E-Commerce Security and Fraud Issues and Protections

11

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. Describe the major technologies for protection of EC networks, including access control.
7. Describe various types of controls and special defense mechanisms.
8. Describe consumer and seller protection from fraud.
9. Discuss enterprisewide implementation issues for EC security.
10. Understand why it is so difficult to stop computer crimes.
11. Discuss the future of EC.

E. Turban et al., *Electronic Commerce 2018*, Springer Texts in Business and Economics, DOI 10.1007/978-3-319-58715-8_11

OPENING CASE
KANSAS HEART HOSPITAL BECOMES A VICTIM TO RANSOM

Kansas Heart Hospital of Wichita, Kansas, provides specialized comprehensive cardiovascular care to Kansas residents at its hospital and clinical services. The hospital is known for its quality surgical services, and it is well respected, except by ransom attackers.

The Incident

In May 2016, the hospital became a victim of ransomware attacks. Hackers demanded a ransom payment in order to release data which the hackers were able to lock up after they infiltrated the hospital computers (probably from outside the United States). In section "Nontechnical Methods: From Phishing to Spam and Fraud", we will present this topic, explaining the process.

In short, the hackers locked up the data files, refusing to give back access unless the hospital paid a ransom in Bitcoins (Chap. 12), to avoid tracking.

Hospitals are common targets of attacks since they have sensitive patient data. If the hackers succeed, the hospital usually pays the ransom.

(In 2016, Hollywood Presbyterian Medical Center in Los Angeles, California, paid $17,000 after a long negotiation. During the negotiation, nearly 1000 patients had to be sent to nearby hospitals.)

The attack in Kansas occurred at 9:00 pm and within minutes, hospital employees lost access to the files. Within a short time, the problem was felt throughout the hospital.

The hospital negotiated the ransom and paid the money. The hackers provided access to some, but not all, of the files, demanding more money.

Repeated attacks on hospitals are common. However, usually a second attack will be made by different hackers. This time, the same hackers had the nerve to hold some of the files. However, the hospital refused to pay.

The Solution

The hospital immediately activated a preplanned defense system.

The hackers encrypted the data in the file; the plan was ready for this, and the defense system was able to minimize the damage the encrypted malware agent was able to do.

The Results

According to the hospital, no patient information was jeopardized. The incident helped the hospital improve its defense security system.

Sources: Compiled from Newman (2016) and Sun (2016).

LESSONS LEARNED FROM THE CASE

Hackers' attacks are getting to be more innovative and sophisticated. Recently, demand for ransoms mushroomed. Hospitals are major targets for hacking. However, hospital administrators are aware of this risk and have found ways to try to protect patient information. Ransomware is only one attack method of information systems. Several other major methods are used. It is an endless war between the attackers and the defenders. A growing area closely related to e-commerce is *fraud*, which is committed by sellers, buyers, and intermediaries. This chapter provides an overview of information systems security with special attention to topics related to e-commerce.

11.1 THE INFORMATION SECURITY PROBLEM

Information security, or information systems 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 (see Kim and Solomon 2016). In this chapter, we provide an overview of some 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 and the magnitude of the problems and introduce some essential terminology of information security. For an overview, see John (2016) and Smith (2015).

What Is EC Security?

Computer security in general refers to the risks and 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, repair, or at least minimize the attacks.

Information security has been ranked consistently as one of the top management concerns in the United States and many other countries. Fig. 11.1 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.

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.

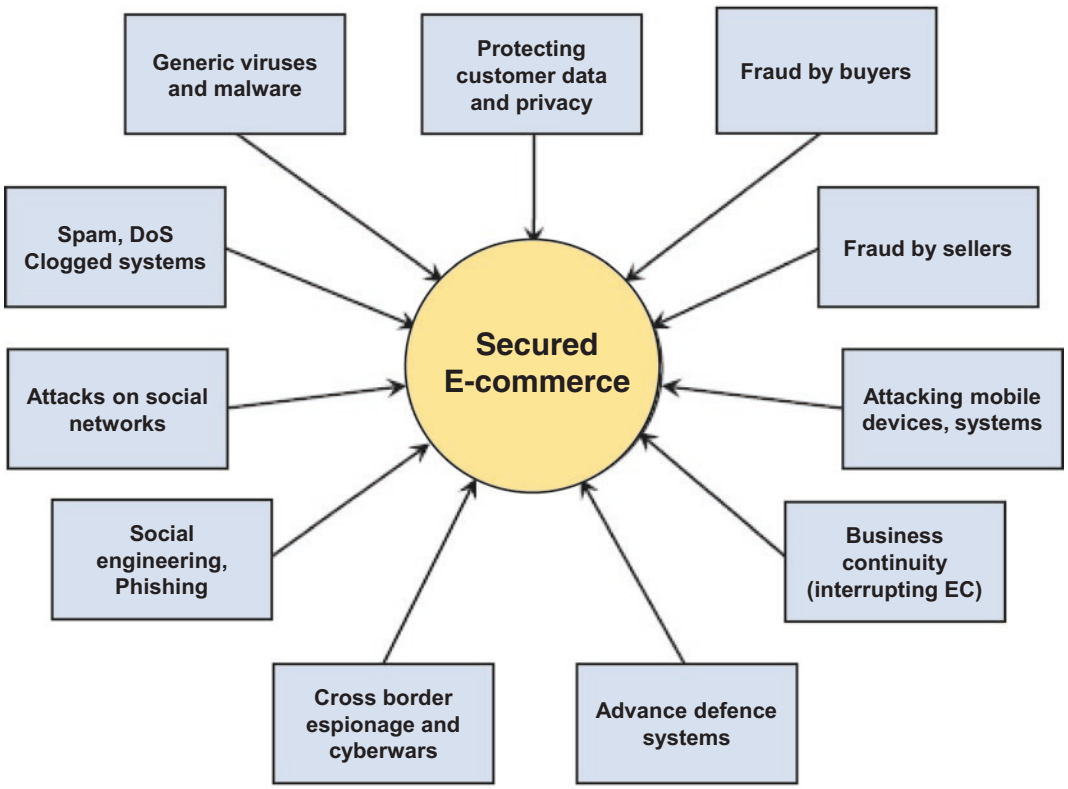

Fig. 11.1 Major EC security management concerns

Personal Security

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

National Security

Protection of US 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 cyber threats through this program.
- **United States Computer Emergency Readiness Team (US-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.

Hackers are increasingly attacking the most critical infrastructures of the United States (e.g., power, nuclear, and water facilities). They even tried to influence the US presidential elections.

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

Security Risks for 2017 and 2018

The major security risks for the near future are:

- Cyberespionage and cyberwars, including terrorist attacks, are growing threats (see Laudicina 2016 and Armerding 2016).
- Attacks are now also occurring against mobile assets, including smartphones, tablets, and other mobile devices. Enterprise mobile devices are particular targets.
- Ransomware is growing very rapidly.
- Attacks on social networks and social software tools are growing. User-generated content is a major source of malware.
- Attacks on BYOD ("bring your own device") and DOYA ("develop your own applications") are increasing.
- 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 texting, e-mail, and web content 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) is increasing.
- Attackers are using more sophisticated spyware tools.
- Attacks on new technologies such as cloud computing, IoT, and virtualization are growing.
- Attacks on mobile apps are rapidly growing.
- Fake news products and services are mushrooming.
- More analytics invite more attacks.

For more, see Olavsrud (2016).

We cover all the major topics on the above list in the rest of this chapter. The major attacks on corporations are on customers or employees' personal data, companies' strategies and plans, and on executives (plans and strategy) and sales. While most of the attacks are against large enterprises, hackers attack medium and small companies as well. Additionally, 93% of companies affected are in the healthcare, high technology, retail, banking, or IT industries. For more information, see SlideShare by Singh (2016), **sans.org**, **baselinemag.com/security**, **enisa.europa.eu/topics/threat-risk-management/risk-management**, and the Information Systems Security Certification Consortium (**isc2.org**).

Security Risks in Mobile Devices

The major security concerns of mobile devices are loss of devices that include sensitive information, data leaks, mobile devices infected by malware, theft of data from the device, users downloading malicious apps, identity theft, and other user personal loss. For more security risks for mobile commerce, see **usa.kaspersky.com/internet-security-center/threats/mobile-device-security-threats#.WKsaeG_yvIU**. This security company points to the unsecured nature of Wi-Fi, network, spoofing, phishing attacks, spyware, and broken encryption.

According to Kang (2017), the old smartphone used by President Trump for tweeting could be an opening to security threats.

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.

Cyberwarfare

According to the UN Crime and Justice Research Institute (UNICRI), *cyberwarfare* 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. According to Laudicina (2016), 2017 will be the year of cyberwarfare.

- 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). For example, in 2015, hackers attacked the German Parliament's computer network (Troinovski 2015).

According to Khanal (2016), the United States and Russia are on the brink of an open cyberwar.

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. For cyberspying on US firms by the Chinese, see Yan (2016).

Attacking Information Systems

The GhostNet attack was not an isolated case of cross-border cyberattacks. The US Congress is working on legislation to protect the country from what some call the "Cyber Pearl Harbor" attack or a digital 9/11. In May 2014, the US government named five Chinese military hackers who were responsible for stealing data and spying on several thousand companies in the United States, stealing trade secrets (Kravets 2014).

Types of Cyberwar Attacks

Cyberattacks can be classified into two major interrelated categories:

1. **Corporate espionage.** Many attacks target energy-related companies because their inside information is valuable. Almost half of all power plants and other infrastructures surveyed have been infiltrated by "sophisticated adversaries," with extortion being a common motive. 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 attackers' Internet address used was tracked back to Russia. There were suspected cyberattacks against Iranian oil production and refineries. Cyberattackers 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.

   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 US government agencies and large corporations.

   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, US 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.

Example 1

According to US Intelligence Reports, the Russians were actively involved in hacking the US Democratic Party e-mails (e.g., the DNC e-mails) during the 2016 presidential election. There was a clear attempt to influence the results of the election (see Khanal 2016).

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. For more on GhostNet, see Chalakkal (2016).

Example 3

One of the most complex cyberespionage incidents that has ever occurred is the suspected Russian spyware Turla, which was used to attack hundreds of government computers in the United States and Western Europe.

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**.

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 *underground Internet 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 Spread of Computerized Medical Data

With the requirements to computerize medical and healthcare data came the danger of breaches; see Greengard (2016a).

The Shift to Profit-Induced Crimes

There is a clear shift in the nature of the operation of computer criminals. In the early days of e-commerce, many hackers simply wanted to gain fame or notoriety by defacing websites. There are many more criminals today, and they are profit-oriented and sophisticated. Most popular is the theft of personal information such as credit card numbers, bank accounts, Internet IDs, and passwords. According to the Privacy Rights Clearinghouse (**privacyrights.org**), millions of records containing personal information are breached every year. In 2016, Yahoo! admitted that hackers stole data associated with 1 billion of its user accounts. The data that were stolen were to be sold to criminals.

Ransomware

Criminals today are even holding data for ransom and trying to extort payments from their victims. An illustrative CNN video (2:30 min) titled "Hackers Are Holding Data for Ransom" is available at **money.cnn.com/video/technology/2012/10/08/t-ransomware-hackers.cnnmoney**. In 2016, a hospital was forced to pay a ransom (with Bitcoins) to get back its data, which were not backed up (see Winton 2016). CryptoLocker is a new ransomware virus (Trojan type) used for such crimes (see **usatoday.com/story/news/nation/2014/05/14/ransom-ware-computer-dark-web-criminal/8843633**). For more on ransomware, see section "Nontechnical Methods: From Phishing to Spam and Fraud".

Thefts of Devices

Lemos (2016) provides a slideshow that illustrates the 2016 top secret trends that include ransomware and cyberspying.

Note that laptop computers, tablets, and smartphones are stolen for two reasons: selling them (e.g., to pawnshops and 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.

Computers Everywhere

As described in Chap. 7, computers are everywhere, from your home to your work, study place, entertainment area, etc. Even your car can be hacked (see Pagliery 2014b).

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 (Chap. 6) may create security problems. In addition, hackers can exploit the features of smartphones and related devices (e.g., Bluetooth) with relative ease.

The Globalization of the Attackers

Many countries have cyberattackers (e.g., China, Russia, Nigeria, Iran, and India). For an example of Iranian attacks on US banks, see Nakashima and Zapotosky (2016).

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, mobile commerce, 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. Cybercriminals change their tactics because of improved security (i.e., they are adapting quickly to a changing environment).

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 nonstandard protocols (IP addresses that are not listed). Darknet allows anonymous surfing. The darknet's contents are not accessible through Google or other search engines. The TOR technology is used in file sharing (e.g., in the well-known Pirate Bay case). The darknet is often used for political dissent and conducting illegal transactions, such as selling drugs and pirating intellectual property via file sharing. The latter activity is known as the *underground Internet economy*. In November 2014, law enforcement authorities in Europe and the United States shut down many of TOR websites. However, it seems they have not cracked TOR encryptions yet. In 2015, the US government shut down a market for stolen personal data called Darkode. See Victor (2015).

The Underground Internet Economy

The **underground Internet economy** refers to the e-markets for stolen information. These markets includes thousands of websites that sell credit card numbers, social security numbers, e-mail addresses, bank account numbers, social network IDs, passwords, and much more. Stolen data are sold to spammers or to criminals, from 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 the spammers' 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 is about a billion annually. Forty-one percent of the underground economy is in the United States, while 13% is in Romania. For a discussion of the digital underground, see Goodman (2016).

The Internet Silk Road

This was 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 United States shut down the site and arrested its founder, who was sentenced to more than 20 years in jail. However, shortly thereafter, Silk Road was "resurrected" as Silk Road 2.0.

