

CHAPTER 8

SECURING INFORMATION

LEARNING OBJECTIVES

By reading and completing the activities in this chapter, you will be able to

- Explain the various types of threats to the security of information
- Identify the main goals of information security
- Discuss the different categorizations of security technologies and solutions
- Explain the basic functioning of security technologies and solutions, such as passwords, firewalls, biometrics, encryption, virus protection, and wireless security
- Discuss the main purposes and content of security policies
- Identify risk management options

CHAPTER OUTLINE

- [Focusing Story: My Mac Is More Secured than Your Windows-Based PC!](#)
- [Introduction and Definitions](#)
- [Learning Activity 8.1: How Protected Is Your Computer?](#)
- [Information Security Threats](#)
- [Learning Activity 8.2: What Do Hackers Break into the Most?](#)
- [Learning Activity 8.3: Detecting Phishing](#)
- [Security Technologies and Solutions](#)
- [Learning Activity 8.4: How Strong Is Your Password?](#)
- [Learning Activity 8.5: Biometrics on the PC](#)
- [Learning Activity 8.6: Breaking the Encryption](#)
- [Learning Activity 8.7: Where's the Security?](#)
- [Chapter Summary](#)
- [Review Questions](#)
- [Reflection Questions](#)
- [Additional Learning Activities](#)
- [References](#)
- [Further Readings](#)
- [Glossary](#)

FOCUSING STORY

My Mac Is More Secured than Your Windows-Based PC!

I am sure some of you have heard it and probably even shared the rumors with others. If you get a Mac (an Apple computer with a Macintosh operating system), you are much less likely to have security breaches than if you get a regular PC, plus they're really cool. We might agree with the cool part, but what is the status of Apple computer security?

For quite a while, there were few viruses and other such programs (called *malware*) that targeted Mac systems. That resulted in a reputation that Mac systems were substantially safer than Windows-based PCs. Experts do recognize that this is still true; Apple computers are less likely to be victims of viruses, but they also warn that this does not mean there are no security issues! One Mac lover and security researcher named Charlie Miller revealed in the spring of 2010 that he had identified 20 security vulnerabilities in Apple's software, each of which could result in the computer being compromised (taken over). Miller first hacked an iPhone in 2007 and then a MacBook Air in two minutes at a competition in Vancouver a few months later.

When Apple released the iPhone in 2007, it generated new interest in Apple's platforms and might have attracted the attention of many more hackers who had targeted Microsoft's platforms before. As a result, many hackers started to identify security flaws in the iPhone, such as the ability to bypass the phone's PIN by placing it in recovery mode or the ability to extract encrypted data using basic forensic software (i.e., software used by investigators to perform such tasks as logging into a computer or recovering lost or deleted files). This software is available for free online, and a YouTube video even explains how to do this. Of course, Apple released fixes for these security issues as soon as they could. Nevertheless, as a result of these issues, many firms that deal with sensitive data, such as law firms, decided iPhones were too risky to use. In the summer of 2010, new security issues surfaced with the release of the iPad. One group of computer experts discovered a flaw that allowed them to uncover 114,000 email addresses, including those of prominent officials in companies, politics, and the military. What they did is guess numbers that identified iPads connected to AT&T's mobile network.

In the end, it is still true that Macs face fewer attacks. One reason is that Macs only account for 8% of the U.S. market for computers, making this a much smaller pool of potential victims. Some say, however, that with the growth of the iPhone and iPad markets, Macs are becoming much more interesting to hack and that their software vulnerabilities (bugs) are steadily increasing. As one expert says, Mac users "do have less to worry about than their PC cousins, but still have enough potential vulnerability to justify a solid interest in security safeguards" (Furnell 2010, p. 10).

FOCUSING QUESTIONS

1. Why is forensic software available online to everyone?
2. Will increased use of Apple platforms lead to more security issues?
3. Why are security issues in iPhones and iPads of concern to Mac users?

Sources: Ante, S. E. 2010. "AT&T Says iPad Owners' Email Data Was Breached." *Wall Street Journal*, June 10: B.1; Ante, S. E., and B. Worthen. 2010. "FBI to Probe iPad Breach—Group That Exposed AT&T Flaw to See Addresses Says It Did a 'Public Service.'" *Wall Street Journal*, June 11: B.1; Furnell, S. 2010, January. "Mac Security: An Apple That Can't Be Bitten?" *Network Security*, no. 1: 7–11; Greenberg, A. 2010. "The Mac Hacker Strikes Again." *Forbes* 85(6): 40; Monroe, I. 2010. "Worms in the Apple?" *ABA Journal* 96(3): 33; Hooper, L. 2007. "iPhone: Apple's Worm?" *CRN* 1256 (December 10): 16.

Introduction and Definitions

Information security is an important topic for everyone in today's interconnected world. What is **information security**? It is defined as the set of protections put in place to safeguard information systems and/or data from security threats such as unauthorized access, use, disclosure, disruption, modification, or destruction.

Risk Management

Before discussing information security, it is important to understand that information security is one aspect of risk management that organizations pursue. No matter what efforts an organization may make to provide the best security possible, or which technologies and tools it might invest in, there will always security risks involved. **Risk management** is the process of identifying, assessing, and prioritizing the security risks an organization may face. As a result of this process, organizations may decide to accept the risks, try to mitigate or prevent those risks by investing in security protections, or share the security risks with another organization—for example, by buying insurance. Organizations can refer to different standards for risk management that are available from organizations like the Project Management Institute, the National Institute of Science and Technology, and the International Standards Organization (ISO).

While security and risk management do go hand in hand, they have a few differences as well. Security is focused on protecting the assets a company has from both external and internal threats. External threats such as hackers and viruses threaten the valuable information a company collects while in business. Security must be able to secure these data from attacks to ensure the company can run smoothly without interruption. Internal threats are important to guard against as well. For example, security must monitor the network to make sure that policies are not being breached in a harmful way (either deliberately or accidentally) and that employees are only able to access systems they are authorized to. Risk management has a broader focus, analyzing and balancing risks with the resources available to mitigate them. Risk management determines where the company is most vulnerable and how likely it is to be affected by a risk. While weighing these risks, the company looks at the cost of addressing these issues and makes decisions based on both the financial aspect and the acceptable level of security needed to protect different areas in the company. A graphical representation of how a multitude of threats work together to increase risk is presented in [Figure 8.1](#).

