etc.htm**). Employees direct customers to the site and provide information about fraudulent schemes when the customers come into a branch. The bank also instituted an "Employee Rewards Program" (to be described later).

It is critical to combat social engineering attempts in order to increase customer confidence in Internet security. According to Kitten (2010), "the bank's information security team regularly attend workshops and participate in forums related to social engineering and other fraud schemes. The information collected is immediately shared with the staff in order to keep the entire bank team abreast of new and emerging fraud threats. All staff members also are required to complete online training in scheme detection that is designed by the bank."

Also according to Kitten (2010), the training program includes:

- Ability to identify phone scams, especially automated ones (e.g., *vishing attempts*) that lure customers into divulging sensitive information.
- Ability to identify *phishing e-mails* and use caution when clicking on links or opening file attachments.
- Conduct monthly training and employee-oriented demonstrations on face-to-face personal social engineering schemes.

Employee Rewards

Employees who identify scams are rewarded with certificates and small monetary rewards; their manager is notified and employees can take pride in the acknowledgement.

The Results

According to the bank's information security administrator, although the number of schemes has not decreased, the number of employees reporting such schemes has increased significantly.

To read BankWest's tips on how to protect yourself against identity theft, phishing, and so forth, see **bankwest-sd.com/etc.htm**.

Sources: Based on Kitten (2010) and BankWest (2014).

Questions

1. List the major security problems faced by BankWest and relate them to the attack methods described in Sections 10.2, 10.3, and 10.4.
2. In what ways is BankWest helping to stop scams before they cause damage?
3. Given the problems of BankWest and its solutions, can you suggest an even better defense mechanism?

ONLINE FILES

available at **affordable-ecommerce-textbook.com/turban**

W10.1 Application Case: How Seattle's Hospital Survived a Bot Attack

W10.2 Business Continuity and Disaster Recovery

COMPREHENSIVE EDUCATIONAL WEBSITES

cert.org: A comprehensive site, listing many resources.
csrc.nist.gov: Computer Security Resource Center.
eseminarslive.com: Webinars, events, news on security.
ic3.gov/crimeschemes.aspx: A comprehensive list of Internet crime schemes and descriptions.
itworld.com/security: A comprehensive collection of information security news, reviews and analysis, blogs, and white papers, and so forth.
nvd.nist.gov: National Vulnerability Database; a comprehensive cybersecurity and vulnerability database.
onguardonline.gov: A U.S. government comprehensive guide for online security.
sans.org/security-resources: Information security resources, glossary, and research.
spamlaws.com: Providing up-to-date information on issues affecting Internet security. News, cases, legal information, and much more; information on spam, scams, security, and so forth.
darkreading.com: *InformationWeek*'s security website. News and commentary; blogs; top stories and information on many different aspects of security.
technet.microsoft.com/en-US/security/bb291012: Microsoft Security TechCenter. Security updates, bulletins, advisories, updates, blogs, tools, and downloads.
microsoft.com/security/default.aspx: Microsoft Internet Safety and Security Center. Download updates and security essentials; tips on online security and how to avoid scams and hoaxes; resources.
technologyevaluation.com: Research articles and reports; white papers, etc. on software and security.
techsupportalert.com/best_computer_security_sites.htm: A detailed directory of computer security sites.
computer-protection-software-review.toptenreviews.com: 2014 Best computer software comparisons and reviews.
ddosattackprotection.org/blog/cyber-security-blogs: Top 100+ cyber security blogs and information security resources.

GLOSSARY

Access control A defense mechanism that determines who (person, program, or machine) can legitimately use the organization's computing resources (which resources, when, and how).
Application controls Controls that guard applications.
Authentication A process to verify (assure) the real identity of an EC entity, which could be an individual, software agent, computer program, or EC website.
Authorization The provision of permission to an authenticated person to access systems and perform certain operations in those specific systems.
Availability The assurance that access to any relevant data, information websites, or other EC services and their use is available in real time, whenever and wherever needed.
Banking Trojan Malicious software programmed to create damage when users visit certain online banking or e-commerce sites.
Biometric authentication A technology that measures and analyzes the identity of people based on measurable biological or behavioral characteristics or physiological signals.
Biometric systems A system that can *identify* a previously registered person by searching through a database for a possible *match* based on the person's observed physical, biological, or behavioral traits, or the system can *verify* a person's identity by matching an individual's measured biometric traits against a previously stored version.
Botnet Malicious software that criminals distribute, usually to infect a large number of computers.
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.
Business impact analysis (BIA) An analysis of the impact of losing the functionality of an EC

activity (e.g., e-procurement, e-ordering) to an organization.