Transactions on Silk Road are paid only by *Bitcoins* (Chap. 12). In February 2014, hackers stole over 4400 Bitcoins that were held in escrow (between buyers and sellers); over $2.7 million value of Bitcoins are gone forever (see Pagliery 2014a). The owner of the Silk Road site declared bankruptcy. However, by May 2014, the site was back in business as Silk Road 2.0 and back online in May 2016 as Silk Road 3.0.

The Cost of Cybercrime

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" 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. For an infographic regarding the cost of cyberattacks, see Alto (2016).

SECTION 10.1 REVIEW QUESTIONS

1. Define computer security.
2. List the major current security risks.
3. Describe the vulnerable design of the Internet.
4. Describe some profit-induced computer crimes.
5. Describe the dynamic nature of EC systems.
6. Describe the underground Internet economy and the darknet.

11.2 BASIC E-COMMERCE SECURITY ISSUES AND LANDSCAPE

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

Basic Security Terminology

In section "The Information Security Problem", 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: A plan that keeps the business running after a disaster occurs. Each function in the business should have a valid recovery capability plan.

Cybercrime: Intentional crimes carried out on by using the Internet.

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

Exposure: An instance of being exposed to losses from an attack that exploits vulnerability (including estimate of damages).

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

Conclusion

Cybercrime is a diversified phenomenon with many methods and potential damages. It keeps changing since criminals are getting more innovative and sophisticated. For the state of cybercrime in 2016, see the White Paper by RSA (2016).

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

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

Ransomware: A method of attack where the attacker encrypts files so the victim cannot open them unless they pay a ransom.

Risk: The probability that a vulnerability will be known and exploited.

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.

Vulnerability: Weakness in software or other mechanisms that threatens the confidentiality, integrity, or availability of an asset. It can be used directly by a hacker to gain access to a system or network.

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

Detailed definitions of these terms are provided at **webopedia.com/TERM**.

The EC Security Battleground

The essence of EC security can be viewed as a battleground between attackers and defenders of the EC and IT systems. This battleground includes the following components, as shown in Fig. 11.2:

- 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 strategies

The Threats, Attacks, and Attackers

Information systems, including EC, are vulnerable to both unintentional and intentional threats.

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, system operation, 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.

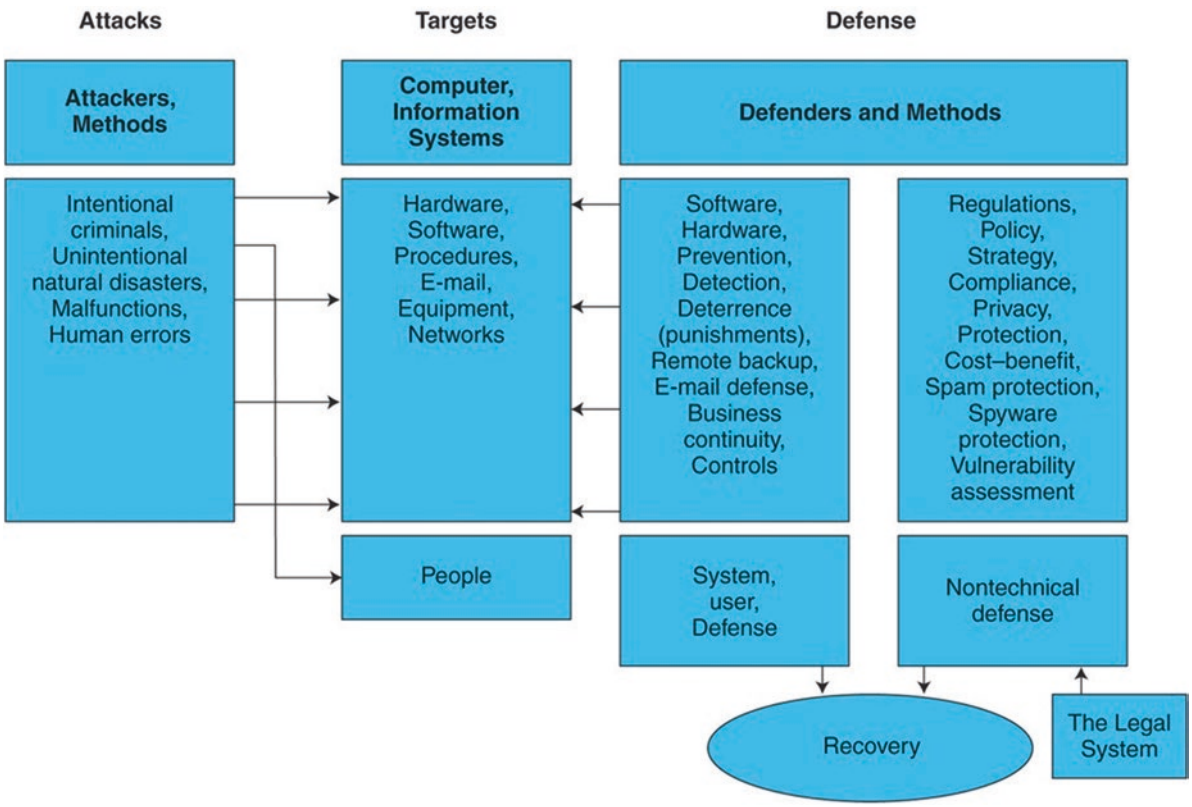

Fig. 11.2 The EC security battleground

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 sandstorms), 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.

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.

In January 29, 2017, a computer outage grounded Delta Airline flights in the United States. One hundred and fifty flights were canceled (CNN News, January 29, 2017).

Another example is Amazon's Cloud (EC2), which hosts many major websites (e.g., Reddit, Airbnb, Foursquare). In the past, the cloud hosting service crashed due to problems with the company's data centers. The crash took down Netflix, Foursquare, Dropbox, Instagram, and Pinterest due to severe weather hitting the North Virginia data center. These problems were fixed after few hours.

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 inserting 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 Sects. "Technical Malware Attack Methods: From Viruses to Denial of Service" and "Nontechnical Methods: From Phishing to Spam and Fraud". The opening and closing cases of this chapter provide examples of intentional attacks.

The Criminals and Their Methods

Intentional crimes carried out using computers and the Internet are called *cybercrimes*, which are done by *cybercriminals* (*criminals* for short) that include *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. Some hacker groups (such as the international group Anonymous) are considered unstoppable in penetrating organizations of all kinds (many US government agencies, including the US Army and the Department of Energy). The danger is that some companies may not take even minimal precautions to protect their customer information placing the blame for the attacks on the cybercriminals.

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**.

Money Mules

Hackers and crackers may recruit unsuspecting people, including company insiders, to assist in their crimes. For example, according to Malwarebytes, 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 cybercriminal. Since the mules are used to transfer stolen money, they can face criminal charges and become victims of identity theft.

Example: The Bangladesh Bank

Some hackers installed malware in the Bangladesh Central Bank computer systems that enabled them to watch, for weeks, how funds were being withdrawn from the bank's US account. The hackers then attempted to steal about $1 billion but were stopped after stealing $80 million from the reserves of Bangladesh at the Federal Reserve Bank of New York. For details, see Reuters (2016).

The Targets of the Attacks in Vulnerable Areas

As seen in Fig. 11.2, 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**). *Exposure* can result when a cybercriminal exploits a vulnerability. See 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.

Attacking Smartphones and Wireless Systems

Since mobile devices are more vulnerable than wired systems, attacking smartphones and tablets is becoming popular due to the explosive growth of mobile computing. According to Fink (2014), hackers can even steal your phone password wearing digital glasses.

The Vulnerability of RFID Chips

These chips are embedded everywhere, including in credit cards and US 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

Vulnerabilities can be of *technical nature* (e.g., unencrypted communications, insufficient use of security programs and firewalls), or they can possess *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).

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. For example, online piracy occurs when illegal software is downloaded illegally 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. For facts and statistics about online piracy around the globe, see Ernesto (2016).For additional coverage, see Chap. 15.

EC Security Requirements

Good security is a key success factor in EC.

The following set of security requirements is 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 nonrepudiation 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.

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.

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.

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 numbers 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.

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 later in this chapter.

Recovery

In security battles, there are winners and losers in each security episode, but it is difficult to win the security war. 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 check **issa.org/** and search Google.

SECTION 11.2 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 nonrepudiation?
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 is it needed?

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

There are many ways criminals attack information EC systems and users. Here, we cover only major representative methods. For an example from India (32 slides), see Singh (2016).

It is helpful to distinguish between two common types of attacks—*technical* (which we discuss in this section) and *nontechnical* ones, which we discuss in section "Nontechnical Methods: From Phishing to Spam and Fraud".

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.

Nontechnical organizational attacks are those where the security of a network or the computer is compromised (e.g., lack of proper security awareness training). We consider *financial fraud*, *spam*, *social engineering*, that includes *phishing*, *ransomware*, and other fraud methods, as *nontechnical*. Many nontechnical methods also use some malware in their attacks. 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 commit fraud and other crimes. The major nontechnical methods are described in section "Nontechnical Methods: From Phishing to Spam and Fraud". For lists of top 10 attacks by category, see **www.secpoint.com**. Then, search for virus, spyware, etc.

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 Fig. 11.3 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 Software): Viruses, Worms, and Trojan Horses

Malware is a software program 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 program or software (e.g., a virus is a "subset" of malware). Malware attacks are the most frequent security breaches. Computer systems infected by malware take orders from the criminals and do things such as send spam or steal the user's stored passwords.

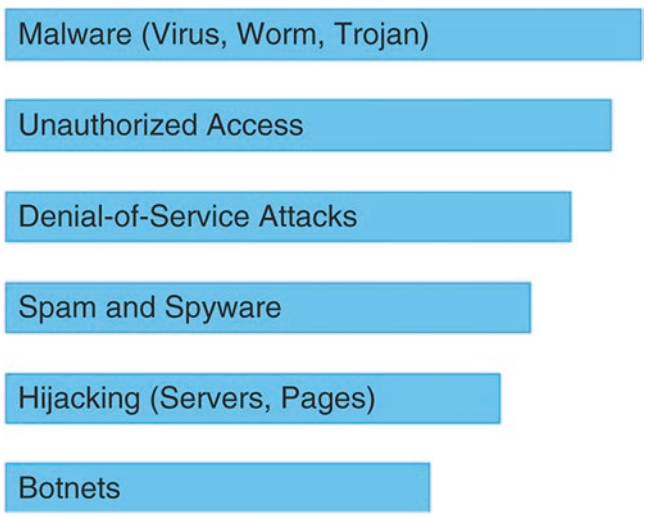

Fig. 11.3 The major technical security attack methods (in descending order of importance)

Malware includes computer viruses, worms, botnets, Trojan horses, phishing tools, spyware tools, and other malicious and unwanted software. According to Harrison and Pagliery (2015), nearly one million new malware threats are released worldwide every day.

According to Adhikari (2016), an Android malware called Gooligan breached more than one million Google accounts. The malware affected devices running Androids 4 and 5.

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 once it is activated. Sometimes a particular event triggers the virus's execution. The problem is that existing virus protection systems may not work against new viruses, and unfortunately, new viruses are created all the time. 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. In 2014, a virus by the name of "Pony" infected hundreds of thousands of computers to steal Bitcoins and other virtual currencies (see Finkle 2014). Finally, Finkle reports that a virus named Agent BTZ attacked over 400,000 computers in Russia, the United States, and Europe. This big attack was not successful, but viruses continue to spread all the time. For how computer viruses work, see **computer.howstuffworks.com/virus.htm**.

Web-based malware is very common today. Virus attacks are the most frequent computer attacks. The process of a virus attack is illustrated in Fig. 11.4.

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 the scariest viruses of 2001–2015, see Van Allen (2016). 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**).

The ILOVEYOU Virus

The ILOVEYOU virus was one of the most damaging viruses in history. It was sent via an e-mail note with "I LOVE YOU" in the subject line, and it contained an attachment that, when opened, resulted in the message being resent to everyone in the recipient's Microsoft Outlook address book and, perhaps more seriously, led to the loss of every JPEG, MP3, and certain

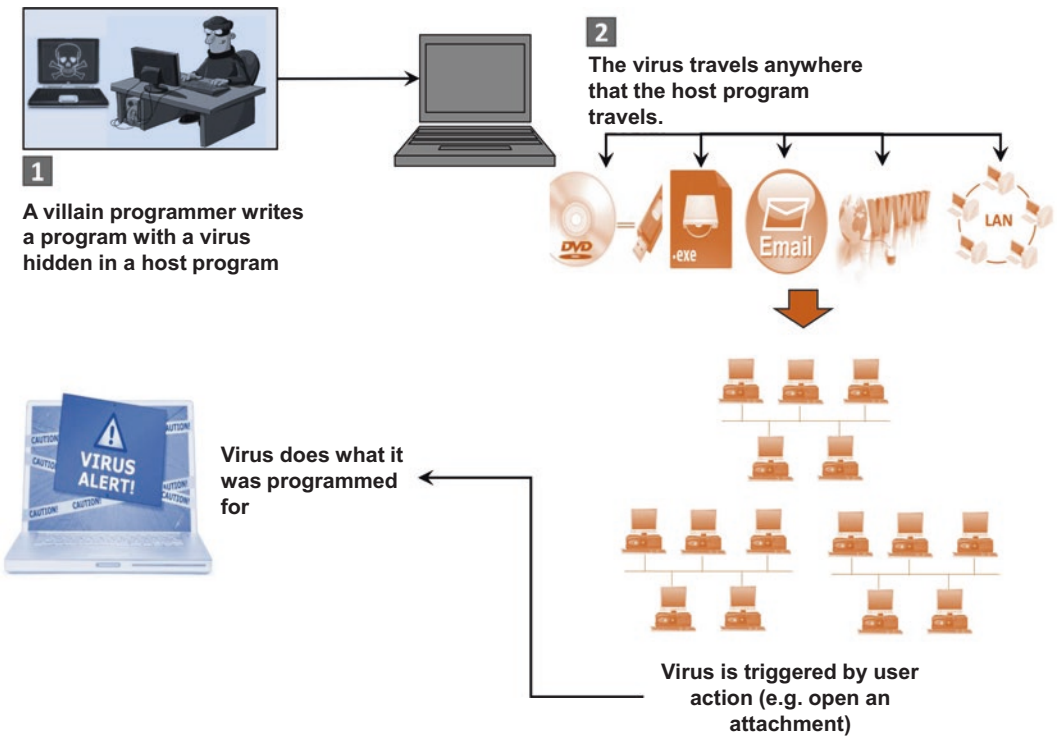

Fig. 11.4 How a computer virus can spread

other files on the recipient's hard drive. Therefore, it was able to spread rapidly from user to user within a corporation. On May 4, 2000, when the virus first showed up, it spread so quickly that e-mail had to be shut down in a number of major enterprises. The virus reached an estimated 45 million users in a single day.