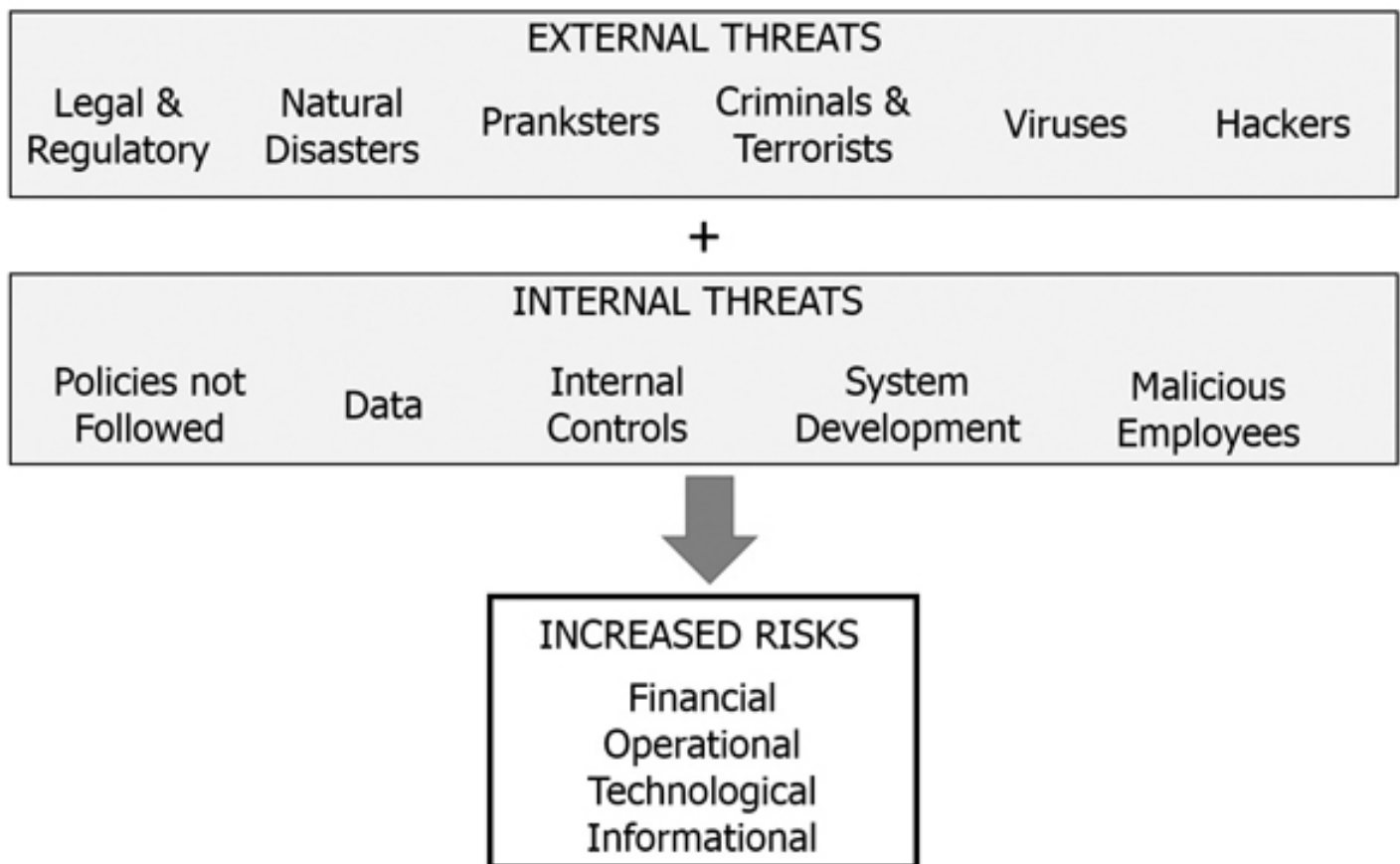


FIGURE 8.1 Threat Types and Causes That Lead to Increased Risk Exposure

In this chapter, the focus is on the steps that can be taken to mitigate or prevent risks. That is the essence of why information security steps are taken. First various high-level information security concepts are discussed.

This is followed by a discussion of various information security threats, and finally by solutions to these threats. It is important to note that some of the solutions are employed to counteract multiple threats. There is not a direct one-to-one relationship between threats and solutions.

Information Security Concepts

Whether you need to secure your own computer to prevent a virus from destroying your files or an organization needs to secure access to its data and servers to ensure that hackers cannot get information about its clients, the core concepts of security remain the same.

First, security is not only about technology but also about management and people. It is possible to acquire the best-ever security tools, but if employees do not use them or, even worse, decide to bypass the security protections mandated by the organization, the systems and data are vulnerable to attacks or security failures. Top-to-bottom commitment to security in the organization is needed to ensure that security tools are properly used and security policies are followed adequately.

Second, the world of information security is somewhat unfair. How many security weaknesses does the hacker need to break into a system? One. How many security weaknesses does the organization or individual need to fix or protect against? All of them. This is referred to as **asymmetrical security warfare**. One party must do everything to protect oneself, while the other party (the attacker) only needs to find the one weakness.

Third, as a result of having to protect the computer systems and data from all possible weaknesses, security for individuals, and even more so for organizations, requires what is called *defense in depth*. **Defense in depth** means that there must be multiple layers of security protections in place. For example, if you have very important data on your computer, such as personal financial information, defense in depth would mean having a lock on the computer, a password to access it, a firewall to protect it against breaches from the Internet, and even encryption of the data so it is unreadable without the passcode or password. We will discuss all these technologies in this chapter. Below we explore various levels of security protection in depth.

Security Levels

The concept of defense in depth refers to multiple layers of protection, which can include multiple devices performing similar functions. Similarly, there must exist protection technologies and policies to secure stored information, as well as information in transit. Some like to refer to three main levels: (1) protection of the information itself, (2) protection of the computer on which the information is stored, and (3) protection of the network to which the computer is connected. A more fine-grained set of security levels is shown in [Figure 8.2](#). In this case, data can only be accessed with proper authorization for the data, the application that uses the data, the host computer on which the data are stored, and the network to which the host is connected.