Certificate authorities (CAs) Independent agencies that issue digital certificates or SSL certificates, which are electronic files that uniquely identify individuals and websites and enable encrypted communication.

CIA security triad (CIA triad) A point of reference used to identify problem areas and evaluate the information security of an organization that includes *confidentiality*, *integrity*, and *availability.*

Ciphertext An encrypted plaintext.

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 spam.

Cracker A malicious hacker who may be more damaging than a hacker.

Confidentiality The assurance of data secrecy and privacy. Namely, the data is disclosed only to authorized people.

Cybercrime Intentional crimes carried out on the Internet.

Cybercriminal A person who intentionally carries out crimes over the Internet.

Data breach A security incident in which data are obtained illegally and then published or processed.

Denial-of-service (DoS) attack "A malicious attempt to make a server or network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet." (Incapsula, Inc.)

Detection measures Methods that help find security breaches in computer systems. Usually this means to find out whether intruders are attempting (or have attempted) to break into the EC system, whether they were successful, whether they are still damaging the system, and what damage they may have done.

Deterrent methods Countermeasures that make criminals abandon their idea of attacking a specific system (e.g., a possible deterrent is a realistic expectation of being caught and punished).

Digital envelop The pair of encryptions that occurs the sender encrypts with the recipients' public key, both the original message and the digital signature.

Digital signatures The electronic equivalent of personal signatures on paper. They are difficult to forge since they authenticate the identity of the sender that uses the public key.

EC security strategy Multiple layers of defense that includes several methods. This defense aims to deter, prevent, and detect unauthorized entry into an organization's computer and information systems.

E-mail spam Occurs when almost identical messages are e-mailed to many recipients (sometimes millions of unsolicited e-mails).

Encryption The process of encoding data into a form (called a *ciphertext*) that will be difficult, expensive, or time-consuming for an unauthorized person to understand.

Encryption algorithm The set of procedures or mathematical algorithms used to encrypt or decrypt a message.

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

Firewalls Barriers between an internal trusted network (or a PC) and the untrustworthy Internet. Technically, it is composed of hardware and a software package that separates a private computer network (e.g., your LAN) from a public network (the Internet).

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

General controls Controls designed to protect all system applications.

Hacker Someone who gains unauthorized access to a computer system.

Hash function A secured mathematical algorithm applied to a message.

Honeynet A network of honeypots designed to attract hackers, just as bees are attracted to honey.

Honeypot Simulated information system components such as EC servers, payments gates, routers, database servers, and even firewalls that look like real working systems.

Identity theft Wrongfully obtaining and using the identity of another person in some way to commit crimes that involve fraud or deception (e.g., for economic gain).

Information assurance (IA) The performance of activities (steps) to protect information systems

and their processes against all risks. The assurance includes all tools and defense methods.

Information security Measures taken to protect information systems and their processes against all risks.

Integrity The assurance that data are accurate and that they cannot be altered.

Internet underground economy E-markets for stolen information made up of thousands of websites that sell credit card numbers, social security numbers, e-mail addresses, bank account numbers, social network IDs, passwords, and much more.

Intrusion detection system (IDS) A device composed of software and/or hardware designed to monitor the activities of computer networks and computer systems in order to detect and define unauthorized and malicious attempts to access, manipulate, and/or disable these networks and systems.

Key (key value) The secret piece used with the algorithm to encrypt (or decrypt) the message.

Key space The total universe of possible key values that can be created by a specific encryption algorithm.

Keystroke logging (keylogging) The process of using a device or software program that tracks and records the activity of a user in real time (without the user's knowledge or consent) by the keyboard keys they press.

Macro virus (macro worm) A malware code that is attached to a data file rather than to an executable program (e.g., a Word file).

Malware (malicious software) A generic term for malicious software.

Message digest The results of the hash function that is a special summary of the message converted into a string of digits.