One of the first steps companies used to ward off the ILOVEYOU virus was to screen out notes with ILOVEYOU in the subject line. However, the hackers quickly introduced copycat variations. The total damage was estimated at $10 billion. Other damaging viruses/worms were Code Red, Melissa, and Sasser.

Worms

Unlike a virus, a **worm** can replicate itself automatically (as a "stand-alone"—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 Micro Worms

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**. Computer programs that are very similar to viruses are worms and Trojan horses.

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

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 Wueest (2013).

Example 2: The DDOS Attacks on WordPress Corporation

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.

Some Security Bugs: Heartbleed and CryptoLocker

Two dangerous computer bugs were discovered in 2013 and 2014.

Heartbleed

According to Russell (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."

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.

CryptoLocker

Discovered in September 2013, CryptoLocker is a ransomware Trojan bug. This malware can come from many sources including e-mail attachments and 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).

Mirai (Malware)

According to Wikipedia, "**Mirai** (Japanese for "the future") is malware that turns computer systems running Linux into remotely controlled "bots" that can be used as part of a botnet in large-scale network attacks. It primarily targets online consumer devices such as remote cameras and home routers…The Mirai botnet has been used in some of the largest and most disruptive distributed denial of service (DDoS) attacks, including an attack on 20 September 2016 on computer security journalist Brian Krebs's web site,… and the October 2016 Dyn cyberattack…." (see closing case).

Denial of Service (DoS and DDoS)

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 distributed denial-of-service (DDoS) attack, which involves many devices and multiple Internet connections. For example, the attack on the Dyn (closing case) was done by thousands of computers taken hostage by the hackers. Hackers also use the IoT (Chap. 7) to capture computers and to bombard the victims; see Mello Jr. (2016). 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.

Example

On Oct 22, 2016, during the attack on Dyn (see closing case), several social networks were off for over an hour. These included Twitter, Spotify, and Reddit; see Lake (2016).

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**.

Note: In 2014, a hacking group called Lizard Stresser offered to take down any website by employing DoS, for a fee of $3 (see Goldman 2014a).

Web Server and Web Page Hijacking

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

Botnets

According to the Microsoft Safety and Security Center, a **botnet** (also known as "zombie army") is a 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.* A botnet made up of 75,000 systems infected, in 2010, with Zeus Trojan contaminated computers. Botnets are used in scams, spams, and frauds or just to damage systems. 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. Microsoft was one of the companies that helped shut down Rustock. In 2013, Microsoft and the FBI "disrupted" over 1000 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. For an analysis of malicious botnet attacks, see Katz (2014).

Home Appliance "Botnet"

The Internet of things (IoT) can also be hacked. Since participating smart home appliances (Chap. 7) 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 connected home appliances and used them to send over 750,000 malicious e-mails to enterprises and individuals worldwide (see Bort 2014).

For criminal attacks using botnets, see Mello, Jr. (2016).

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 to hide malware 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!

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.

SECTION 11.3 REVIEW QUESTIONS

1. Describe the difference between a nontechnical and a technical cyberattack.
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 malvertising.
8. Describe botnet attacks.

11.4 NONTECHNICAL METHODS: FROM PHISHING TO SPAM AND FRAUD

As discussed in section "The Information Security Problem", there has been a shift to profit-related Internet crimes. These crimes are conducted with the help of both technical tools, 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.

Note: Most of the nontechnical methods listed here use some technical malware (e.g., virus). Then, the criminals employ some nontechnical approach (e.g., psychological pressure).

Fraud can take many forms. The major ones are covered in this chapter. Some methods are a combination of technical and nontechnical (e.g., ransomware). For the global EC fraud trends, see Altshull (2017). For methods, business impacts, and solutions, see Perret (2016).

Social Engineering and Fraud

Social engineering refers to a collection of methods where criminals use human psychology to persuade or manipulate people into revealing their confidential information, or their employment 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 hackers 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 Fig. 11.5. The growth rate of unpatched vulnerabilities and the volume of e-mail, text, or Web scam/phishing activities are increasing rapidly (for predictions, see Damri 2016).

As you can see in the figure, phishers 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 Wallen (2016). In this section, we will describe how phishing, which is a subset of social engineering, is used.

Notorious hacker Kevin Mitnick, who served jail time for hacking, used social engineering as his primary method to gain access to computer systems.

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. A phisher sends an e-mail, IM, comment, or text message that appears to come from a legitimate, well-known, popular company, bank, school, or public institution. The user is instructed to enter a corrupted website, where 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 "*Marlins Cry A Phishing Story*" by Swann (2012). The process of Web-based phishing is illustrated in Fig. 11.6. For a quarterly report, see APWG (2016).

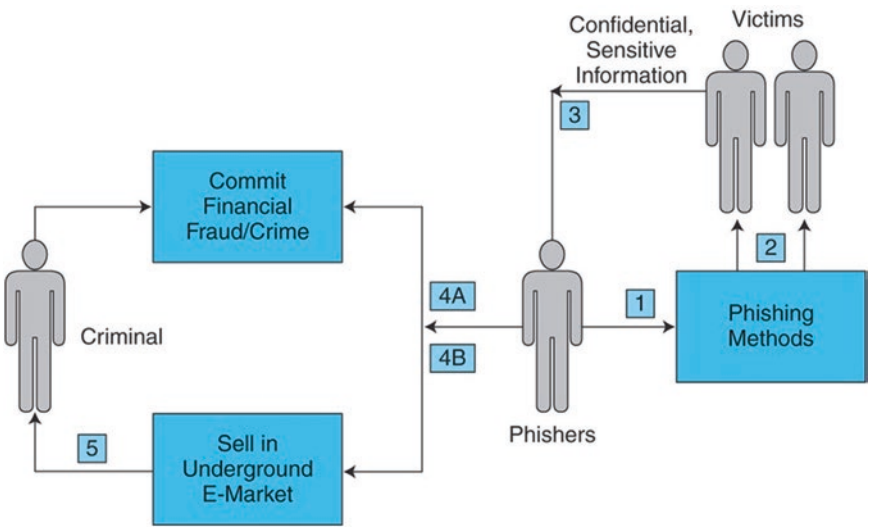

Fig. 11.5 Social engineering: from phishing to financial fraud and crime

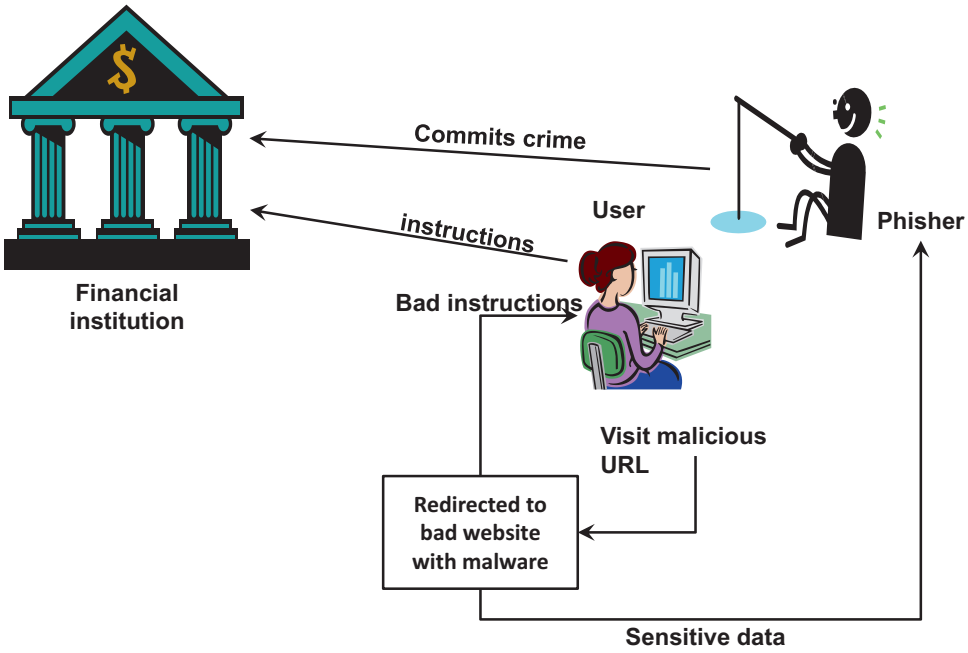

Fig. 11.6 How phishing is accomplished

Example: The Amazon 2016 Phishing Scam

According to Jones (2016b), "Just in time for the holiday shopping season, a massive email phishing scam is making the rounds. You really need to watch out for this fake Amazon email.

What's happening is people are getting emails claiming to be from Amazon, but they are actually from scammers. The email warns the recipient that there is a problem processing an order that they placed and that it will not be shipped.

It goes on to say you won't be able to access your account or place orders with Amazon until your information is confirmed. Inside the email is a malicious link that takes you to a fake Amazon page where you need to confirm your information. It asks for your name, address and all of your credit card information." Jones suggested sending the suspicious e-mail to stop-spoofing@amazon.com.

According to Shepard (2017), Amazon scams are on the rise.

For a discussion of what phishing is and how to recognize it, see **ehow.com/how_2003277_yahoo-messenger-scam.html**. See also **www.phishing.org/phishing-techniques** for how phishing works. Anti-phishing companies provide educational reports (see APWG 2016). The quarterly reports include comprehensive coverage of phishing with statistics and forecasts. Casti (2014) 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 many other companies, such as AT&T and Comcast, by drawing users to fake websites via phony sponsored ads. For 2015 phishing attacks, see Lemos (2016). See also Forrest (2016) for why phishing is getting more dangerous.

Selling stolen information, like selling any stolen goods, can be profitable and unstoppable.

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. 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).

Spear Phishing

Spear phishing is a variant of phishing that targets victims with e-mails purporting to be from colleagues, or family members, or friends. For example, a well-known spear phishing incident is one that you get from a friend that tells you that she is in another country and she was robbed of her wallet. Then, the request for money for a ticket comes so that she can return

home and return the money to you. According to Perret (2016), there is a significant increase in such attacks, especially on businesses. Another example is that you can get an e-mail, allegedly from your boss, who is traveling, to transfer money to a "client" in Korea or to e-mail the "boss" the list of customers with their e-mails. Perret (2016) presents possible solutions for both phishing and spear phishing. For the top 10 phishing scams, see **secpoint.com/top-10-spam-attacks.html**. Jones (2016c) reports that Russia's Fancy Bear, which targeted the Democratic National Commission, launched a spear phishing attack and exploited vulnerabilities in Adobe Flash and Microsoft Windows.

Other Phishing Methods

Bisson (2016) lists the following additional methods: deceptive phishing, CEO fraud, Dropbox phishing, Google Docs phishing, and pharming. Bisson also provides protection measures.

Pharming

Similar to phishing, **pharming** is a scam where malicious code installed on a computer is used to redirect victims to bogus websites without the victims' knowledge or consent. Pharming can be more dangerous than phishing since users have no idea that they have been redirected to a fake website. Pharming is directed toward 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 **en.wikipedia.org/wiki/Pharming**.

Fraud and Scams on the Internet

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.

Phishing can lead 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 **fbi.gov/scams-and-safety/common-fraud-schemes/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. Visit **dmoz.org/Society/Issues/Fraud/Internet** for a comprehensive collection of fraud resources. Mobile fraud attacks are growing rapidly; see Damri (2016). For a discussion, see section "Consumer and Seller Protection from Online Fraud".

Examples of Typical Online Fraud Attacks

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

- 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 $6000 to $10,000 and send them back the balance of $4000 to $8000. 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 min), 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 (2016).

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 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/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 posts common examples at (**dogbreedinfo.com/internetfraud/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 h 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 portion 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 **payments.mail.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! Safety (**safety.yahoo.com**).

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 ten hackers; top ten security tips and tools; pages relating to anti-phishing, anti-DoS, antispam, and more. For SecPoint IT resources for top ten spam attacks, see **secpoint.com/Top-10-Spam-Attacks.html**.

Identity Theft and Identify Fraud

Identity theft, according to the US 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 US Federal Trade Commission (**ftc.gov**), identity theft is one of the major concerns of EC shoppers. According to Safe Smart Living statistics, identity theft affects over 12 million Americans each year, (2015) for a loss of over $55 billion, and is growing about 20% annually. According to Alt (2016), over 1 billion leaked records affected 500,000 victims in June 2014. Identity thieves collect $5.8 billion each year. In addition, 19 people become victims of identity theft every minute. Finally, children are easy prey. For an entertaining comedy movie, see the 2013's "Identity Thief."

Example

According to Constantin (2016a), in January 2016, identity thieves stole 100,000 social security numbers and other personal data from the US IRS files.

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 information and protection, see **idtheftcenter.org** and **fdic.gov/consumers/assistance/protection/IdTheft.html** and Velasco (2016).

Cyber Bank Robberies

Cyberattacks can happen to individuals and organizations, including banks.

Example

Secureworks.com uncovered the following check fraud operations: Russian cybercriminals used "money mules" (people who thought they were signing up for a legitimate job), 2000 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.