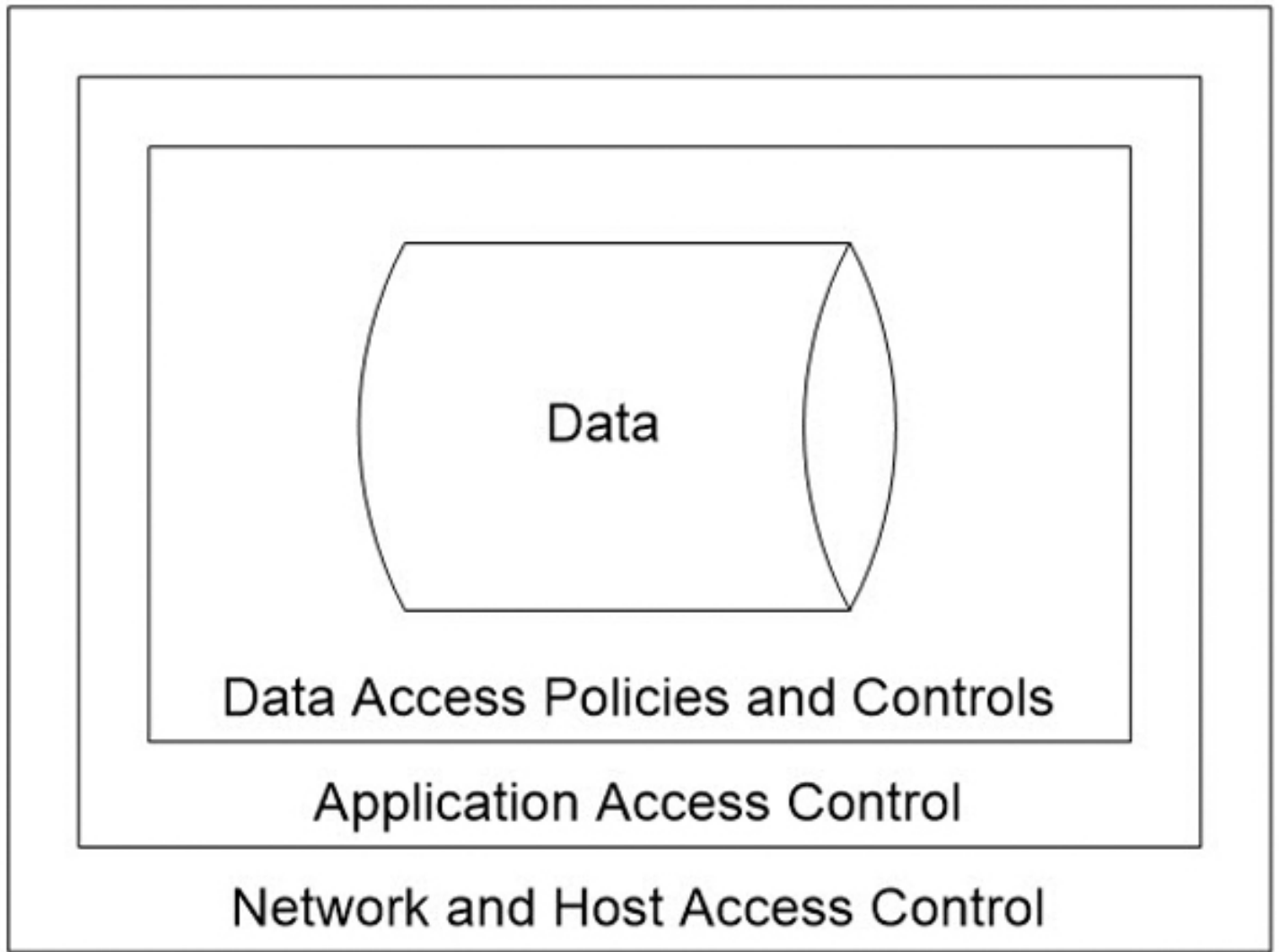


FIGURE 8.2 Access Levels for Information Security

An example of securing access to data could be the university grade-entry application that your instructors use. In order to give you a grade for the semester, the professor needs to have access to the university's network with a user ID and password. To change grades, the instructors are required to connect to a specific application on a specific system, which also requires the use of a user ID and password. In addition, only authorized users (instructors) are able to access the grade-entry application. The student data are protected through an additional level of security, since only certain instructors are allowed to change certain grades for certain students. At many universities, an employee ID is required in addition to the user ID and password when accessing specific information about students. Finally, data can be encrypted at the data level, providing yet another level of security. In this case, the instructor (or her computer) will need to have software to handle the encrypted information and make it legible.

LEARNING ACTIVITY 8.1

How Protected Is Your Computer?

For many individuals, students and nonstudents, security is the job of information technology (IT) specialists and something they do not feel comfortable handling themselves. However, many studies show that the weakest link in security is these same individuals who fail to perform basic steps in securing their computers, data, and networks. Does this describe you? Let's see how secure your computer is with this learning activity.

1. Run one of the following applications and print (to file) a copy of the vulnerability report.

a. Shields Up application: <http://www.grc.com>

b. Firewall test at Audit My PC: <http://www.auditmypc.com>

2. Try to fix the issues identified, if applicable.

3. Bring your online report to class for discussion.

Information Security Threats

Most people think of information security as unauthorized access to individual or organizational data or systems. But it is much broader; it also includes dealing with natural disasters, such as earthquakes and fires, as well as dealing with any threats to computerized systems, such as viruses, hackers, and accidental loss of data or systems.

There are a large number of **security threats** to individuals and organizations alike, particularly today, as most people are connected to the Internet on a regular if not permanent basis. Threats are often broadly categorized as denial of service, unauthorized access, and theft and fraud. **Denial-of-service threats** are those that render a system inoperative, limit its capability to operate, or make data unavailable. **Unauthorized access threats** refer to someone accessing systems and/or data illegally. **Theft and fraud threats** are related to the loss of systems or data due to theft or fraudulent activities.

Denial of Service

Security threats that can cause denial of service can result from intentional acts, careless behavior, or even natural disasters. While natural disasters such as earthquakes, tornadoes, hurricanes, or fires cannot be prevented and can completely destroy systems or data, a careful security **disaster recovery** plan will include steps to recover from such disasters (backups, duplicate systems, etc.). Careless behavior can include forgetting to perform proper backups of one's computer, not installing security updates to an operating system, or failing to update one's antivirus software. Often, individuals even turn off security features because they find them annoying. Was this the case in [Learning Activity 8.1](#)? Did you remove password protection from your PC? Did you forget to update your operating system software? No one should underestimate the potential security issues that careless behaviors can generate. What solutions exist to protect against these? Education is the first one, and the second is the automation of security tools and updates so that the user does not have to perform security tasks or is prevented from reducing the effectiveness of the current security of the systems and data.

The last category of denial-of-service security threats includes those that are intentional. Some threats could be fairly simple, like vandalism from a disgruntled employee who reformats a server's main drive or starts a fire in the computer room. Others can involve sophisticated tools meant to disrupt use of or destroy systems or data. These threats include viruses and other malware, email bombing and other attacks, and break-ins (also unauthorized access, as discussed in that section).

Viruses and Other Malware

Viruses have been around for several decades and have become a major issue for all organizations, as well as individuals. It is likely that at least one person in your class has been a victim of a virus. Two of the authors have at some point in time had computer virus issues. Viruses are often referred to as targets of opportunity, which means they are sent out to find any victim they can.

What are viruses? What do they look like? **Viruses** are computer programs designed to perform unwanted events. Some cause minor harm, such as sending undesirable messages. Others are very destructive, deleting all files on a computer or creating so much traffic on a network that it crashes and cannot be used by its customary users. The lines of code that make up a virus can be embedded into other files, or they can be attached to the initial boot sectors of disks or USB drives (so they automatically infect anyone using that device).

What the virus looks like is called the **virus signature**; it is the particular bit patterns that can be recognized, which is how virus detection software knows your computer has contracted a virus. If viruses are embedded into a legitimate file, they are often called **Trojan horses**. If they can propagate themselves throughout the Internet with no user intervention, they are referred to as **worms**. A stealth **virus** is a more advanced virus that changes its own bit pattern to become undetectable by virus scanners. Some viruses are downloaded when users access certain websites. Browsers today often protect you from downloading what is called **active content** (for example, ActiveX programs). However, when asked, many users simply say yes to downloading any content from a website. Once viruses are installed on a computer, it may be difficult to remove them. (We discuss later how to do this.) Viruses can also modify themselves as they move to other computers, changing their signatures to become less easy to detect. Finally, **spyware** (which we discuss in [Chapter 9](#)) is a form of virus, since the software logs everything users do on their computers, unbeknownst to them.

There are also **virus hoaxes** on the Internet. These are not viruses but false virus alerts being sent and resent by individuals. Their consequences include either substantial unnecessary network traffic or unwanted actions by users (for example, telling users that certain files must be deleted to avoid the virus). Usually, unsophisticated users who panic at the idea that they might have caught a virus propagate these hoaxes. In case of doubt, the best action is to go to the website of the company that built the targeted application and search for virus hoaxes.