Nonrepudiation The assurance that online customers or trading partners cannot falsely deny (repudiate) their purchase, transaction, sale, or other obligation.

Packet Segment of the data and information exchanged between computers over the Internet.

Page hijacking Illegally copying website content so that a user is misdirected to a different website.

Penetration test (pen test) A method of assessing the vulnerability of a computer system, which is done by allowing experts to act as malicious attackers.

Personal firewall A firewall that protects desktop systems by monitoring all incoming traffic to your computer.

Pharming A scam where malicious code is installed on a computer and used to redirect victims to a bogus websites without their knowledge or consent.

Phishing A fraudulent process of attempting to acquire sensitive information by masquerading as a trustworthy entity.

Plaintext A human-readable text or message.

Prevention measures Ways to help stop unauthorized people from accessing the EC system (e.g., by using authentication devices and firewalls or by using *intrusion prevention* which is, according to TechTarget "a preemptive approach to network security used to identify potential threats and respond to them swiftly").

Private key A key that only its owner knows.

Protocol tunneling Method used to ensure confidentiality and integrity of data transmitted over the Internet by encrypting data packets, and then encapsulating them in packets that can be transmitted across the Internet.

Public key A key that is known to all.

Public (asymmetric) key encryption An encryption method that uses two keys: public key and private key.

Public key infrastructure (PKI) A comprehensive framework for securing data flow and information exchange that overcomes some of the shortcomings of the one-key system.

Risk The probability that a vulnerability will be known and used.

Search engine spam The technology that enables the creation of spam sites.

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.

Spam site Pages that trick search engines into offering biased search results such so that the ranking of certain pages is inflated.

Splog Blogs created by spammers solely for advertising.

Spyware Tracking software that is installed by criminals or advertisers, without the user's consent, in order to gather information about the user and direct it to advertisers or other third parties.

Standard of due care The minimum and customary practice that a company is reasonably expected to take to protect the company and its resources from possible risks.

Symmetric (private) key encryption A scheme in which the same key is used to encrypt and decrypt the plaintext.

Trojan horse A program that seems to be harmless or even looks useful but actually contains a hidden malicious code.

Virtual private network (VPN) A network that uses the Internet to transfer information in a secure manner.

Virus Programmed software inserted by criminals into a computer to damage the system; running the infected host program activates the virus.

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.

Vulnerability assessment A process of identifying and evaluating problem areas that are vulnerable to attack on a computerized system.

Worm A software code that can replicate itself automatically (as a "standalone" – without any human intervention). Worms use networks to propagate and infect a computer or handheld device and can even spread via instant messages.

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

REFERENCES

Acohido, B. "Black Hat Shows Hacker Exploits Getting More Sophisticated." *USA Today*, August 3, 2011 (updated August 9, 2011).

Albanesius, C. "Microsoft, FBI Take Down 'Citadel' Botnet Targeting Bank Info." *PCMag.com*, June 6, 2013. **pcmag.com/article2/0,2817,2420046,00.asp** (accessed May 2014).

Apps, P., and J. Finkle. "Suspected Russian Spyware Turla Targets Europe, United States." *Reuters.com U.S. Edition*, March 7, 2014. **reuters.com/article/2014/03/07/us-russia-cyberespionage-insight-idUSBREA260YI20140307** (accessed May 2014).

Bailey, T., J. Kaplan, and A. Weinberg. "Playing War Games to Prepare for a Cyberattack." *McKinsey Quarterly*, July 2012.

BankWest. "About Us." **bankwest-sd.com/about.htm** (accessed May 2014).

BBC News Technology, Wordpress website targeted by hackers. April 15, 2013. **bbc.com/news/technology-22152296** (accessed December 2013).

BBC News Technology. "Spammers Sought After Botnet Takedown." March 25, 2011. **bbc.com/news/technology-12859591** (accessed May 2014).

Bort, J. "For the First Time, Hackers Have Used a Refrigerator to Attack Businesses." *Business Insider*, January 16, 2014.

Brooks, J. "Conficker: What It Is, How to Stop It and Why You May Already Be Protected." *eWeek,* March 31, 2009.

Cannel, J. "Cryptolocker Ransomware: What You Need to Know." October 8, 2013. **blog.malwarebytes.org/intelligence/2013/10/cryptolocker-ransom** (accessed June 2014).