Ransomware

File-encrypting ransomware programs become one of the biggest threats to organizations' networks. Unfortunately, ransomware programs are constantly evolving and get more sophisticated. Some believe that ransomware is becoming an epidemic (Greengard 2016b). The opening case is one example of an attack. According to Fitzpatrick and Griffin (2016), the FBI received 2453 complaints in 2015, where the victims paid $24 million in ransom. In 2016/2017, the magnitude of the problem is much larger. For example, security firm Malwarebytes checked over 50,000 incidents and found that Las Vegas is the most attacked region in the USA (per capita).

What Is Ransomware?

In a nutshell, criminals encrypt and lock digital files by using malware and demand a ransom before the system is unlocked. The process of ransomware is illustrated in Fig. 11.7.

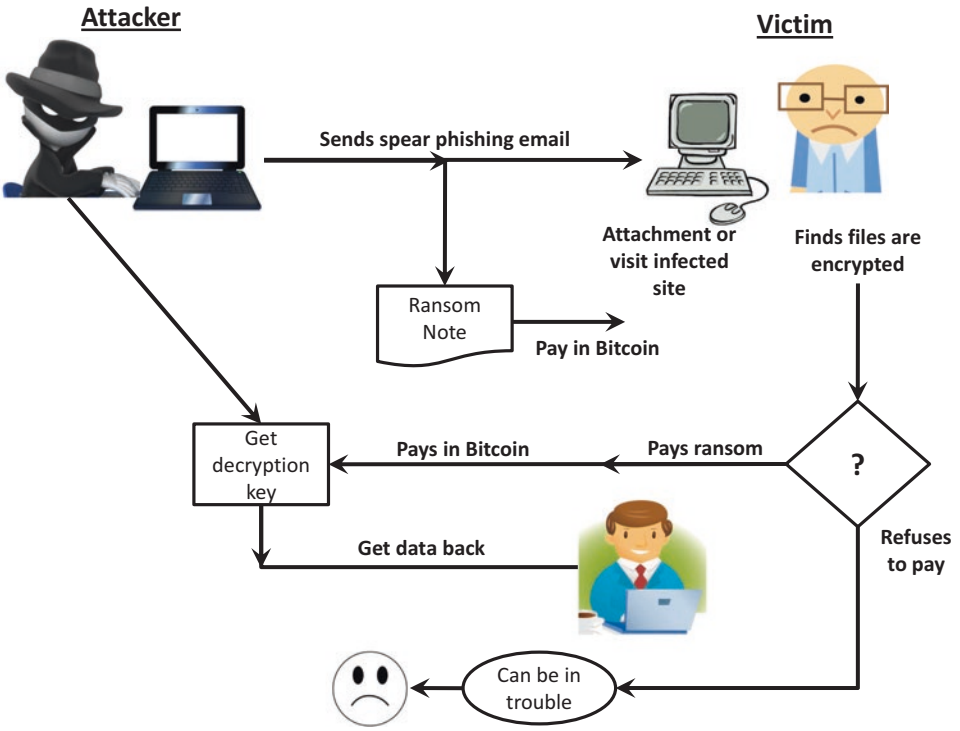

Fig. 11.7 The process of ransomware

The hackers can use an e-mail with an attachment sent to the victim. Using spear phishing or other social engineering trick, they persuade the unsuspecting employee to open the attachment, which has a virus. A few hours later, all the loosely protected files get encrypted. The data in the files are then taken hostage and a ransom demand is made.

The decryption price asked by ransomware author(s) is calculated per system locked. Payments are usually made in Bitcoins (Chap. 12). The victims need to get decryption keys for the affected systems. Otherwise, the malware may spread even further. Therefore, it is necessary to detect the malware as soon as possible before it spreads inside a network, affecting more systems.

Possible Solutions

The most obvious solutions are having a good antivirus package, good backup of the data, and well-trained users. These solutions are good, but they may not stop all hackers. Most security vendors provide additional solutions and security tips. For example, Tripwire provides 22 ransomware prevention tips at **tripwire.com/state-of-security/security-data-protection/cyber-security/22-ransomware-prevention-tips**.

Mello Jr. (2017) provides an overview of the problem and discusses solutions. For a free 2016 e-book, see Staff (2016b).

Hassell (2016) also suggests some methods to fight ransomware. The future is looking brighter. The security industry is finding new ways to block ransomware. For example, according to Constantin (2016b), machine learning (Chap. 7) could help companies react faster to ransomware. This AI method can significantly improve ransomware detection and reaction time, enabling to stop the fast spread of malware in organizations.

A special (2016) comprehensive e-book is available for free from Symantec. You can get it at **symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf**.

Example 1

Even the President of the United States can be affected by ransomware. According to Constantin (2017), "around 70 percent of the cameras hooked up to the police's closed-circuit TC (CCTV) system in Washington D.C. were reportedly unable to record footage for several days before President Donald Trump's inauguration due to a ransomware attack.

The attack affected 123 of the 187 network video recorders that form the city's CCTV system. Each of these devices is used to store video footage captured by up to four cameras installed in public spaces.

The incident occurred on January 12, 2017, eight days before the inauguration of President Trump, and it took three days to restore the system. The city refused to pay the ransom and sent teams at each site to take the affected devices offline, replace their software and restart them." If the criminal would have been clever enough and started the incident 1 day before the inauguration, the city would have had little choice but to pay the ransom or put the President at a security risk.

Example 2
Even a small company can be attacked. Bolton (2016) provides an example of a small taxi firm with 12 networked PCs in East London (UK). Malware penetrated the system via an e-mail attachment. An attempt to remove the culprit by Spy Hunter failed. A ransom of 1.2 Bitcoins was demanded. Luckily, the company was in the process of replacing the old PCs, so they did this and did not pay the ransom. Bolton's suggestions for SMEs are to (1) have an e-mail scanner and (2) back up your data frequently.

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, most of messages on corporate networks are e-mail spam. Nearly 58% of spam came from botnets; the worst botnet was called *Dotnet*. The situation is better today (2017) due to improved filtering of junk mail. Spammers can purchase millions of e-mail addresses and then 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/statistics**. Securelist is a comprehensive site that also provides descriptions of spam and viruses, a glossary, and information on threats. 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 clever and more sophisticated (e.g., see Ban 2015 for an analysis of cases). Clever spam techniques require advanced antispam technologies (Ban 2015).

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 a tracking software that is installed by criminals, 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 news and a video titled "Ethiopian Government Spying on U.S.-Based Journalists" (2:23 min) of how some regimes use spyware against journalists, see Timberg (2014).

Social Networking Makes Social Engineering Easy

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

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 networking 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 antispam 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 networking 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 a 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 Chap. 10, companies are looking for search engine optimization (SEO), which is conducted unethically by the above techniques.

Examples

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

- Instant messaging in social networks is frequently vulnerable to spam attacks.
- King (2016) describes phishing attacks on the major social networks (Facebook, Twitter, LinkedIn). These attacks have increased 150% in 1 year.

King listed the following five examples:

1. Fake customer service accounts on Twitter
2. Fake comments on popular posts
3. Fake livestream videos
4. Fake online discounts
5. Fake online surveys and contests

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. There are many purposes for data breaches. For instance, one person in the US 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 (2014b). For the most frightening data breaches, see TechRepublic Staff (2015).

The discussion so far has concentrated on attacks. Defense mechanisms, including those related to spam and other cybercrimes, are provided in section "Defending Information Systems and E-Commerce Including Mobile Systems". First, let us examine what is involved in assuring information security.

SECTION 11.4 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).
9. Describe the process of ransomware.

11.5 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 activities. For example, securing the EC 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.
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 "Basic E-Commerce Security Issues and Landscape". Some sources list more concepts (e.g., Techopedia).

To assure these attributes, e-commerce applies technologies such as encryption, digital signature, and certification. 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 Fig. 11.7, 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 Defense Side EC Systems

We organize the defense into eight categories:

1. **Defending access to computing systems, data flow, and EC transactions.** This includes 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.** This includes mainly protection 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 detection 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.
4. **Protection against social engineering and fraud.** Several defense methods are used against spam, phishing, and spyware.
5. **Disaster preparation, business continuity, and risk management.** These topics are managerial issues that are supported by software.
6. **Implementing enterprisewide security programs.** To deploy the abovementioned defense methods, one needs to use appropriate implementation strategy.
7. **Conduct a vulnerability assessment and a penetration test.** (See the following text.)
8. **Back up the data.**

For a comprehensive coverage of all aspects of information protection, see Harwood (2015).

To implement the above defense, first conduct some assessment and then plan and execute. Two possible activities are *vulnerability assessments* and *penetration tests*.

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 EC system includes online ordering, communication networks, payment gates, product database, fraud protection, and so forth. The most critical vulnerabili-

ties 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 searchmidmarketsecurity.techtarget.com/definition/vulnerability-analysis.

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 **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**. For more on penetration tests, see Maxwell (2016).

SECTION 11.5 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 eight categories of defense in EC systems.
6. Describe vulnerability assessment.
7. What is a penetration test?

11.6 DEFENDING INFORMATION SYSTEMS AND E-COMMERCE

Defending information systems regardless of their nature is similar and is described in generic IT books (e.g., by Kim and Solomon 2016).

We provide only highlights of this security, dividing it into three categories: (1) access control, encryption, and PKI; (2) security e-commerce networks; and (3) general controls, spam, pop-ups, and social engineering. In section "Consumer and Seller Protection from Online Fraud", we describe fraud protection.

Comprehensive coverage of cybersecurity threats and defense is provided by Scott in several volumes titled *Cybersecurity 101*. Volume 1 (Scott 2016a) covers mostly nontechnical areas, while Volume 2 (Scott 2016b) covers mostly technical areas. A comprehensive book regarding defense against attacks on the Web is provided by Harwood (2015).

The Defense I: Access Control, Encryption, and PKI

In this section, we describe the following topics: access control methods, biometric systems, encryption, and PKI encryption. For an overview of this area of defense, see Cloud (2015).

Access Control

Access control determines who (person, program, or machine) can legitimately use the organization's computing resources (which resources, when, and how).

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.

Antivirus Protection

A large number of companies provide basic to super protection. Some are free. Representative names are McAfee, Norton, and Kaspersky (from Symantec), Webroot, and Bitdefender, and PC Magazine and other technical publications review different products. For the best of 2017, see Rubenking (2017).

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 (e.g., used by Apple Pay).
- **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 (used by Amazon.com and Alibaba).
- **Signature recognition.** Signatures of access seekers are matched against stored authentic signatures.

In 2017, Apple was exploring two-step touch ID and facial recognition for iPhones; see Hardwick (2017).

Note that Alibaba is using facial recognition for online payments. You scan your face in front of the camera on your smartphone (see Kan 2015 for details). Amazon is using a similar system (Hinckley 2016).

Other biometric 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.** For more on biometrics, see **biometricsociety.org**.

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. For how encryption works, see **computer.howstuffworks.com/encryption.htm**.

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 "Advertising Strategies and Promotions")
- 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

Encryption has two basic options: the *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 Fig. 11.8). 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.

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 remain secret. The PKI solution is 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.

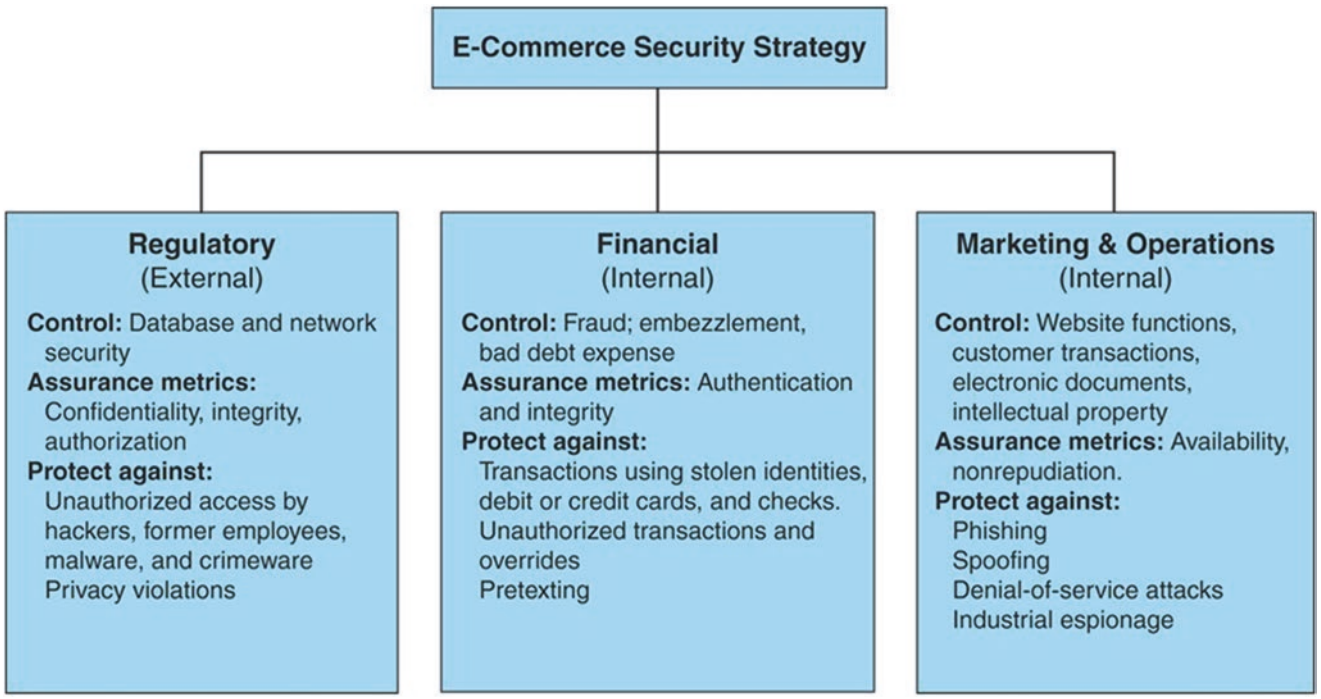

Fig. 11.8 E-commerce security strategy framework

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 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. Digital signatures are legally treated as signatures on paper. To see how a digital signature works, go to **searchsecurity.techtarget.com/definition/digital-signature**.