Email Bombing and Other Computer Attacks

Computer attacks, including **email bombing**, involve targeting a specific computer or network with the intent of disrupting its normal functioning. These attacks send a large number of requests, emails, or synchronization (SYN) messages to fill the target's mailboxes, system, communication ports, or memory buffers with the intent of blocking legitimate messages from entering the systems or overloading the systems to make them crash. When a hacker uses an innocent third party to multiply the messages being sent to the intended target, such as a university server, this is called **smurfing**. To do this, hackers place software agents on the innocent third party's computer. These programs will then help them launch their attacks when they decide to strike. If many computers are being used for such attacks, we call them **distributed denial-of-service (DDOS) attacks**.

Why would anyone perform such malicious acts? Some may be disgruntled employees. Others may attack a given target for political reasons—for example, protesting a company's stand on some issue. The groups who perform such actions often use the term **hacktivism**, which involves finding information that, if revealed, will advance human causes. However, these and other denial-of-service attacks by hackers continue to be very damaging to organizations. Any downtime in computer systems or networks can mean lost sales and lost revenue for companies or major losses in productivity if employees cannot perform their normal duties.

Unauthorized Access

Unauthorized access involves illegal access to systems, applications, or data. One of the biggest worries for organizations is theft of data, including customer information, trade secrets, or other important information regarding the organization, its business partners, or its employees. Unauthorized access through break-ins can also be used to damage information or applications on a system, leading to a type of denial of service.

When thinking of unauthorized access, we often imagine a hacker who lives on the margins of society and tries to access an organization's data files to do something good for the world or to prove he can. However, the reality is that organizational insiders often perpetrate unauthorized access; they have the knowledge needed to hack into the systems to obtain information, such as credit card numbers. Some incidences of unauthorized access are difficult to identify because they are passive, such as recording transmissions. By doing so, a hacker can obtain passwords, which can then be used to access information on an organization's systems through a valid account. Break-ins can also be used to actively modify the system or data being hacked—for example, creating false account information for fraud purposes, downloading customer data, or changing the content of messages to

falsely implicate the company in certain events or to delay negotiations on an important contract. [Figure 8.3](#) shows the differences between passive and active unauthorized access.

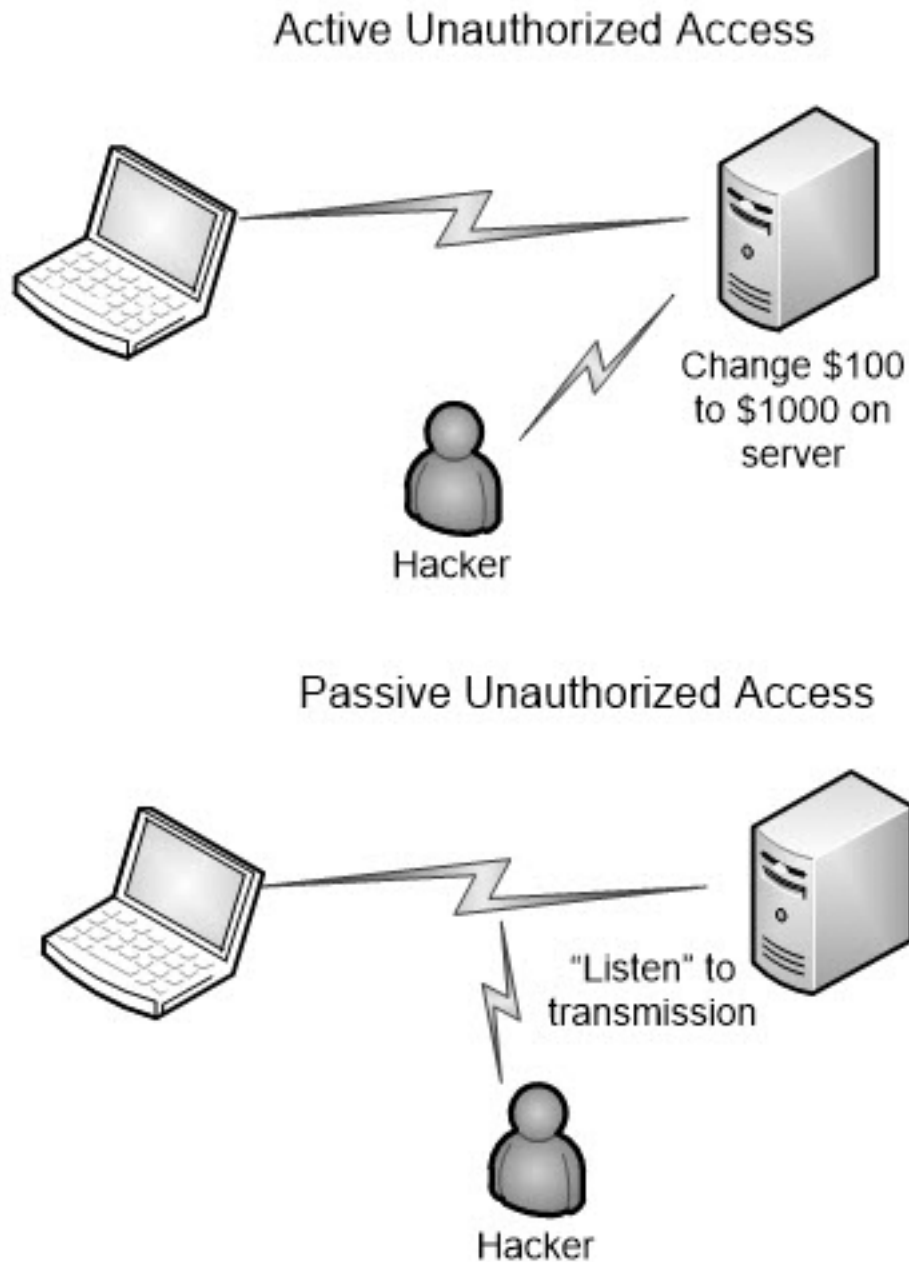


FIGURE 8.3 Passive versus Active Unauthorized Access

How is hacking actually performed? It requires a combination of skills and patience. Most of the tools available for hacking are unfortunately easy to find on the Internet, but not everyone has the skills, patience, or intent to perform break-ins. Software, such as **sniffers**, can be used to map information on someone's network and identify weaknesses in computers and networks. When you performed [Learning Activity 8.1](#), the scanning software identified **open ports** on your computer. This means that some specific applications are installed and running on your computer. Once this is known, a hacker can test the targeted system for vulnerabilities (like unpatched software), and if a vulnerability is found, he or she can exploit it. Hackers often do this using **spoofing**, which means they pretend to be someone else (or another computer). In an email message, you can easily spoof an address by simply changing the information in the "From" line to reflect the name of the person you want to impersonate. This is not very sophisticated, and many individuals are able to detect such simple spoofing. More advanced spoofing can be done at the IP address level by changing the source (sender's) IP address to look like it comes from a different address. This is done by changing the information in the address field of the IP packet. A packet is a small unit of data that flows through networks, allowing for the transmission of messages. Hackers

usually spoof IP addresses when they launch spamming denial-of-service attacks so that the attacks cannot be traced back to them. Spamming involves sending emails to many individuals at once, sending unsolicited commercial email to individuals, or targeting one individual computer or network and sending thousands of messages to it.

What are vulnerabilities? They are often called *software security holes*. All operating systems and applications have them. The Internet is again a source of information, since vulnerabilities are documented. Software patches (updates) are meant to address these vulnerabilities once they are found. When new software is made publicly available, it usually takes very little time for hackers to identify the security holes. The software developers then have to quickly react by developing fixes, which are made available to users via download on the software developers' website. Unfortunately, many users do not update their operating systems fast enough or even turn off automatic updates.