Casti, T. "Phishing Scam Targeting Netflix May Trick You With Phony Customer Service Reps." *The Huffington Post Tech*, March 3, 2014a. **huffingtonpost.com/2014/03/03/netflix-phishing-scam-customer-support_n_4892048.html** (accessed May 2014).

Casti, T. "Scammers are Targeting Netflix Users Again, Preying on the Most Trusting among Us." *The Huffington Post Tech*, April 17, 2014b. **huffingtonpost.com/2014/04/17/netflix-comcast-phishing-_n_5161680.html** (accessed May 2014).

Chickowski, E. "Closing the Security Gap." *Baseline*, June 2, 2008. **baselinemag.com/c/a/Security/Closing-the-Security-Gap/** (accessed May 2014).

Cluley, G. "Phishing and Diet Spam Attacks Hit Twitter Users." *Cluley Associates Limited*, January 9, 2014. **grahamcluley.com/2014/01/phishing-diet-spam-attacks-hit-twitter-users** (accessed May 2014).

CompTIA. "Trends in Information Security: A CompTIA Analysis of IT Security and the Workforce." 2008.

Constantin, L. "Kill Timer Found in Shamoon Malware Suggests Possible Connection to Saudi Aramco Attack." *PC World*, August 23, 2012.

Cooney, M., "10 Common Mobile Security Problems to Attack." *PC World*, September 21, 2012

Cowley, S. "Former FBI Cyber Cop Worries about a Digital 9/11." July 25, 2012. **money.cnn.com/2012/07/25/technology/blackhat-shawn-henry** (accessed May 2014).

CyberSource. *13th Annual 2012 Online Fraud Report*, CyberSource Corporation (2012).

CyberSource. *14th Annual 2013 Online Fraud Report*, CyberSource Corporation (2013).

Dawn Ontario. "Virus Information: Guide to Computer Viruses." Undated. **dawn.thot.net/cd/206.html** (accessed May 2014).

Dalton, M., and A. Grossman. Arrests signal breach in 'darknet' sites, November 7, 2014. **online.wsj.com/articles/illegal-websites-seized-by-eu-u-s-authorities-1415368411** (Accessed November 2014).

Davis, M. A. "Data Encryption: Piling On." *Information Week Reports*, January 30, 2012a.

Davis, M. A. "2012 Strategic Security Survey." *Information Week*, May 14, 2012b.

Dickey, C., M. Bahari, R. Bergman, and J. Barry."The Covert War against Iran's Nuclear Program." *Newsweek*, December 13, 2010.

Dog Breed Info Center. "Examples of Scam E-Mails." Undated. **dogbreedinfo.com/internetfraud/scamemailexamples.htm** (accessed May 2014).

Drew, S. GPS loophole could allow mass smartphone hacking. August 16, 2012. **geoawesomeness.com/gps-loophole-could-allow-mass-smartphone-hacking** (accessed December 2014).

Duncan, G. "Why Haven't Biometrics Replaced Passwords Yet?" *Digital Trends*, March 9, 2013. **digitaltrends.com/computing/can-biometrics-secure-our-digital-lives/#!Qebtp** (accessed May 2014).

EMC/RSA. "2013 A Year in Review." Report # JAN RPT 0114, January 2014. **emc.com/collateral/fraud-report/rsa-online-fraud-report-012014.pdf** (accessed May 2014).

Esposito, R., and L. Ferran. "Feds: Cyber Criminals Hijacked 4 Million Computers." November 9, 2011. **abcnews.go.com/Blotter/feds-cyber-criminals-hijacked-million-computers/story?id=14915648** (accessed May 2014).

Falliere, N., and E. Chien. "Zeus: King of the Bots." Security Response White paper, Symantec, November 2009.

Finkle, J. "'Pony' Botnet Steals Bitcoins, Digital Currencies: Trustwave." *Reuters.com US Edition*, February 24, 2014. **reuters.com/article/2014/02/24/us-bitcoin-security-idUSBREA1N1JO20140224** (accessed May 2014).

Fisher, R. *The Book on Networks: Everything You Need to Know about the Internet, Online Security and Cloud Computing.* Seattle, WA: CreateSpace Independent Publishing Platform, 2014.