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.

Secure Sockets Layer (SSL)

PKI systems are further secured with SSL—a protocol for e-commerce. The PKI with SSL makes e-commerce very secure but cumbersome for users. One of the major protocols in use today is Secure Sockets 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 Controls

Several other methods are used for access control. For example, Shipley (2017) provides a list of the best DDos services of 2017 (e.g., f5, Arbor Network, Akamai, and Incapsula). Some are free.

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

The Defense II: Securing E-Commerce Networks

Several technologies exist that ensure that an organization's network boundaries are secure from cyberattack or intrusion and that if the organization's boundaries are compromised the intrusion is detected quickly and combated.

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). 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. A popular defense system is a DMZ. The DMZ can be designed in two different ways, using a single firewall or with dual firewalls. For intelligent firewalls, see Teo (2016).

The Dual-Firewall Architecture: The DMZ

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 (see Fig. 11.9). 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.

For more on DMZ and its benefits, see Mitchell (2016).

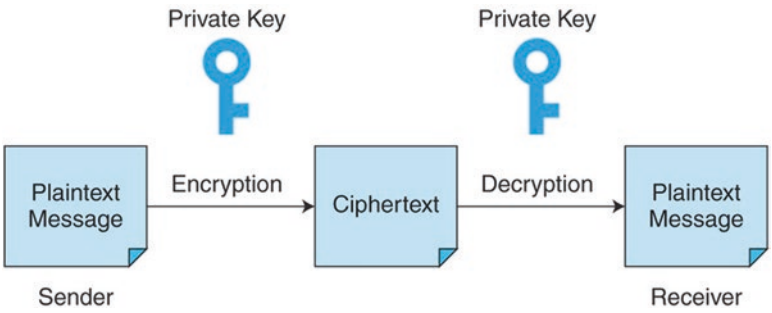

Fig. 11.9 Symmetric (private) key encryption

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.

For details on VPNs, see **searchenterprisewan.techtarget.com/definition/virtual-private-network**. For the best VPN services, see **pcmag.com/article2/0,2817,2403388,00.asp**.

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. For details, the technology, benefits, and limitations, see Parker II (2016) and **searchsecurity.techtarget.com/guides/Introduction-to-IDS-IPS-Network-intrusion-detection-system-basics**. For the future of IDS, see Guri (2016). For defeating DDos attacks, see Cisco (2014).

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.

The Defense III: General Controls, Spam, Pop-Ups, and Social Engineering Controls

The objective of IT security management practices is to defend information systems. A defense strategy requires several *controls*.

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

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

Administrative Controls

Administrative controls are defined by management and cover guidelines and compliance issuing and monitoring.

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 US 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.

Protecting Your Computer from Pop-Up Ads

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? Here are some resources:

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.

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. Thus, EC security becomes a necessity for any successful social networking initiative.

Mangis (2016) provides an interesting example of an attempt to extort money by using social engineering and locking up an individual's PC. It was a clever scam, but it failed.

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.

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.

Bisson (2016) classifies phishing into six categories and suggests a solution for each category.

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 US 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 US government is developing tools that will mine social media sites to predict cyberattacks. The tools will monitor all Facebook, Twitter, and other social networks sites to interpret content. The idea is to automate the process.

Protecting Users of Social Media

As indicated earlier, there is an increased threat to users of social media and members of social networks. It can be difficult to defend, particularly against social media impersonators who try to commit fraud. Velasco (2016) suggests the following:

- "Make use of any security settings offered by social media platforms. Examples of these include privacy settings, captcha puzzles and warning pages informing you that you are being redirected offsite.
- Do not share login info, not even with people you trust. Close friends and family might still accidentally make you vulnerable if they are using your account.
- Be wary of what information you share. Keep your personal info under lock and key, and never give out highly sensitive information like your social number or driver's license number.
- Do not reuse passwords. Have a unique password for every account you hold.
- Consider changing inessential info. You don't have to put your real birthday on Facebook.
- Only accept friend requests from people seem familiar."

Business Continuity and Disaster Recovery

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 or data.

Example: Hospital Paid Ransom After Malware Attack Because They Had No Disaster Recovery Plan
Hollywood Presbyterian Medical Center paid a ransom of $17,000 in Bitcoins (so the blackmailer/hacker could not be identified; see Chap. 12 for Bitcoins). The hacker encrypted the data that were not backed up. The hospital failed with its disaster recovery plan, so there was no choice (per the hospital management) but to pay the ransom. For details, see Jennings (2016). This case is similar to the opening case.

SANS's CIS Critical Security Controls

SANS Institute is a company that specializes in information security. The company is well known for its training, education, and certification programs. One of the company's most known projects is the "Monitoring and Measuring the CIS Critical Security." These 20 controls are the core of the recommended security configuration of computer network infrastructure. They are recommended for effective cyber defense. SANS provides a free poster that includes the highlights of the controls; see **sans.org/media/critical-security-controls/SANS_CSC_Poster.pdf**. The 20 items are the considered first priority items. The poster includes the major vendors and their products, along with a matrix that shows the degree to which the products can satisfy each of the 20 items. A description of the 20 items is available on the poster as well as at **sans.org/critical-security-controls**. Greene (2015) provides additional discussion. SANS provided case studies, Internet monitoring systems staffed by global experts, research documents, and news. A notable development is *NetWars*, a suite of interactive learning tools for simulating scenarios such as cyberattacks. NetWars is used by the US Air Force and the US Army.

Several of the critical controls (e.g., access controls, data protection, data recovery, firewalls, and penetrating tests) are discussed in this chapter.

SECTION 11.6 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. List the basic types of firewalls and briefly describe each.
11. How does a VPN work and how does it benefit users?

12. Briefly describe the major types of IDSs.
13. What are general controls? List the various types.
14. How does one protect against spam?
15. How does one protect against pop-ups?
16. How does one protect against phishing, spyware, and malvertising?
17. How does one protect against ransomware?

11.7 CONSUMER AND SELLER PROTECTION FROM ONLINE FRAUD

Internet fraud is a major problem in e-commerce and it is growing rapidly. The fraud is mostly against consumers, but there is some against sellers and merchants. Governments are especially eager to educate the public about the many types of fraud, which target senior citizen in particular. General information on what are common frauds are provided by agencies such as the FBI (see **fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud**). FBI also operates the Internet Crime Complaint Center, IC3 at **ic3.gov**. Internet fraud is a growing problem (about 25% of all consumers are victims). The problem is growing due to the blending of social commerce and e-commerce and the increase use of m-commerce (see Frenkel 2016). For an overview, see **paypal.com/us/webapps/mpp/paypal-safety-and-security**. Online fraud attacks are growing at an alarming rate in the United States, according to Meola (2016). Fraud activities exist in many formats, as discussed in section "Nontechnical Methods: From Phishing to Spam and Fraud". See also Lonergan (2016). For trends in global e-commerce fraud, see Khaitan (2016).

For 20 tips for keeping your EC website protected against hacking and fraud, see Karol (2017).

It is necessary to protect EC consumers, which the IC3 attempts to do, by informing the public about Internet scams and by publishing public service announcements.

Consumer (Buyer) Protection

Consumer protection is critical to the success of any commerce, especially electronic ones, where transactions between buyers and sellers are not face-to-face. The Federal Trade Commission (FTC) enforces consumer protection laws in the United States. The FTC provides a list of common online scams (see **onguardonline.gov/articles/0002-common-online-scams**). In addition, the European Union and the United States are attempting to develop joint consumer protection policies. For details, see the Transatlantic Consumer Dialogue website at **tacd.org**.

In 2016, the FTC released the OECD's recommendations on consumer protection in e-commerce. The recommendations aim to increase payment protection, reduce privacy and security risks, expand product safety, and encourage the use of plain language in advertising. For details, see Law Blog (2016) and **oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf**.

Representative Tips and Sources for Your Protection

A representative list follows:

- Users should make sure that they enter the real website of well-known companies, such as Walmart, Disney, and Amazon.com, by going directly to the site rather than through a link.
- Check any unfamiliar site for an address and telephone and fax numbers. Call and quiz a salesperson about the company and the products.
- Investigate sellers with the local chamber of commerce, Better Business Bureau (**bbb.org**), or TRUSTe (**truste.com**).
- Investigate how secure the seller's site is and how well it is organized.
- Examine the money-back guarantees, warranties, and service agreements before making a purchase.
- Compare prices online with those in regular stores—prices that are too low may be too good to be true.
- Ask friends what they know about the websites. Find testimonials and endorsements (be careful, some may be biased).
- Find out what remedy is available in case of a dispute.
- Consult the National Consumers League Fraud Center (**fraud.org**).
- Check the resources available at **consumerworld.org**.
- Amazon.com provides comprehensive protection. See **pay.amazon.com/us/merchant**.

In addition to these tips, consumers and shoppers also have rights on the Internet, as described in the following list of sources:

- The Federal Trade Commission (**ftc.gov**): Protecting America's Consumers. Abusive e-mail should be forwarded to spam@uce.go. For tips and advice see **ftc.gov/tips-advice**.
- The Federal Government Safety Online (**usa.gov/online-safety**)
- National Consumers League Fraud Center (**fraud.org**).
- Federal Citizen Information Center at (**gsa.gov/portal/**).
- US Department of Justice (**justice.gov**).
  - Internet Crime Complaint Center (**ic3.gov**).
- The American Bar Association provides online shopping tips at **americanbar.org/groups/business_law/migrated/safeshopping.html**.
- The Better Business Bureau (**bbb.org**).
- The US Food and Drug Administration provides information on buying medicine and medical products online (**www.fda.gov/forconsumers/protectyourself/default.htm**).
- The Direct Marketing Association (**thedma.org**).

For specific tips on how to spot fake sites and products, see Horowitz and Horowitz (2015).For fighting fake news that may include fraud, see LaCapria (2017).

Disclaimer: This is general information on consumer rights. It is not legal advice on how any particular individual should proceed. If you require specific legal advice, consult an attorney.

Third-Party Assurance Services

Several public organizations and private companies also attempt to protect consumers. The following are just a few examples.

Protection by a Third-Party Intermediary

Intermediaries who manage electronic markets try to protect buyers and sellers. A good example is eBay, which provides an extensive protection program (see eBay Money Back Guarantee (**pages.ebay.com/ebay-money-back-guarantee/**) and Dispute Resolution Center).

TRUSTe's "Trustmark"

TRUSTe (**truste.com**) is a for-profit company whose mission is to ensure that "businesses adhere to best practices regarding the collection and use of personal information on their website" (see **truste.com/about-TRUSTe/**).

The TRUSTe program is voluntary. The licensing fee for use of the Trustmark is paid by sellers, depending on the size of the online business.

Better Business Bureau

The Better Business Bureau (BBB; **bbb.org**), a nonprofit organization supported largely by membership, collects and provides reports on businesses that consumers can review before making a purchase. The BBB responds to millions of inquiries each year. The BBB also handles customer disputes against businesses.

WebTrust Seal

The WebTrust seal program is similar to TRUSTe. The American Institute of Certified Public Accountants (**aicpa.org**) sponsors it (see **webtrust.org/item64428.aspx**).

Evaluation by Consumers

A large number of sites include product and vendor evaluations offered by consumers. For example, on Yelp!, community members rate and comment on businesses.

The Computer Fraud and Abuse Act (CFAA)

The **Computer Fraud and Abuse Act (CFAA)**, passed in 1984 and amended several times, is an important milestone in EC legislation. Initially, the scope and intent of CFAA was to protect government computers and financial industry computers from criminal theft by outsiders. In 1986, the CFAA was amended to include stiffer penalties for violations, but it still only protected computers used by the federal government or financial institutions. As the Internet expanded in scope, so did the CFAA.

Seller (Merchant) Protection

The Internet also makes it easy for buyers engaging in EC to commit fraud against merchants.

For an example of how buyers attempt to trick money or goods out of sellers, see Shrubb (2015). Mellor (2016) discusses the issue and makes some suggestions for making use of available data by researching customers' profiles and behavior.

- Customers who deny that they placed an order
- Customers who download copyrighted software and sell it to others
- Customers who give fraudulent payment information (fake credit card or a bad check) for products and services that they buy
- Customers with a false identity
- Imposters—sellers using the name of another seller (see the CyberSource Annual Reports)
- Other sellers using the original seller's names, trademarks, and other unique features and even their Web addresses (or similar to it)

Sellers must be protected against:

Payment fraud by consumers and by criminals (e.g., use of invalid credit cards).

Sellers also can be attacked illegally or unethically by competitors. Merchants also are subject to piracy. This issue is described in Chap. 15.

Example

A class action lawsuit was filed against McAfee in the US District Court for the Northern District of California (Case No. 10-1455-HRL) alleging that after the plaintiffs purchased McAfee software from McAfee's website, a deceptive pop-up ad (from one of McAfee's partners) that looks like a McAfee page appeared and thanked the plaintiffs for their software purchase. The pop-up ad asked them to click on a "Try it Now" button, which they assumed would download the software they had just purchased, but unbeknownst to them, they received a 30-day trial subscription to Arpu, Inc. (a non-McAfee product). They found out later that McAfee transmits customer credit/debit card and billing information to Arpu (customers are charged $4.95 per month after the trial period) and collects an undisclosed fee for each customer who "tries" Arpu via the McAfee website.

What Can Sellers Do?

Companies like Chargeback Stopper (**chargebackstopper.com**) and Chargeback Protection (**chargebackprotection.org**) provide merchants with a database of credit card numbers that have had "chargeback orders" recorded against them. Sellers who have access to the database can use this information to decide whether to proceed with a sale. In the future, the credit card industry is planning to use biometrics to manage electronic shoplifting. In addition, sellers can use PKI and digital certificates, especially the SET protocol, to help prevent fraud.