LEARNING ACTIVITY 8.2

What Do Hackers Break into the Most?

Hackers have been increasingly making the news for stealing information from a number of large companies. For this learning activity, visit <http://www.verizonenterprise.com/verizon-insights-lab/dbir/> and download Verizon's latest Data Break Investigations Report. As you are reading the report, do the following and be prepared to discuss in class:

1. List the targets of hackers and how many report incidents there were.
2. Determine which of these incidents were of the greatest concern to consumers.
3. Create various ideas for how you can protect yourself from hackers seeking to gain access to information you have shared with organizations.

Finally, it is important to reiterate that many unauthorized access situations arise because users have access to someone else's legitimate passwords and accounts. In many cases, individuals are negligent about protecting their passwords. In other cases, individuals can be tricked into giving out this (and other) information. This is referred to as **social engineering** (and sometimes called *phishing*). Examples of social engineering actions include tricking someone into telling you his or her password by claiming to be someone with rights to know it or tricking someone into sending you an important file or opening a link to a dangerous website. Sophisticated social engineering can even involve listening to lunch conversations among unsuspecting professionals with privileged information. Today, most Internet users are familiar with phishing through email messages sent from hackers pretending to be banks or large companies such as [eBay.com](http://www.eBay.com), PayPal, or Amazon.com. The problem is that for most individuals, it is hard to identify whether such emails are phishing emails when they actually have an account with those companies.

BUSINESS EXAMPLE BOX 8.1

Even Big Technology Companies Can Be Hacked

One would think that large technology companies should have the resources and expertise not to be victims of hackers, right? Well, in fall 2014, big, mighty Apple was the victim of hackers.

In August and September 2014, you may remember that a number of celebrity photos stored on Apple's iCloud were leaked. Apple claims that their system was not compromised but that hackers compromised selected user accounts through a "brute force" method of guessing their user names, passwords, and security questions. However, other reporters suggested that a user's Apple ID was easy to crack with the right tools, laying responsibility on Apple. The best approach for individuals who use products such as iCloud and other Internet-based services is to enable two-factor authentication. This requires a password along with a one-time-use code, often sent to a user's phone or email address. Doing this forces hackers to have access to not only something that the user knows but also something that the user possesses.

Source: Kovach, S. 2014. “We Still Don’t Have Assurance from Apple That iCloud Is Safe.” *Business Insider*, September. <http://www.businessinsider.com/apple-statement-on-icloud-hack-2014-9>.

Even when a system has been hacked, organizations do not necessarily know that this has happened unless a problem occurs immediately. Some organizations have tools to detect hacking attacks, which we will discuss in the next section of this chapter. The hacker, however, will often start the attack by erasing audit logs that would show what has happened and installing **rootkits**, or software that will allow him to have unfettered access to everything on the system, including adding, deleting, and copying files. Hackers often install **backdoors**, allowing them to reaccess the system at their will. Finally, they can install victimization software, such as **keystroke capture programs** that will log all information entered into the computer, spyware, attack software for denial-of-service attacks, or other remote tools to control the systems that have been hacked.

LEARNING ACTIVITY 8.3

Detecting Phishing

There are many ways to detect phishing emails. Look for the following common problems to identify phishing emails:

1. The email is not addressed to you directly.
2. The email is addressed to you using your email account info (without the @provider).
3. The email does not have a personalized salutation (i.e., Dear Bélanger).
4. When you hover the mouse over the hyperlink, the site does not seem to be from the proper company. (Look at the domain name.)
5. When you hover the mouse over the hyperlink, the site seems to be located in another country.
6. The email contains poor grammar and spelling mistakes real companies would not make (we hope).
7. The email makes you feel your response is urgent or something bad is going to happen.

Read more about phishing at the following sites:

- <http://www.antiphishing.org/>
- <http://www.spamlaws.com/phishing.html>

Then test your skills detecting phishing emails here: <http://www.sonicwall.com/furl/phishing/>. You can also identify the problems mentioned above in the sample phishing email in [Figure 8.4](#).

From: customer.center@BankOfAmerica.com

To: belanger@vt.edu

Date: Oct-22–10 2:36 PM

Subject: Online Banking Alert

Your Online Banking Is Blocked! Please Take Immediate Action.

Dear Belanger,

We recently reviewed your account and we suspect that your Bank of America account may have been compromised by an unauthorized person. Protecting the security of your account is our primary concerns. Therefore, as a preventive measure, we have temporarily limited access to important account features.

To restore your online account access, we need you to confirm your information at the following website within 48 hours of receiving this email. It is very important that you update your information within this time frame if you do not wish your online access to be placed on hold.

<https://www.bankofamerica.com/update/>

We thank you for your rapid attention to this matter.

FIGURE 8.4 Example of a Phishing Email

Theft and Fraud

Theft and fraud concerning information have become important concerns for companies. We discussed some fraud and theft of data in the unauthorized access discussion. Two additional issues need to be explored regarding theft and fraud: theft of software or hardware devices that increasingly contain huge amounts of information and theft of data using small hardware devices.

Theft of software usually occurs when employees copy legitimate software installed on their company's servers to bring home or to give to someone else. These copies do not carry licenses and are therefore illegal copies. This is a major concern for organizations, and many have started to perform audits of installed software. The best security control for this problem, though, is user education. Many employees do not see a problem with copying software this way, although it is illegal. Other organizations provide only personal computers that do not allow saving to any external mediator devices, preventing software from being copied.

As hardware has become more portable and powerful, theft of hardware has become an increasing concern for organizations. Think of how much data can be stored on a laptop, tablet, or even a personal digital device like an iPhone. Besides the cost of the hardware itself, organizations have to worry about the information contained on these devices as well as the access that the devices often have to the organization's internal systems.

Finally, theft of data is also possible thanks to storage devices with ever-increasing capacities. Today, a small USB thumb drive can contain gigabytes of data. Think of a complete list of all of an organization's customers, with addresses and historical purchases; this can fit easily on a thumb drive. An individual can install software that automatically copies everything on a device when the USB thumb drive is inserted. There have been reports of such tools being inserted into computers in hotel business centers, in kiosk devices in shopping malls, and others. A nonemployee roaming an office could easily copy tons of files if allowed in with the device and not supervised while in the organization's offices.

Summary of Security Threats

Before a manager can evaluate security measures and come up with a proper security plan, she must identify all the threats to security that her organization faces. We presented some of the most common security threats in this section. There are, however, other threats to security that can occur. Each year since the late 1990s, the Computer Security Institute and the FBI have conducted a survey of the most prevalent threats. Their data show that viruses, insider abuse of information systems, and laptop theft remain the most important issues. It is necessary to distinguish here between prevalence (how often the threats occur) and impact (cost of the threat). For example, financial fraud is considered a low-prevalence but high-impact security threat. In 2013, 75% of companies believed that they were more susceptible to security breaches than they were in 2012 (Davis 2014). This is due to the increased prevalence of security breaches during the course of the year. Even more interesting is that not all intrusions are reported because companies do not want to spend the energy on reporting incidents, are afraid of negative publicity or competitors taking advantage of the incidents, or do not believe law enforcement can help or would be interested. The following is a list of the security breaches that tend to occur most often over the years in order of prevalence (i.e., those reported most often listed first):

1. Malware (e.g., viruses, worms, botnets)
2. Phishing
3. Exploitation of Web or software applications
4. Denial of service
5. Theft of computers or storage devices
6. Attacks of operating system vulnerabilities
7. Compromises to database, content, or data management systems

8. Vandalization of website or manipulation of site content
9. Physical break-in
10. Intrusion into mobile applications
11. Trafficking in illicit materials or illegal data

Security Technologies and Solutions

Security Goals

Before we discuss each of the security tools, we need to briefly mention that all tools and policies are meant to address one or more core security goals, which are known as CIA: confidentiality, integrity, and availability.