Fowler, G. A., and J. Valentino-DeVries. "Spate of Cyberattacks Points to Inside India." *The Wall Street Journal*, June 23, 2013.

Gandel, S. "At Financial News Sites, Stock Promoters Make Inroads." March 20, 2014. **fortunewallstreet.wordpress.com/author/stephengandelfortune/page/6** (accessed June 2014).

Gil, P. "Spyware-Malware 101: Understanding the Secret Digital War of the Internet." July 2013. **netforbeginners.about.com/od/antivirusantispyware/a/malware101.htm** (accessed May 2014).

Goldman, D. "Hacker Hits on U.S. Power and Nuclear Targets Spiked in 2012." January 9, 2013. **money.cnn.com/2013/01/09/technology/security/infrastructure-cyberattacks** (accessed May 2014).

Goldman, D. "The Real Iranian Threat: Cyberattacks." November 5, 2012. **money.cnn.com/2012/11/05/technology/security/iran-cyberattack** (accessed May 2014).

Goldman, J. "Data Breach Roundup: January 2014." February 14, 2014. **esecurityplanet.com/network-security/data-breach-roundup-january-2014.html** (accessed May 2014).

Goodchild, J. "Policy-Based Security and Access Control." April 5, 2011. **csoonline.com/article/2128022/mobile-security/case-studDOUBLEHY-PHENolicy-based-security-and-access-control.html** (accessed June 2014).

Goodchild, J. "Social Engineering: The Basics." December 20, 2012. **csoonline.com/article/2124681/security-awareness/social-engineering-the-basics.html** (accessed May 2014).

Gudkova, D. "Kaspersky Security Bulletin. Spam Evolution 2013." *Kaspersky Lab*. 2014. Available for download at **securelist.com/en/analysis/204792322/Kaspersky_Security_Bulletin_Spam_evolution_2013** (accessed May 2014).

Habal, R. "How to Assess Cloud-Based E-Mail Security Vendors." *eWeek*, September 28, 2010.

Harkins, J.M. *Spyware.* Charleston, NC: CreateSpace, 2011.

HP Enterprise Security. "2013 Cost of Cyber Crime Study: Global Report." A Ponemon Institute Research Report. October 2013. (Available for download at **hpenterprisesecurity.com/register/thank-you/2013-fourth-annual-cost-of-cyber-crime-study-global**) (accessed May 2014).

IBM. "IBM X-Force Threat Intelligence Quarterly 1Q 2014." February 2014. **public.dhe.ibm.com/common/ssi/ecm/en/wgl03045usen/WGL03045USEN.PDF** (accessed June 2014).

IBM Corporation. "IBM X-Force 2012 Mid-year Trend and Risk Report." *IBM Security Systems*, White Paper # WGE03019-USEN-00, September 2012. **public.dhe.ibm.com/common/ssi/ecm/en/wgl03014usen/WGL03014USEN.PDF** (accessed May 2014).

Jaishankar, K. (Ed.). *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. Boca Raton, Florida: CRC Press, 2011.

Jones and Bartlett Learning LLC. "Fundamentals of Information Systems Security: Unit 1 – Information Systems Security Fundamentals." 2012. **ccahs.net/Fundamentals.U1.pdf** (accessed May 2014).

Kaiser, T. "Hackers Use Refrigerator, Other Devices to Send 750,000 Spam Emails." January 17, 2014. **dailytech.com/Hackers+Use+Refrigerator+Other+Devices+to+Send+750000+Spam+Emails+/article34161.htm** (accessed May 2014).

Kalomni, R. "Dark Net 101." *Ask The Computer Guy*, June 13, 2012. **askthecomputerguy.com/opinions/dark-net-101** (accessed May 2014).

Kaplan, J., C. Rezek, and K. Sprague. "Protecting Information in the Cloud." *McKinsey Quarterly*, January 2013.

Katz, O. "Analyzing a Malicious Botnet Attack Campaign through the Security Big Data Prism." January 6, 2014. **blogs.akamai.com/2014/01/analyzing-a-malicious-botnet-attack-campaign-through-the-security-big-data-prism.html** (accessed May 2014).