Other possible solutions include the following:

- Use intelligent software to identify questionable customers (or in small companies, do this identification manually). One technique, for example, involves comparing credit card billing and requested shipping addresses.
- Identify warning signals—i.e., red flags—for possible fraudulent transactions.
- Ask customers whose billing address is different from the shipping address to call their bank and have the alternate address added to their bank account. Retailers will agree to ship the goods to the alternate address only if this is done.
- Ask the customer to disclose the credit card verification code.
- Delay shipment until money is received.

For security merchant terminals and EC systems, see the Report by the Retail Cyber Intelligence Sharing Center (R-CISC); see details at ISAC (2016).

For a further discussion of what merchants can do to protect themselves from fraud, see CyberSource (e.g., **www.cybersource.com/products/fraud_management**). For ten measures to reduce credit card fraud for Internet Merchants (a FraudLabs.com White Paper), see **fraudlabs.com/docs/fraudlabs_white_paper.pdf**.

Grant (2016) provides a list of the following scams against business: (1) the old switcheroo, (2) fake returns, (3) phony audit, (4) the altered, and (5) the international overpayment. Grant (2016) also suggests how to avoid these frauds and scams.

Protecting Marketplaces and Social Networking Services

Marketplaces such as eBay, Yahoo!, Amazon.com, and Alibaba face a problem of sellers who try to sell counterfeit products online. The problem is especially acute for Alibaba and eBay, whose business model is to connect sellers and buyers, in contrast with Amazon.com and other e-tailers that mostly buy products and retail them to consumers. Marketplaces try to crack down on the counterfeiter, but it is not an easy job.

Facebook and other social networks that have moved to commercialization are facing the problem of fake accounts. For the problem and solutions, see Jones (2016a).

Fraud Detection Software

A large number of software products are available to detect fraud by consumers, other businesses, compliance losses, etc. For an evaluation of the major software products, see **capterra.com/financial-fraud-detection-software**.

Protecting Both Buyers and Sellers: Using Electronic Signatures and Other Security Features

There are several methods that protect EC transactions and both the customers and sellers. For details, see Hyatt (2016).

One method to help distinguish between legitimate and fraudulent transactions is electronic signatures.

An **electronic signature** is "the electronic equivalent of a handwritten signature" (per **pcmag.com/encyclopedia/term/42500/electronic-signature**). Electronic signatures provide high level of security and are recognized by most legal entities as being equivalent to handwritten signatures. All electronic signatures are represented digitally. Signed electronic documents and contracts are as legally binding as paper-based documents and contracts.

Authentication

In the online environment where consumers and merchants do not have physical contact with one another, proving the authenticity of each person is necessary since buyers and sellers do not see each other. However, if one can be sure of the identity of the person on the other end of the line, there could be more e-commerce applications. For example, students would be able to take exams online from anywhere without the need for proctors. Fraud among recipients of government payments would be minimized. Buyers would be assured who the sellers are, and sellers would know, with a very high degree of confidence, who the buyers really are. Online job interviews would be accurate because it would be almost impossible for an applicant to impersonate another person. Overall, trust in online transactions and in EC in general would increase significantly. Authentication can be achieved in several ways, including the use of biometrics.

Fraud Detecting Systems

There are a large number of fraud detection systems such as the use of data mining for credit card fraud. CyberSource also has developed several tools for detecting fraud. For details, see CyberSource periodic reports and **authorize.net/resources/files/fdswhitepaper.pdf**.

SECTION 11.7 REVIEW QUESTIONS

1. Describe consumer protection measures.
2. Describe assurance services.
3. What must a seller do to protect itself against fraud? How?
4. Describe types of electronic signatures. Who is protected? Why?
5. Describe authentication.

11.8 IMPLEMENTING ENTERPRISEWIDE E-COMMERCE SECURITY

Güldenast (2016) recommends following these four steps: (1) define clear requirements, (2) set your standards, (3) search for flows, and (4) conduct continuous monitoring.

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. For security management in general, see Sennewald and Baillie (2015).

The Drivers of EC Security Management

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

- 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.

How Serious Is Cybersecurity?

According to Editors (2016), $1 trillion will be spent globally on cybersecurity (the defense side alone) from 2017 to 2021. Cybercrime predicted in 2016 report that cybercrimes will cost the world $6 trillion. Obviously, senior management must be involved. For comprehensive coverage of management of information security, see Whitman and Matford (2016).

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 Fig. 10.10. The model views EC security (as well as the broader IT security) as a combination of commitment and support, policies and training, procedures and enforcement, and tools, all executed as a continuous process (Figs. 11.10 and 11.11).

According to the *Delta Risk* White Paper (see Staff 2016a), the Board of Directors' involvement in cybersecurity should follow the following four key areas:

- "Ensuring that board members themselves receive cybersecurity training that is appropriate for their level and role.
- Incorporating cybersecurity protection into the organization's Statement of Risk Appetite.
- Driving the implementation of a cyber risk management program that is integrated with the institution's broader enterprise management of all risks, such as financial risk (e.g., market. liquidity, credit), compliance risk and other operational risks (e.g., fraud, litigation, reporting, safety, physical security).
- Fostering a cybersecurity throughout the institution."

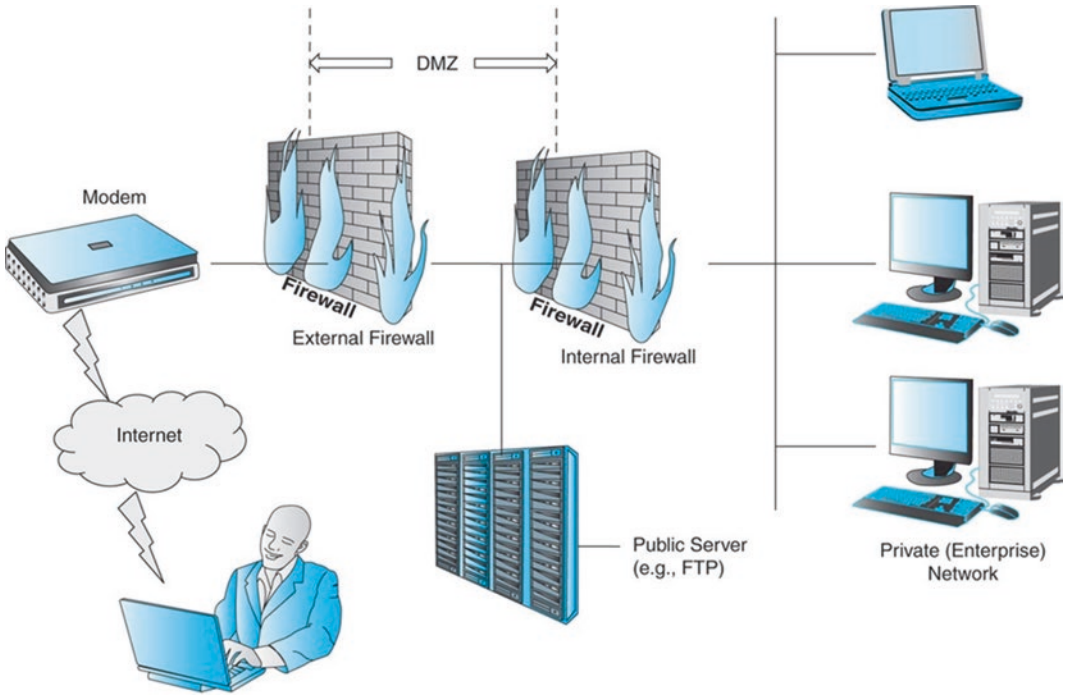

Fig. 11.10 The two firewalls: DMZ architecture

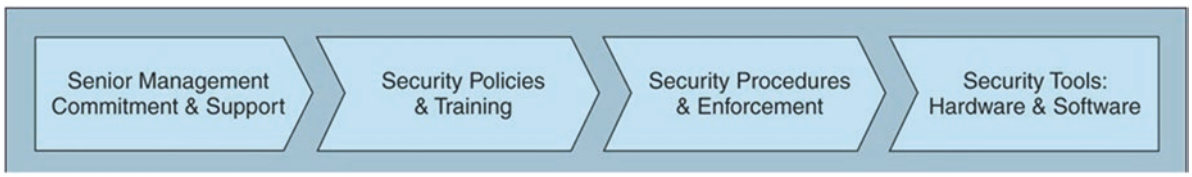

Fig. 11.11 Enterprisewide EC security and privacy process

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. Customers should:

- Know that data is being collected and when this 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

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

Training to Do Hacking

While some train people to hack in order to make money, others believe that if you learn how to hack, you will be better in defending your system. For a video that shows how to hack Facebook using phishing, see the 10-min video at **youtube.com/watch?v=Z2z9zncsYW8**.

Cyber Intelligence

According to WiseGeek (2017), "Cyber intelligence is the tracking, analyzing and countering of digital security threats. This type of intelligence is a blend of physical espionage and defense with modern information technology. Various cyber intelligence efforts help to combat viruses, hackers and terrorists that exist on the Internet with the aim to steal sensitive information. Protecting parties, like a government, from these threats is a major part of this field, but so is aggressively fighting these threats."

"One of the biggest duties of the cyber intelligence community is providing security against these digital threats. An intelligence professional will likely have a dual background in espionage and Internet security or information technology. Setting up firewalls, virus scanning programs, and routinely checking for breaches in security are important roles that keep a computer system secure from outside forces."

"Analyzing terror threats is another important aspect of cyber intelligence. This aspect of the field is most like traditional intelligence and espionage tactics of information gathering. Using third party sources, either informants or one of the many independent companies that help identify cyber threats, professionals must gather this data and determine how it threatens what is being protected. Often, creating reports and recommendations for others is more common in this area than electronic work."

According to **sans.org**, cyber intelligence 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.

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.

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 even consider using biometrics to be a violation of privacy.

Note: In 2015, the US Congress pressured President Obama to institute national biometric IDs for all Americans (Newman 2015). This suggestion is still being discussed.

Handling the privacy versus security dilemma is difficult. There are other ethical and legal obligations that may require companies to "invade the privacy" of employees and monitor their actions. In particular, IT security measures are needed to protect against loss, liability, and litigation.

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 time 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 (e.g., changing passwords).

Ignoring EC Security Best Practices

Many companies do not have prudent IT security management or employee security awareness. Many widespread threats in the United States stem from the lack of user awareness of malware and hacking attacks. In addition, many businesses do not meet security compliance standards (see Blog 2016).

Design and Architecture Issues

It is well known that preventing vulnerability during the EC design and pre-implementation stage is far less expensive than mitigating problems later; unfortunately, such prevention is not always made. Even minor design errors can increase hacking.

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. For a major survey, see PwC (2013).

Protecting Mobile Devices and Mobile Apps

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. For an overview, see Faulkner (2016). For a prediction made by Gartner Consulting, see Krishnan (2016).

Mobile Security Issues

Typical security issues range from wireless transmissions not being encrypted to lack of firewalls or passwords on mobile devices or connecting to an unsecured Wi-Fi network.

Reisinger (2014) lists additional security issues such as data theft and unlocked jailbreaking devices. The proliferation of BYOD also brings threats to the enterprise (see Faulkner 2016) and Security News (2016).

The Defense of Mobile Systems

To defend mobile systems, it is necessary to implement tools and procedures such as those described in section "Defending Information Systems and E-Commerce Including Mobile Systems" and modify them for the mobile environment. A practical checklist for reducing security risks is offered by Lenovo (2013). 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 smartphones. In 2016, this feature was still only available in California.

The Internet of Things Security

The IoT is very vulnerable to cybercrime. In the IoT, one can find a large number of devices from different manufacturers and vintages connected to one system. If the connection is via the Internet, the situation can be even worse. According to DeNisco (2017), there are a lot of security risks in the IoT. The author based his conclusion on Gartner's report. The report estimates that more than 8.4 billion devices are already connected to the Internet. Most users are individual consumers (5.2 billion devices) and enterprises 3.1 billion (devices). Cars and trucks are getting connected to the Internet as well. Gartner also predicts that by 2018, there will be 1 billion cross industry devices. All of these contribute to security risks.

McLellan (2017) provides a very comprehensive, 47-page, free report on how to harness the IoT in the enterprise (you need to register, but pay no fees, to get the report).

SECTION 11.8 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 may be 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. In addition, insiders can be victims of security crimes. Therefore, 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.
4. **What should we do in case we are victims of ransomware?** It is not good for you if you do not have a backup system. However, you may have to pay to get your data back. If a ransom is requested to avoid a DoS, quickly try to set up protection to avoid the problem spreading. In either case, report the incident to the police.

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.
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. **Security measures slow our EC transactions.** E-commerce can be greatly affected by delays and interruption of service known as *friction*. According to Mello, Jr. (2017), both ransomware and DDoS, or other security attacks, can damage EC. "Consumers do not respond well to any delays doing what they want to do online. That's why so many shopping carts are abandoned before shoppers pull the trigger on a purchase. More than two out of three carts (68.81 percent) are deserted by shoppers, according to the Baymard Institute. Friction creates a ticklish problem for security teams, because protecting merchants and consumers from fraud can create friction. Ideally, the best security scheme is one that gives consumers their cake and lets them eat it, too, one that offers maximum protection but is invisible to shoppers."
6. **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.
7. **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.
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. **Fraud on the Internet and how to protect consumers and sellers against it.** Protection is needed because there is no face-to-face contact between buyers and sellers; there is a great possibility of fraud; there are insufficient legal constraints; and new issues and scams appear constantly. Several organizations, private and public, attempt to provide the protection needed to build the trust that is essential for the success of widespread EC. Of note are electronic contracts (including digital signatures), the control of gambling, and what taxes should be paid to whom on interstate, intrastate, and international transactions. The practice of no sales tax on the Internet is changing. States are starting to collect sales tax on Internet transactions.