Confidentiality involves making sure that only authorized individuals can access information or data. **Integrity** involves making sure that data are consistent and complete. For example, as a message is transmitted, its content must not be modified unwillingly during the transmission. Finally, **availability** involves ensuring that systems and/or data are available when they are needed. For systems to be considered highly available, the organization must protect them from disruptions not only due to security threats such as denial-of-service attacks but also due to power outages, hardware failures, and system upgrades.

There are two additional goals of security to consider: authentication (or authenticity) and nonrepudiation. **Authentication** is basically making sure that the parties involved are who they say they are and that transactions, data, or communications are genuine. **Nonrepudiation**, which is particularly important in e-commerce, refers to making sure one cannot renege on his or her obligations—for example, by denying that he or she entered into a transaction with a Web merchant. In e-commerce, digital signatures and encryption are used to ensure that the goal of nonrepudiation is met.

Preventive, Corrective, and Detective Controls

A large number of security technologies and solutions exist to address the threats we have discussed so far. One way to classify the security solutions and tools (often called *security controls*) is to consider whether they are preventive, detective, or corrective controls. The goal of **preventive controls** is to stop or limit the security threat from happening in the first place. For example, **antivirus software** scans computers and programs and alerts users if potential viruses exist before they can infect files or computers. The goal of **detective controls** is to find or discover where and when security threats occur. For example, **audit logs** can be used to track access to a system to see if multiple false attempts are made from a particular user ID. Finally, the goal of **corrective controls** is to repair damages after a security problem has occurred. An example is the antivirus software previously discussed, which can remove a virus, quarantine the file with the virus, or simply delete the problematic file.

Physical Security versus Logical Security

Security solutions can also be classified as physical or logical. **Physical access controls** are those security solutions that involve protecting physical access to systems, applications, or data, whereas **logical access controls** include security solutions that protect access to systems, applications, or data by ensuring users or systems are authenticated and allowed to have such access.

Physical access controls can include locks for laptops, locked computer rooms, and secured rooms for backup storage. Once devices are no longer needed, software programs called *drive shredders* should be used to make sure that all discarded disk drives cannot be read again. Physical security also involves ensuring that wiring closets, where all the routers and connections are located, are properly locked and secured. Another important aspect of

physical security is selection of personnel. Remember that insider abuse is one of the most significant security threats. Organizations must ensure that only proper personnel have access to key information systems and data. Organizations should run background checks on such personnel and provide appropriate training. Several surveys have identified onsite contractors as a major threat to security for organizations.

Logical access controls use many technologies to require authentication of users and systems trying to access specific applications, networks, data, or computers. These include user profiles, biometrics, firewalls, and encryption.

User Profiles

User profiles are one of the main solutions used to prevent unauthorized access to systems, data, and applications. Users are assigned profiles that consist of a user identification (self-selected or assigned by the organization) and a set of privileges. Once the user confirms his identification, he can access the system, application, or data with the level of privileges given to him. For example, faculty can view student data but cannot modify some of those data (such as personal addresses). This is considered the **principle of least privilege**. Give users only access to what they need and no more!

User profiles require that individuals be differentiated from one another using one or several levels of identification: possession, knowledge, or trait.

- *Possession* is when an individual owns a form of identification. For example, your driver's license, your student ID, and your passport are possession forms of identification.
- *Knowledge* is when an individual needs to know something to gain access. Passwords are a good example of knowledge required to access systems. Combining possession and knowledge, such as requiring a personal identification number (PIN) with a banking card, provides more security.
- *Traits* require recognition of physical or behavioral human characteristics, such as a fingerprint or a signature style, to gain access to systems, data, or applications. This is part of biometrics, which will be described in the next section.

LEARNING ACTIVITY 8.4

How Strong Is Your Password?

Passwords are one of the most used security solutions to control access to systems, applications, and data. We have no doubt that you have several passwords you use on a regular basis. But how strong are these passwords? Let's see what a strong password is.

1. Select two passwords you use frequently and test their level of security using one of the following password checkers:

- <https://howsecureismypassword.net/>
- <http://www.passwordmeter.com>

2. Read the information on how to create a strong password:

- <http://windows.microsoft.com/en-us/windows-vista/tips-for-creating-a-strong-password>

3. Create a strong password. Test it. Do not use it for your accounts!

4. Bring the following to class:

- The level of security of your two passwords (Be honest, but do not tell the passwords!)
- The strong password you created and what it stands for

User profiles remain one of the most used security solutions for access to systems and data. Yet there are many issues with using user profiles for authentication. First, users often use words or numbers that are easy to remember for their passwords. Many systems today will not accept such passwords, which can be easily "broken" with a **dictionary attack**, where all words of several dictionaries in multiple languages are tested as passwords

with numbers before and after the words. With this method, it often takes only a few seconds for a password to be discovered. The second problem is that users also write their passwords down on a sticky note taped to their computer or taped to the inside of their desk drawers because they have too many passwords to remember. Alternatively, they use the same password for everything. If someone finds out about it, all systems the user accesses are compromised. Password recovery can be a problem too, since it is often easy to know the name of a person’s pet, family members, school attended, or city of birth, as well as birthday or important numbers. Just think how much of that information can be found on social networking sites like Facebook!

To increase the effectiveness of user profiles, security systems now often require users to change their passwords regularly, such as every one, three, or six months. Many systems will not allow more than a few attempts at entering a password before they block access to the user account. Most systems also require the use of strong passwords. As you discovered in [Learning Activity 8.4](#), strong passwords require a mix of uppercase letters, lowercase letters, alphanumeric characters, and numbers. Tools exist to help manage passwords. For example, **password crackers** are available online for various systems to recover passwords that are forgotten. Of course, they can also be used to crack someone else’s password—for example, on a stolen laptop. There are also password generators that can help you generate strong passwords. Even with all these tools, however, most individuals still create poor passwords. SplashData analyzed more than 3.3 million leaked passwords in 2014 and posted them online. An analysis of these passwords revealed that most users had really weak passwords; the top 20 passwords are shown in [Table 8.1](#).

TABLE 8.1 Top 20 Passwords in 2014

Rank	Password	Rank
1	123456	11
2	password	12
3	12345	13
4	12345678	14
5	qwerty	15
6	123456789	16
7	1234	17
8	baseball	18
9	dragon	19
10	football	20

Source: Based on data from SplashData, available at <http://splashdata.com/press/worst-passwords-of-2014.htm>.