Kavilanz, P. "6 Most Dangerous Cyberattacks." (Last updated November 21, 2013a). **money.cnn.com/**

gallery/smallbusiness/2013/11/21/dangerous-cyberattacks/index.html (accessed May 2014).

Kavilanz, P. "Cyberattacks Devastated My Business!" (Last updated May 28, 2013b). **money.cnn.com/gallery/smallbusiness/2013/05/28/cybercrime/index.html?iid=Lead** (accessed May 2014).

Kirk, J. "Security Company Scours 'Dark Web' for Stolen Data." *Computerworld*, September 30, 2013.

Kitten, T. "Case Study: How to Stop Scams." July 14, 2010. **bankinfosecurity.com/case-study-how-to-stop-scams-a-2748** (accessed May 2014).

Kontzer, T. "Cyber-Attacks Spur Innovative Security Approaches." *Baseline*, May/June 2011.

LabTech. "Mobile Security: Controlling Growing Threats with Mobile Device Management." *LabTech Software*, White Paper #1866272, 2012. **thinkhdi.com/~/media/HDICorp/Files/White-Papers/LabTech-Mobile-Security.pdf** (accessed May 2014).

Kravets, D. "How China's Army Hacked America." May 19, 2014 **arstechnica.com/tech-policy/2014/05/how-chinas-army-hacked-american-companies** (accessed June 2014).

Lawinski, J. "Companies Spend on Security Amid Mobile and Social Threats." *Baseline*, September 14, 2011.

Lawinski, J. "Security Slideshow: Malicious Attacks Skyrocket as Hackers Explore New Targets." *CIO Insight*, May 7, 2012.

Lenovo. "Lenovo Recommends 15 Steps to Reducing Security Risks in Enterprise Mobility." White Paper, August 2013. Available for download in .pdf format at **techrepublic.com/resource-library/whitepapers/lenovo-recommends-15-steps-to-reducing-security-risks-in-enterprise-mobility/post** (accessed May 2014).

Lerer, L. "Why the SEC Can't Stop Spam." *Forbes*, March 8, 2007.

Lyne, J. "What Justin Bieber's Twitter Hack Teaches Us about Social Media Security." March 12, 2014. **forbes.com/sites/jameslyne/2014/03/12/what-justin-biebers-twitter-hack-teaches-us-about-social-security** (accessed May 2014).

Mandalia, R. "Spammers, Phishers Increasingly Targeting Users of Social Networking Sites." December 27, 2011. **itproportal.com/2011/12/27/spammers-phishers-increasingly-targeting-users-social-networking-sites/** (accessed May 2014).

Mashable Team. "The Heartbleed Hit List: The Password You Need to Change." April 9, 2014. **mashable.com/2014/04/09/heartbleed-bug-websites-affected** (accessed June 2014).

McAfee. "Global Energy Cyberattacks: 'Night Dragon.'" White paper. Santa Clara, CA: McAfee Foundstone Professional Services and McAfee Labs, February 10, 2011. **mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf** (accessed May 2014).

McMillan, R. "90 Percent of E-Mail Is Spam, Symantec Says." *PCWorld*, May 26, 2009. **pcworld.com/article/165533/article.html** (accessed May 2014).

McNeal, A. "What's Your Fraud IQ?" *Journal of Accountancy*, August 2012. **journalofaccountancy.com/Issues/2012/Aug/20125443.htm** (accessed May 2014).

MessageLabs. "How to Defend Against New Botnet Attacks." A MessageLabs (Now Part of Symantec) White paper, 1011979. 2009.

Murray, A. C. "Omnipotent Hacker Myth Lets Business Off the Hook." *InformationWeek*, June 27, 2011. **informationweek.com/it-leadership/omnipotent-hacker-myth-lets-business-off-the-hook/d/d-id/1098580** (accessed May 2014).

Nakashima, E. "Foreign Hackers Targeted U.S. Water Plant in Apparent Malicious Cyber Attack, Expert Says." *Washington Post*, November 18, 2011. **washingtonpost.com/blogs/checkpoint-washington/post/foreign-hackers-broke-into-illinois-water-plant-control-system-industry-expert-says/2011/11/18/gIQAgmTZYN_blog.html** (accessed May 2014).