Many procedures are used to protect consumers. In addition to legislation, the FTC tries to educate consumers so they know the major scams. The use of seals on sites (such as TRUSTe) can help, as well as tips and measures taken by vendors. Sellers can be cheated by buyers, by other sellers, or by criminals. Protective measures include using contacts and encryption (PKI) keeping databases of past criminals, sharing information with other sellers, educating employees, and using artificial intelligence software.

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.

9. **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.

10. **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.
11. **The future of EC.** EC is growing steadily and rapidly, expanding to include new products, services, business models, and countries. The most notable areas of growth are the integration of online and offline commerce, mobile commerce (mostly due to smartphone apps), video-based marketing, and social media and networks. Several emerging technologies, ranging from intelligent applications to wearable devices, are facilitating the growth of EC. On the other hand, several factors are slowing down the spread of EC such as security and privacy concerns, limited bandwidth, and lack of standards in some areas of EC.

KEY TERMS

Access control
Application controls
Authentication
Authorization
Availability
Banking Trojan
Biometric authentication
Biometric systems
Botnet
Business continuity plan
Business impact analysis (BIA)
Certificate authorities (CAs)
CIA security triad (CIA triad)
Ciphertext
Computer Fraud and Abuse Act (CFAA)
Confidentiality
Cracker
Cybercrime
Cybercriminal
Darknet
Data breach
Denial-of-service (DoS) attack
Detection measures
Deterrent methods
Digital signature
EC security strategy
Electronic signature
E-mail spam
Encryption
Encryption algorithm
Exposure
Firewall
Fraud

General controls
Hacker
Identity theft
Information assurance (IA)
Information security
Integrity
Intrusion detection system (IDS)
Key (key value)
Keystroke logging (keylogging)
Macro virus (macro worm)
Malware (malicious software)
Nonrepudiation
Page hijacking
Penetration test (pen test)
Pharming
Phishing
Plaintext
Prevention measures
Private key
Public key
Public (asymmetric) key encryption
Public key infrastructure (PKI)
Ransomware
Risk
Search engine spam
Social engineering
Spam
Spam site
Spear phishing
Splog
Spyware
Standard of due care
Symmetric (private) key encryption
Trojan horse
Underground Internet economy
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?
7. 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.
8. Report on the status of using biometrics in mobile commerce. (Start with **nxt-id.com**.)
9. Find several definitions of "information warfare" and discuss the major attributes of the definitions.
10. What contribution does TRUSTe make to e-commerce?
11. Describe the issue of ransomware.

TOPICS FOR CLASS DISCUSSION AND DEBATES

1. 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?
2. Why is it so difficult to fight computer criminals? What strategies can be implemented by financial institutions, airlines, and other heavy users of EC?
3. 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.
4. Why is phishing so difficult to control? What can be done? Discuss.
5. Debate this statement: "The best strategy is to invest very little and only in proven technologies such as encryption and firewalls."
6. Debate: Can the underground Internet marketplace be controlled? Why or why not?
7. Debate: Is taking your fingerprints or other biometrics to assure EC security a violation of your privacy?
8. Watch the video "How to hack Facebook with phishing" (10 min, 2016). Also, learn how to protect your Facebook account.
9. Discuss the issue of providing credit card details on Facebook. Would you do it?
10. Discuss the recent security trends pointed out by Lemos (2016).
11. Examine the identity theft and identity crime topics from the FBI site **fbi.gov/about-us/investigate/cyber/identity-theft**. Report the highlights.
12. Research the state of the art of fake posting and fake comments about popular posts. Review the defense measures. Write a summary report.
13. Under what circumstances should a company pay a ransom? Debate the issue.

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 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.
5. Conduct a Google search for examples of underground Internet activities in five different countries. Prepare a summary.
6. Enter **verisign.com** (a Symantec company) and find information about PKI and encryption. Write a report.
7. Enter **hijackthis.com**. What is offered on the site? Write a report.

8. Enter **blackhat.com**. Find out what the site is about. Describe some of the site's activities.
9. Enter **ftc.gov** and identify some of the typical types of fraud and scams on the Internet. List ten of them.
10. Enter **scambusters.org** and identify and list its antifraud and anti-scam activities.

TEAM ASSIGNMENTS AND PROJECTS

1. **Assignment for the opening case**

   Read the opening case and answer the following questions:

(a) Why did the hackers attack this hospital?
(b) Research the case to find out why the hospital paid a small ransom to begin with.
(c) Why it is difficult, sometimes impossible, to find the hackers that receive a ransom?
(d) Read section "Nontechnical Methods: From Phishing to Spam and Fraud" about ransomware and the tactics hacker use.

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. Watch the video "Cyberattacks and Extortion" (13:55 min) 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?

4. 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.
5. 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.
6. Armies of botnets were used in the 2016 US presidential elections to boost candidate popularity. Is this the end of democracy? Discuss.
7. In class, watch the video how to protect yourself from fraud at **youtube.com/watch?v=gsSQqSSHrAI**. Summarize the lessons learned.

CLOSING CASE: HOW DYN WAS ATTACKED BY DDOS?

Dyn is a cloud-based Internet performance management (IPM) company that provides visibility and control into cloud and public Internet resources (an Oracle company). The company controls and optimizes infrastructure to be faster, safer, and provides more reliable service. Dyn offers domain name system (DNS) services, essentially acting as an address book for the Internet. The company serves networks with many thousands of customers each. For more on the IPM industry and Dyn, see **dyn.com/blog/what-is-internet-performance-management-industry-tech-talk-with-dyn-executive**.

The Incident

If you were on a Dyn-served network and tried to surf the Internet for buying from Amazon.com, reading news, reading some tweets, using Reddit, or trying to connect to Netflix or Spotify, you were unable to do so during most of the day on October 21, 2016, if the site was served by Dyn. Dyn's attacker, which used DDoS, targeted Dyn's headquarters in New Hampshire.

The first attack was launched at 7 am and was resolved by Dyn in about 2 h. A second attack began around noon and a third one around 4 pm. The attackers bombarded Dyn with a flood of malicious requests, sent from tens of millions of IP addresses. The result was that Dyn's Internet directory service was stopped, primarily on the East Coast of the United States and later in other parts of the country. The attack was complex and sophisticated.

The Results

According to Newman (2016), "Dyn offers Domain Name System (DNS) services, essentially acting as an address book for the Internet. DNS is a system that resolves the web addresses we see every day, like wired.com, into IP addresses needed to find and connect with the right servers so browsers can deliver requested content, (like news, finding products and prices or conducting a search). A DDoS attack overwhelms a DNS server with lookup requests, rendering it incapable of completing any. That's what makes attacking DNS so effective; rather than targeting individual sites, an attacker can take out the entire Internet for any end user whose DNS requests route through a given server."

In addition, "DDoS is a particularly effective type of attack on DNS services because in addition to overwhelming servers with malicious traffic, those same servers also have to deal with automatic re-requests, and even just well-meaning users hitting refresh over and over to summon up an uncooperative page."

Dyn experienced DDoS attacks before and successfully fought them, but they were on a much smaller scale. The scale and sophistication of this attack were too much for Dyn to defend, so access to hundreds of sites and services has been disrupted by the attack. This attack highlights how critical DNS is to maintaining stable and secure Internet service.

Using Botnet

The attacker hijacked thousands of Internet-connected computing devices and appliances (e.g., DVRs, routers, home appliances) which are not so secured and infected them with malware. The infected devices became part of a botnet (section "Technical Malware Attack Methods: From Viruses to Denial of Service") that drove malicious traffic to Dyn. The major malware was Mirai (see section "Technical Malware Attack Methods: From Viruses to Denial of Service"). Note that the attackers hijacked devices that were connected to the Internet of things. The botnet addition is the "distributed" part of DDoS, and the attack was the largest of its kind in history.

The Motive

The question is why the attackers attacked Dyn. In many DDoS and DoS attacks, a ransom is requested. Not this time. Maybe the attackers wanted to punish Dyn because the attackers failed previously in small-scale attacks. Other DDoS attacks were done to "show off," were used for protesting against companies, and were used in cyberwars and for intimidation and extortion. The motive in the case of Dyn is not really known. Some speculate that the perpetrators were most likely mad at Dyn for helping Brian Krebs be identified, and the FBI arrested two Israeli hackers who were running a DDoS-for-hire ring.

Sources: Compiled from Newman (2016), Blaine (2016), Gallagher (2016), and Krebs (2016).

Questions

1. Why did the hackers recruit innocent computers and create a botnet?
2. Explain why Dyn was unable to counter the attack.
3. Explain the role of DSN in the IPM process.
4. Relate the case to conducting business on the Internet.
5. Relate the case to IoT.

REFERENCES

Adhikari, R. "Gooligan Ransacks More than 1M Android Accounts." *TechNewsWorld*, December 2, 2016.
Alt, K. "7Alarming Identity Theft Statistics." *Safesmartliving.com*, June 15, 2016.
Alto, P. "Infographic: The Real Cost of Cyberattacks." *Enterprise Innovation*, March 21, 2016.

Altshull, Y. "Global eCommerce & Fraud Trends for 2017." *Riskified.com*, January 12, 2017.
APWG. "Phishing Activity Trends Report." *APWG.org/Reports*, (July-Sept., 2016), December 20, 2016. **docs.apwg.org/reports/apwg_trends_report_q2_2016.pdf** (accessed March 2017).
Armerding, T. "Top 15 Security Predictions for 2016." *CSO News*, April 15, 2016.
Ban, E. "Spammers Getting More Clever-An Analysis of Recent Spam Attacks." *OEM Hub*, June 25, 2015. **oem.hub.bitdefender.com/spammers-getting-more-clever-analysis-spam-attacks** (accessed February 2017).
Bisson, D. "6 Common Phishing Attacks and How to Protect Against Them." *Tripwire*, June 5, 2016.
Blaine, G. "DDoS Attack on Dyn Reveals New Threat Actor Strategies." *AIO Networks, Inc*., October 21, 2016.
Blog. "Does Your Business Meet IT Security Compliance Standards?" *Guardian Data Destruction*, March 13, 2016.
Bolton, D. "A Case Study in Dealing with Ransomware." *Dice.com*, June 7, 2016. **insights.dice.com/2016/06/07/a-case-study-in-dealing-with-ransomware** (accessed February 2017).
Bort, J. "For the First Time, Hackers Have Used a Refrigerator to Attack Businesses." *Business Insider*, January 16, 2014.
Cannell, J. "Cryptolocker Ransomware: What You Need to Know." *Malwarebytes Labs*, October 8, 2013. **blog.malwarebytes.org/intelligence/2013/10/cryptolocker-ransom** (accessed February 2017).
Casti, T. "Phishing Scam Targeting Netflix May Trick You with Phony Customer Service Reps." *The Huffington Post Tech*, March 3, 2014. **huffingtonpost.com/2014/03/03/netflix-phishing-scam-customer-support_n_4892048.html** (accessed February 2017).
Chalakkal, S. "Study of Ghostnet." *University of Berlin*, April 2016. **priyachalakkal.files.wordpress/2016/06/ghostnet_sreepriyachalakkal.pdf** (accessed February 2017).
Cisco. "Defeating DDOS Attacks." *White Paper*, January 23, 2014.
Cloud, J. *Internet Security: Online Protection from Computer Hacking*. North Charleston, USA: CreateSpace Publishing Platform, 2015.
Constantin, L. "Identity Thieves Obtain 100,000 Electronic Filing PINs from IRS System." *IDG News Service*, February 10, 2016a.
Constantin, L. "Machine Learning could Help Companies React Faster to Ransomware." *IDG News Service*, June 13, 2016b.
Constantin, L. "Ransomware disrupts Washington DC's CCTV system." *IDG News Service*, January 30, 2017.
CyberSource. "Annual Fraud Benchmark Report: A Balancing Act." 2016. **NA_2016_Fraud_Benchmark_Report.pdf** (accessed March 2017).
Damri, L. "E-Commerce Fraud Predictions for 2017." *Internet Retailer*, October 20, 2016.
Dawn Ontario. "Virus Information: Guide to Computer Viruses." Undated.
DeNisco, A. "There Will Soon Be More IoT Devices in the World than People, Security Risks Abound." *TechRepublic.com*, February 7, 2017.
Editors. "Cybersecurity Market Report." *CyberSecurity Ventures*, Q4 2016.
Ernesto. "Europe Has The Highest Online Piracy Rates, By Far." *Torrentfreak*, August 1, 2016.
Faulkner, A. "Protecting Against the Top Mobile Security Threats in 2016." *RCA Conference Paper*, February 10, 2016. **rsaconference.com/blogs/protecting-against-the-top-mobile-security-threats-in-2016** (accessed February 2017).
Fink, E. "Google Glass Wearers Can Steal Your Password." *CNN News*, July 7, 2014. **money.cnn.com/2014/07/07/technology/security/google-glass-password-hack** (accessed February 2017).
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 February 2017).
Fitzpatrick, D. and D. Griffin. "'Ransomware' crime wave growing." *CNNTech*, April 4, 2016.
Forrest, C. "Phishing Gets More Dangerous: New Report Analyzes the Weapons of Choice." *TechRepublic*, January 27, 2016.
Frenkel, K. A. "2016 Has the Markings of a Perfect Storm for Fraud." *CIO Insight*, January 28, 2016.
Gallagher, S. "DoS Attack on Major DNS Provider Brings Internet to Morning Crawl [updated]." *ARS Technica*, October 21, 2016.
Goldman, D. "Take Down Any Website for $3." *CNN Tech*, December 31, 2014a. **money.cnn.com/2014/12/31/technology/lizard-squad-attack** (accessed April 2016).
Goldman, J. "Data Breach Roundup: January 2014." *eSecurity Planet*, February 14, 2014b. **esecurityplanet.com/network-security/data-breach-roundup-january-2014.html** (accessed February 2017).
Goodman, M. *Future Crimes: Inside the Digital Underground and the Battle for our Connected World.* New York, NY: Anchor Reprint, 2016.
Grant, E. "How to Avoid Frauds & Scams Targeting Ecommerce Businesses." *Ecommerce Platforms*, June 20, 2016.
Greene, T. "SANS: 20 Critical Security Controls You Need to Add: A List of the Controls You Need Plus How to Implement Them." *NetworkWorld*, October 13, 2015. **networkworld.com/article/2992503/security/sans-20-critical-security-controls-you-need-to-add.html** (accessed February 2017).
Greengard, S. "Breaches of Health Care Data: A Growing Epidemic." *Baseline*, February 12, 2016a.
Greengard, S. "Is Ransomware Becoming an Epidemic?" *Baseline*, August 8, 2016b.
Güldenast, G. "Four Steps to a Secure E-Commerce Solution." *Service Plan*, October 12, 2016.
Guri, M. "The Future of Intrusion Detection." *Help Net Security*, June 16, 2016.
Hardwick, T. "Apple Exploring Two-Step Touch ID and Facial Recognition System for iPhone 8." *MacRumors.com*, January 21, 2017.
Harrison, V., and J. Pagliery. "Nearly 1 Million New Malware Threats Released Everyday." *CNN Tech*, April 14, 2015. **money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security** (accessed February 2017).
Harwood, M. *Internet Security: How to Defend Against Attackers on the Web (Jones & Bartlett Learning Information Systems Security & Assurance)*. 2nd ed. Burlington, MA: John Bartlett Learning, 2015.
Hassell, J. "Fighting Ransomware: A fresh look at Windows Server approaches." *Computer World*, December 8, 2016.
Hinckley, S. "Pay by Selfie? Amazon Says Your Portrait Can Protect Online Purchases." *Christian Science Monitor*, March 15, 2016.
Horowitz, D., and A. Horowitz. "Online Merchandise Scams Target Students." *The Costco Connection*, December 2015.
Hyatt, P. "How to protect your company and customers in e-commerce transactions." *TradeReady.com*, July 29, 2016.
ISAC. "Securing Merchant Terminals and Ecommerce Systems." *R-CISC, TLP White Alert*, December 2016.
Jennings, R. "This Hollywood Hospital Didn't Backup Its Data? 'Ransomware' Payday for Evil Hackers." *Computerworld*, February 18, 2016.
John, A. *Internet Security*. Publisher: Self- Publishing, 2016.
Jones, M. "Facebook Tests Tool that Identifies Fake Accounts." *Value Walk*, March 24, 2016a.
Jones, M. "New Amazon Phishing Scam Spreading Like Wildfire!" *Komando.com*, November 18, 2016b.