Biometrics

Another security method used to authenticate users and control access to systems, data, and applications is **biometrics**, which use human traits and characteristics to recognize individuals. While they go beyond possession and knowledge, biometrics can be used in conjunction with these to provide strong security—for example, requiring a card with a password and a fingerprint to have access to certain data. Fingerprinting is a low-cost example of biometric technology. There are several other biometric technologies, which can be classified as **physiological biometrics** (those that use physical traits) or **behavioral biometrics** (those that use behavior). [Table 8.2](#) briefly describes these security solutions.

TABLE 8.2 Sample Biometric Solutions

Physiological Biometrics		Behavioral Biometrics	
Fingerprint recognition	Analyzes ridges and valleys (minutiae) on the surface tips of human fingers.	Signature recognition	Analyses the signature Static signature recognition compares scanned or ink signatures; dynamic signature recognition analyzes how it is written using pressure points—how much an individual she writes her name.
Facial recognition	Analyzes facial features or patterns (faceprints).	Gait recognition	Analyzes the walking style or gait of individuals.
Finger geometry recognition	Analyzes 3D geometry of the finger.	Keystroke recognition	Analyzes rhythm and patterns of keystroke of individuals.
Hand geometry recognition	Analyzes geometric features of the hand, such as length of fingers and width of the hand.		
Iris/retina recognition	Analyzes features (eyeprints) in the iris or the patterns of veins in the back of the eye (retina).		
DNA recognition	Analyzes segments from an individual's DNA.		
Odor recognition	Analyzes an individual's odor to determine identity.		
Voice recognition (speaker recognition)	Analyzes voice to determine the identity of a speaker (who is speaking); different from speech recognition (what is being said).		
Ear recognition	Analyzes the shape of the ear.		

Source: Based on information provided by Griaule Biometrics, available at <http://www.griaulebiometrics.com/en-us/book/understanding-biometrics/introduction/types/behavioral>.

LEARNING ACTIVITY 8.5

Biometrics on the PC

For this learning activity, start with the list of biometric solutions provided in [Table 8.2](#) and utilize the Internet to list how well each of these could be implemented on your personal computer to provide authentication. Be prepared to discuss this list with the class.

Law enforcement agencies have used fingerprinting for a long time to identify criminals. Today, many laptops have fingerprinting scanners to restrict access or replace passwords. Iris scanning offers some of the best security because the iris is unique among all individuals. (The iris is the colored portion of the eye.) Immigration services in the United States use fingerprinting for noncitizens and iris scanning for frequent travelers who have special cards identifying them as trusted travelers. The English government in the United Kingdom has a large database of earprints because it is said that no two ears are the same.

Biometrics are used in one of two ways: authentication or identification. In **authentication**, also called *one-to-one matching*, the goal is to match the individual with his or her stored biometric data. Fingerprint biometrics on laptops are good example of that. In **identification**, also called *one-to-many matching*, the goal is identify an individual from an entire population of individuals with stored biometric data. An example is facial recognition

at airports used to identify potential terrorists entering a country from a database of facial prints stored by law enforcement agencies. The processes of authentication and identification are shown in [Figures 8.5](#) and [8.6](#).