News24. "Hackers Hit Western Oil Firms." *News24.com*, February 11, 2011. **news24.com/SciTech/News/Hackers-hit-Western-oil-firms-20110211** (accessed May 2014).

Nuerm, J. *Identity Theft Manual: Practical Tips, Legal Hints and Other Secret Revealed.* Seattle, WA: Amazon Digital Services, Inc., 2012.

Nugent, J. "Classical Bank Robbery with a Cyber Twist." *Forbes.com*, November 11, 2013. **forbes.com/sites/riskmap/2013/11/08/classical-bank-robbery-with-a-cyber-twist** (accessed May 2014).

Pagliery, J. "Drug Site Silk Road Wiped Out by Bitcoin Glitch." *CNN Money*, February 14, 2014. **money.cnn.com/2014/02/14/technology/security/silk-road-bitcoin** (accessed May 2014).

Palgon, G. "Simple Steps to Data Protection." *Security Management*, June 2008. (No longer available online.)

Pate, S. "Encryption as an Enabler: The Top 10 Benefits." April 30, 2013. **networkworld.com/news/tech/2013/042613-encryption-269183.html?page=1** (accessed May 2014).

Pattison, III, W. B. *Attack of the Internet: Phishing Attempts, Pharming Scams, Swindles and Frauds.* Seattle, WA: Amazon Digital Services, Inc., 2012.

Perez, E. "Hackers Siphoned $70 Million." *Wall Street Journal,* Updated October 2, 2010.

Phneah, E. "Five Security Risks of Moving Data in BYOD Era." February 4, 2013. **zdnet.com/five-security-risks-of-moving-data-in-byod-era-7000010665** (accessed May 2014).

Pontrioli, S. "Social Engineering, Hacking the Human OS." December 20, 2013. **blog.kaspersky.com/social-engineering-hacking-the-human-os** (accessed May 2014).

Prince, B. "Kneber Botnet Highlights Trend of Social Networking Data Being Used by Hackers." *eWeek*, February 18, 2010a.

Prince, B. "Massive Check Fraud Operation Run by Hackers Revealed at Black Hat." *eWeek*, July 28, 2010b.

PWC. "Key Findings from the 2013 US State of Cybercrime Survey." June 2013. **pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/us-state-of-cybercrime.pdf** (accessed June 2014).

Rand, D. "Threats When Using Online Social Networks." CSIS Security Group, May 16, 2007. **csis.dk/downloads/LinkedIn.pdf** (accessed May 2014).

Reisinger, D. "10 Mobile Security Issues that Should Worry You." *eWeek*, February 11, 2014.

Reske, H. J., and J. Bachmann. "Lieberman Worried that Cyber Attack 'Could be Imminent.'" July 24, 2012. **newsmax.com/TheWire/cyber-attacklieberman-bill/2012/07/24/id/446429** (accessed May 2014).

Riley, M., B. Elgin, D. Lawrence, and C. Matlack. "Missed Alarms and 40 Million Credit Cards Numbers: How Target Blew It." *Businessweek.com*, March 13, 2014. **businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data** (accessed May 2014).

Rhodes-Ousley, M. *Information Security the Complete Reference*, 2nd edition. New York: McGraw-Hill, 2013.

Rubens, P. "Biometric Authentication: How it Works." August 17, 2012. **esecurityplanet.com/trends/biometric-authentication-how-it-works.html** (accessed May 2014).

Russell, K. "Here's How to Protect Yourself from the Massive Security Flaw That's Taken over the Internet." *Business Insider*, April 8, 2014.

Sarrel, M. "Stay Safe, Productive on Social Networks." *eWeek*, March 28, 2010.

Schwartz, M. J. "10 Best Ways to Stop Insider Attacks." *Information Week Dark Reading*, March 12, 2012. **darkreading.com/attacks-and-breaches/10-best-ways-to-stop-insider-attacks-/d/d-id/1103321?**(accessed May 2014).

Schwartz, M. J. "Target Breach: Phishing Attack Implicated." *Information Week Dark Reading*, February 13, 2014. **darkreading.com/attacks-and-breaches/target-breach-phishing-attack-implicated/d/d-id/1113829** (accessed May 2014).