Jones, D. "Russia's Fancy Bear Attacks Microsoft, Adobe as Election Nears." *Tech News World*, November 4, 2016c. **technewsworld.com/story/84059.html** (accessed February 2017).
Kan, M. "Alibaba Uses Facial Recognition Tech for Online Payments." *Computerworld*, March 16, 2015.
Kang, C. "That Old Phone Trump Uses for Twitter Could Be an Opening to Security Threats." *The New York Times*, January 25, 2017.
Karol, K. "20 Simple Tricks to Secure Your WordPress Website in 2017." *Codeinwp*, January 7, 2017.
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 February 2017).
Khaitan, S. "2016 Trends in Global E-Commerce Fraud." *Rippleshot*, July 21, 2016.
Khanal, S. "U.S. & Russia on the Brink of an Open Cyber War: What to Expect?" *Inquisitr*, December 17, 2016. **inquisitr.com/3804493/cyber-war-us-russia-obama-putin-hacking** (accessed February 2017).
Kim, D. and M. G. Solomon. *Fundamentals of Information Systems Security*. 3rd edition. Burlington, MA: Jones & Barlett Learning, 2016.
King, H. "Top 5 social media scams to avoid." *CNN News*, April 22, 2016. **money.cnn.com/2016/04/22/technology/facebook-twitter-phishing-scams** (accessed February 2017).
Kravets, D. "How China's Army Hacked America." *ARS Technica*, May 19, 2014. **arstechnica.com/tech-policy/2014/05/how-chinas-army-hacked-american-companies** (accessed February 2017).
Krebs, B. "Hacked Cameras, DVRs Powered Today's Massive Internet Outrage." *KrebsonSecurity.com*, October 21, 2016.
Krishnan, S. "It Starts Now: 2017 Mobile Security Predictions from Gartner." *Lookoutblog.com*, December 1, 2016. **blog.lookout.com/blog/2016/12/01/gartner-mobile-security-predictions** (accessed February 2017).
LaCapria, K. "Snopes' Field Guide to Fake News Sites and Hoax Purveyors." *Snopes.com*, January 25, 2017.
Lake, E. "Anti-Social Twitter, Spotify and Reddit among Social Media Sites Taken Offline After Major Cyber Attack." *The SUN*, October 21, 2016.
Laudicina, P. "2017 Will Be the Year of Cyber Warfare." *Forbes.com*, December 16, 2016.
Law Blog. "FTC Releases OECS's Recommendation on Consumer Protection in E-Commerce." *Hunton Privacy Blog*, April 7, 2016.
Lemos, R. "Phishing Attacks Continue to Sneak Past Defenses." *eWeek*, February 11, 2016.
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-recommend-15-steps-to-reducing-security-risks-in-enterprise-mobility/post** (accessed March 2017).
Lonergan, K. "The Seven Types of E-Commerce Fraud Explained." *Information Age*, April 15, 2016.
Mangis, C. "How My Neighbor Beat a Social-Engineering Scam." *PCMagazine.com*, June 21, 2016.
Maxwell, D. *Hacking: Bootcamp--How to Hack Computers, Basic Security and Penetration Testing (Hacking The Common Core)*. [Kindle Edition] Seattle, WA: Amazon Digital Services, 2016.
McLellan, C. "Harnessing IoT in the Enterprise." *ZdNet Special Feature*, February 1, 2017. **zdnet.com/topic/harnessing-iot-in-the-enterprise** (accessed March 2017).
Mello, Jr. P. "Cyber Grinches Could Disrupt Holidays' Biggest Shopping Weekend." *TechNewsWorld*, November 23, 2016. **ecommercetimes.com/story/84109.html** (accessed February 2017).
Mello, Jr. P. "Las Vegas Capture Ransomware Crown." *TechNewsWorld*, January 7, 2017. **ecommercetimes.com/story/84211.html** (accessed February 2017).
Mellor, R. "Managing Fraud in E-Commerce: Is your Online Business Bulletproof?" *Security*, July 12, 2016.
Meola, A. "Online Fraud Attacks in the U.S. Are Growing at an Alarming Rate." *Business Insider*, April 20, 2016.
Mitchell, B. "DMZ-De-Militarized Zone (Computer Networking)" *Lifewire*, April 30, 2016.
Nakashima, E., and M. Zapotosky. "U.S. Charges Iran-Linked Hackers with Targeting Banks, N.Y. Dam." *The Washington Post*, March 24, 2016.
Newman, A. "Congress Pushes Obama-Backed National Biometric ID for Americans." *News American*, March 28, 2015.
Newman, L.H. "What We Know About Friday's Massive East Coast Internet Outage." *Wired*, October 21, 2016.
Olavsrud, T. "9 Biggest Information Security Threats through 2018." *CIO*, March 22, 2016.
Pagliery, J. "Drug Site Silk Road Wiped Out by Bitcoin Glitch." *CNN Tech*, February 14, 2014a. **money.cnn.com/2014/02/14/technology/security/silk-road-bitcoin** (accessed April 2016).
Pagliery, J. "Your Car Is a Giant Computer- and It Can Be Hacked." *CNN Money*, June 2, 2014b. **money.cnn.com/2014/06/01/technology/security/car-hack** (accessed February 2017).
Parker II, C. "Intrusion Detection Systems (IDS): Finally for the Vehicles: *National Cybersecurity Institute*, August 19, 2016.
Perret, D. "E-commerce Security Issues: Phishing and Spear Phishing." *Vade Secure*, March 17, 2016.
Pontrioli, S. "Social Engineering, Hacking the Human OS." *Kaspersky Lab Daily*, December 20, 2013. **blog.kaspersky.com/social-engineering-hacking-the-human-os** (accessed February 2017).
PWC. "Key Findings from the 2013 U.S. State of Cybercrime Survey." June 2013. **pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/us-state-of-cybercrime.pdf** (accessed February 2017).
RSA. "2016: Current State of Cybercrime- RSA." **rsa.com/content/dam/rsa/PDF/2016/05/2016-current-state-of-cybercrime.pdf** (accessed February 2017).
Reisinger, D. "10 Mobile Security Issues that Should Worry You." *eWeek*, February 11, 2014.
Reuters. "Malware Suspected in Bangladesh Bank Heist." *Fortune.com*, March 12, 2016. **fortune.com/2016/03/12/malware-bangladesh-bank-heist** (accessed February 2017).
Rubenking, N. J. "The Best Antivirus Protection of 2017." *PCMag.com*, January 13, 2017.
Russell, K. "Here's How to Protect Yourself from the Massive Security Flaw That's Taken over the Internet." *Business Insider*, April 8, 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 February 2017).
Scott, J. *Cybersecurity 101: What You Absolutely Must Know! - Volume 1: Learn How Not to be Pawned, Thwart Spear Phishing and Zero Day Exploits, Cloud Security Basics and Much More.* [Kindle Edition] Seattle, WA: Amazon Digital Services, 2016a.
Scott, J. *Cybersecurity 101: What You Absolutely Must Know! - Volume 2: Learn JavaScript Threat Basics, USB Attacks, Easy Steps to Strong Cybersecurity, Defense Against Cookie Vulnerabilities, and Much More!* [Kindle Edition] Seattle, WA: Amazon Digital Services, 2016b.

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.
Security News. "Security 101: Protecting your BYOD Environment." *VIPRE News*, November 5, 2016. **blog.vipreantivirus.com/viper-for-business/security-101-protecting-byod-environment** (accessed February 2017).
Sennewald, C. and C. Baillie. *Effective Security Management*, 6th edition. Oxford, UK: Butterworth-Heinemann, 2015.
Shepard, W. "Amazon Scams on the Rise in 2017 as Fraudulent Sellers Run Amok and Profit Big." *Forbes.com*, January 2, 2017.
Shipley, R. "The Best DDoS Protection Services of 2017." *Top10reviews.com*, January 24, 2017.
Shrubb, R. "How Do You Beat Bad Buyers on Amazon and eBay." *WebRetailer*, December 7, 2015.
Singh, I. "E Commerce-Security Threats and Challenges." *SlideShare* (32 slides), February 15, 2016. **slideshare.net/InderBarara1/ecommerce-security-threats-and-challenges-58271913/** (accessed February 2017).
Smith, C. "It Turns Out Target Could Have Easily Prevented Its Massive Security Breach." *BGR Media*, March 13, 2014. **bgr.com/2014/03/13/target-data-hack-how-it-happened** .(accessed February 2017).
Smith, R. *Elementary Information Security*. 2nd Edition, Burlington, MA: Jones Bartlett, 2015.
Staff. "Cybersecurity and the Board of Directors." A White Paper, *Delta Risk*, April 2016a.
Staff. "eBook: Defending Against Crypto Ransomware." *Help Net Security*, August 16, 2016b. **helpnetsecurity.com/2016/08/16/ebook-defending-crypto-ransomware** (accessed March 2017).
Sun, D. "Hackers Demand Ransom Payment from Kansas Heart Hospital for Files." *News KWCH12*, May 20, 2016.
Swann, C. T. *Marlins Cry a Phishing Story.* Spokane, WA: Cutting Edge Communications, Inc., 2012.
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 February 2017).
TechRepublic Staff. "The 15 Most Frightening Data Breaches." *TechRepublic*, October 29, 2015.
Teo, F. "Monitoring Your Internal Network with Intelligent Firewalls." *Enterprise Innovation*, January 19, 2016.
Timberg, C. "Foreign Regimes Use Spyware against Journalists, Even in U.S." *Washington Post*, 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 February 2017).
Troinovski, A. "German Parliament Struggles to Purge Hackers from Computer Network." *The Wall Street Journal*, June 12, 2015.
Van Allen, F. "The 18 Scariest Computer Viruses of All Time." *TechRepublic*, January 22, 2016.
Velasco, J. "4 Case Studies in Fraud: Social Media and Identity Theft." *Socialnomics*, January 13, 2016.
Victor, D. "Authorities Shutdown Darkode, a Marketplace for Stolen Personal Data." *New York Times*, July 15, 2015.
Wallen, J. "10 Social Engineering Exploits Your Users Should Be Aware Of." *TechRepublic*, January 27, 2016. **techrepublic.com/blog/10-things/10-social-engineering-ploys-your-users-should-be-aware-of** (accessed February 2017).
Wang, R. "Malware B-Z: Inside the Threat from Blackhole to ZeroAccess." 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 February 2017).
Whitman, M.E. and H. Mattord. *Management of Information Security*, 5th edition. Boston: MA: Cengage Learning, 2016.
Winton, R. "Hollywood Hospital Pays $17,000 in Bitcoin to Hackers: FBI Investigating." *Los Angeles Times*, February 18, 2016.
WiseGeek. "What is Cyber Intelligence? (with pictures)." *WiseGeek.com*, January 29, 2017. **wisegeek.com/what-is-cyber-intelligence.htm** (accessed March 2017).
Wueest, C. "The State of Financial Trojans 2013." *Symantec Official Blog*, December 17, 2013. **symantec.com/connect/blogs/state-financial-trojans-2013** (accessed February 2017).
Yadron, D. "Newest Hacker Target: Ads." *The Wall Street Journal Tech*, January 31, 2014. **online.wsj.com/news/articles/SB10001424052702303743604579350654103483462** (accessed February 2017).
Yan, S. "Chinese Man Admits to Cyber Spying on Boeing and Other U.S. Firms." *Money CNN News*, March 24, 2016.