Scott, W. *Information Security 249 Success Secrets- 249 Most Asked Questions on Information Security- What You Need to Know.* Brisbane, Queensland, Australia: Emereo Publishing, 2014.

Smith, C. "It Turns Out Target Could Have Easily Prevented Its Massive Security Breach." March 13, 2014. **bgr.com/2014/03/13/target-data-hack-how-it-happened** (accessed May 2014).

Snyder, J. "Staying One Step Ahead of Modern Hackers." *BizTech Magazine*, March 14, 2014.

Stone, B. "Sports Leagues Battle Video Pirates Showing Bootleg Live Games on Internet." February 24, 2011. **bloomberg.com/news/2011-02-24/sports-leagues-battle-video-pirates-showing-bootleg-live-games-on-internet.html** (accessed May 2014).

Suby, M. "The 2013 $(ISC)^2$ Global Information Security Workforce Study." Mountain View, CA: Frost and Sullivan, 2013.

Sullivan, D. "The Shortcut Guide to Business Security Measures Using SSL." Symantec White paper, Realtime Publishers, 2009. Available for download at **realtimepublishers.com/chapters/1562/sgbsmus-2.pdf** (accessed May 2014).

SUNY College at Old Westbury. "Website Privacy Policy Statement." 2014. **oldwestbury.edu/policy/privacy_policy.cfm** (accessed May 2014).

Swann, C. T. *Marlins Cry a Phishing Story.* Spokane, WA: Cutting Edge Communications, Inc., 2012.

Symantec. "Infographic: The State of Financial Trojans 2013." Updated January 8, 2014. **symantec.com/connect/blogs/state-financial-trojans-2013** (accessed June 2014).

Symantec. "Reducing the Cost and Complexity of Web Vulnerability Management." White Paper, Symantec Corp., 2011. **verisign.com/ssl/ssl-information-center/ssl-resources/vulnerability-management-white-paper.pdf** (accessed May 2014).

Symantec. *Symantec Report on the Underground Economy: July 07–June 08.* Symantec Corp., November 2008, Report #14525717. **eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf** (accessed May 2014).

Symantec. "Web-Based Attacks." White paper, #20016955, February 2009. **symantec.com/content/en/us/enterprise/media/security_response/whitepapers/web_based_attacks_02-2009.pdf** (accessed May 2014).

Talabis, M., and J. Martin. *Information Security Risk Assessment Toolkit: Practical Assessment through Data Collection and Data Analysis.* Maryland Heights, MO: Syngress, 2013.

Teller, T. "Social Engineering: Hacking the Human Mind." *Forbes*, March 29, 2012.

Thomson, L. (Ed.) *Data Breach and Encryption Handbook.* Chicago, IL: American Bar Association, 2012.

Timberg, C. "Foreign Regimes Use Spyware against Journalists, Even in U.S." February 12, 2014. **washingtonpost.com/business/technology/foreign-regimes-use-spyware-against-journalists-even-in-us/2014/02/12/9501a20e-9043-11e3-84e1-27626c5ef5fb_story.html** (accessed May 2014).

Wang, R. "Malware B-Z: Inside the Threat from Blackhole to Zero Access." A Sophos White Paper, Sophos Ltd., January 2013. **sophos.com/en-us/medialibrary/Gated%20Assets/white%20papers/sophos_from_blackhole_to_zeroaccess_wpna.pdf** (accessed May 2014).

Westervelt, R. "Top 10 BYOD Risks Facing the Enterprise." July 26, 2013. **crn.com/slide-shows/security/240157796/top-10-byod-risks-facing-the-enterprise.htm** (accessed May 2014).

Willhite, J. "On Alert against Cybercrime." *The Wall Street Journal Blogs – CFO Journal*, August 13, 2013. **blogs.wsj.com/cfo/2013/08/13/on-alert-against-cybercrime** (accessed May 2014).

Worley, B., "Does Your PC Have a Virus? Or Is It Just Slow?" April 4, 2012. **news.yahoo.com/blogs/upgrade-your-life/does-pc-virus-just-slow-181117610.html** (accessed May 2014).

Yadron, D. "Newest Hacker Target: Ads." *The Wall Street Journal Tech***, January 31, 2014. online.wsj.com/news/articles/SB10001424052702303743604579350654103483462 (accessed May 2014).**