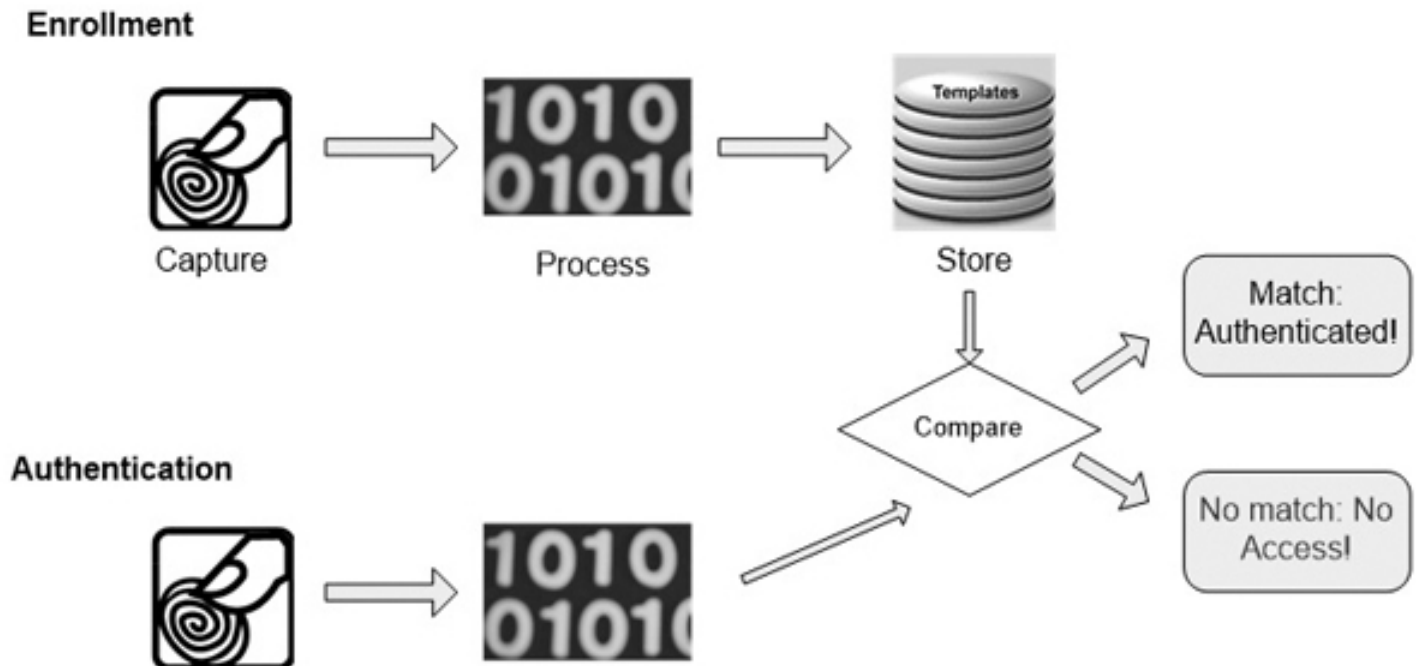


FIGURE 8.5 Authentication in Biometrics

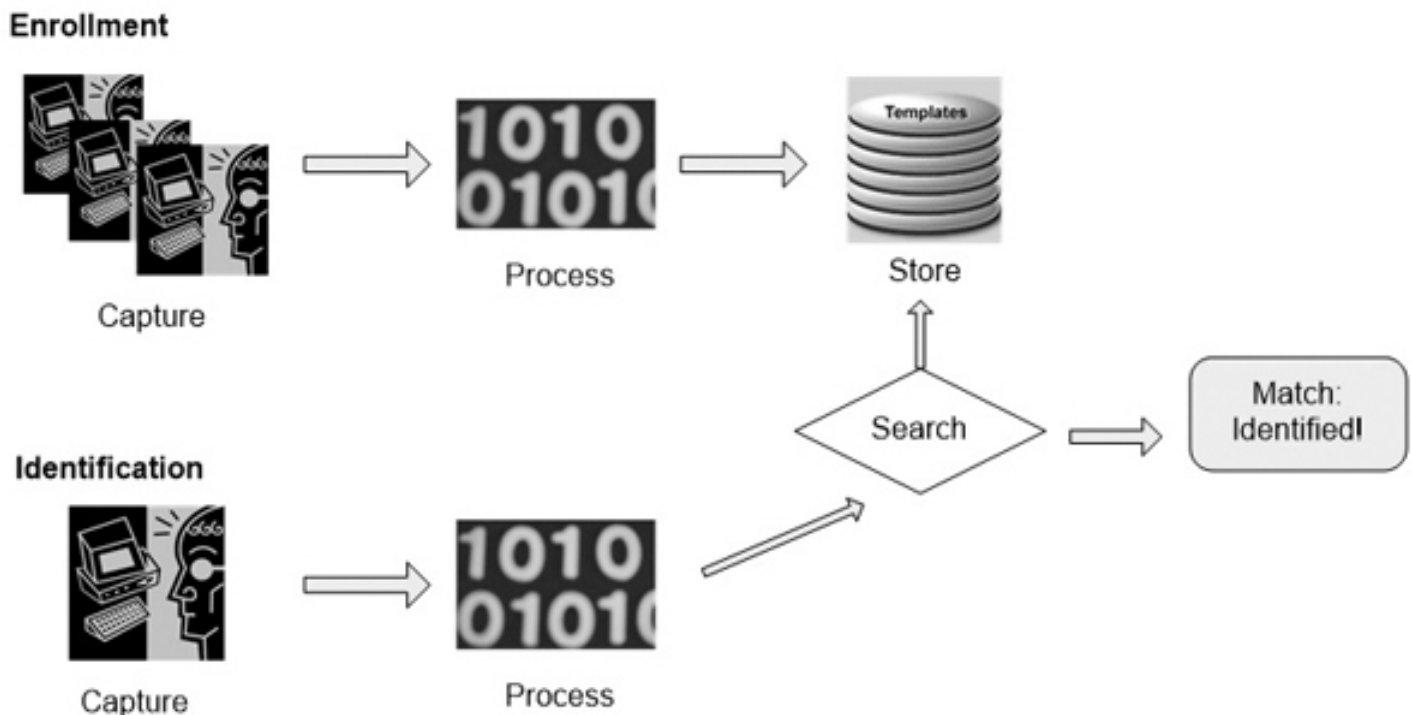


FIGURE 8.6 Identification in Biometrics

Firewalls

At the beginning of the chapter, you tested your computer security using an online tool. The software was looking for whether your computer was letting information out about itself and whether there were open ports or software

applications running. The best protection against these potential problems is a firewall, and if your computer's firewall was running and up-to-date, your computer should indicate that your computer was "stealth" (not visible to outsiders).

A **firewall** is a computer or a router that controls access in and out of the organization's networks, applications, and computers. The term *firewall* comes from the construction industry, where it represents a wall built with fire-resistant materials. If a fire starts in one room of a building, it won't spread to other rooms if firewalls are used. In computer security, firewalls control the transmissions that are attempting to enter and/or leave the organization's networks or computers, as shown in [Figure 8.7](#).

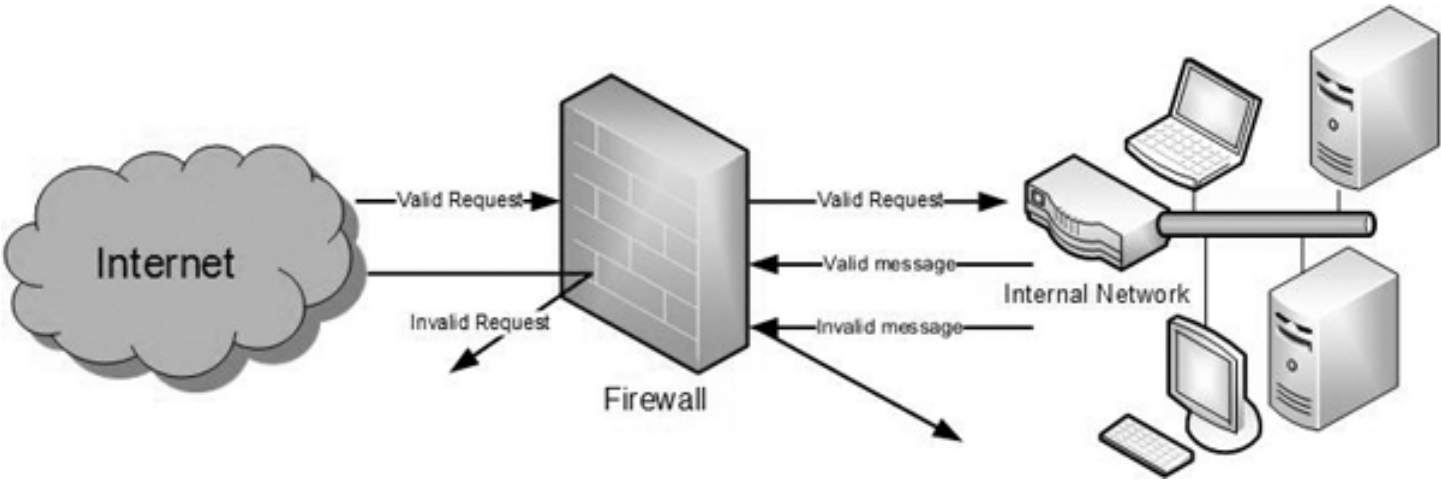


FIGURE 8.7 Firewall

There are several types of firewalls, which vary in how they control access into and out of the organization. [Table 8.3](#) lists various terms used to describe firewalls.

TABLE 8.3 Firewall Types and Terminology

Firewall type	Packet-level firewall (also called screening router firewall)	A firewall that works at the network level, looking at information within the data packets (see online appendix). If the source address of the packet is from an "acceptable" computer, the firewall will let the message through, assuming that the destination address is also a valid internal address.	Easy to implement and such as email bomb service. Sophisticated these.
	Application-level firewall (One form is called a <i>proxy server</i> .)	A firewall that verifies access to applications. Users must log into the firewall before they can access applications inside the organization (from outside).	More complex to implement communication but packet-level firewall
	Firewall appliance	A firewall that is self-contained. In other words, the hardware and software are built to perform only one function, that of a firewall.	Very useful for small technical knowledge than a simple host firewall computers.
Firewall location	Internal firewall	A firewall used between departments or divisions inside the organization.	Organizations can use data and provide greater protection.
	External firewall	A firewall used to protect access to the internal network and computers of the organization.	This is the type of firewall most definitions.
	Host (personal) firewall	A firewall installed on a computer.	Good option for all protecting the computer warning of arrival of firewall often offers

Firewall technology	Static firewall	A firewall with predetermined ways of dealing with transmission requests based on application types and ranges of IP addresses.	Easy to implement.
	Dynamic firewall	A firewall that manages requests as they occur, deciding on both denials and permissions as they arrive.	More difficult to manage.

Firewalls are great security tools, but they cannot handle all security threats. For example, they cannot protect an organization from a virus that is attached to a message with an appropriate destination and source addresses or that is introduced by an individual on a portable storage device. Firewalls also cannot prevent hackers from exploiting an unsecured computer; keep disgruntled employees from copying sensitive information; or stop employees from losing sensitive data loaded on an unsecured laptop, thumb drive, or smartphone, for example. Nevertheless, firewalls are part of the main line of defense for organizations. Consistent with the principle of defense in depth, different firewalls should be implemented at different locations in the organization, as shown in [Figure 8.8](#).

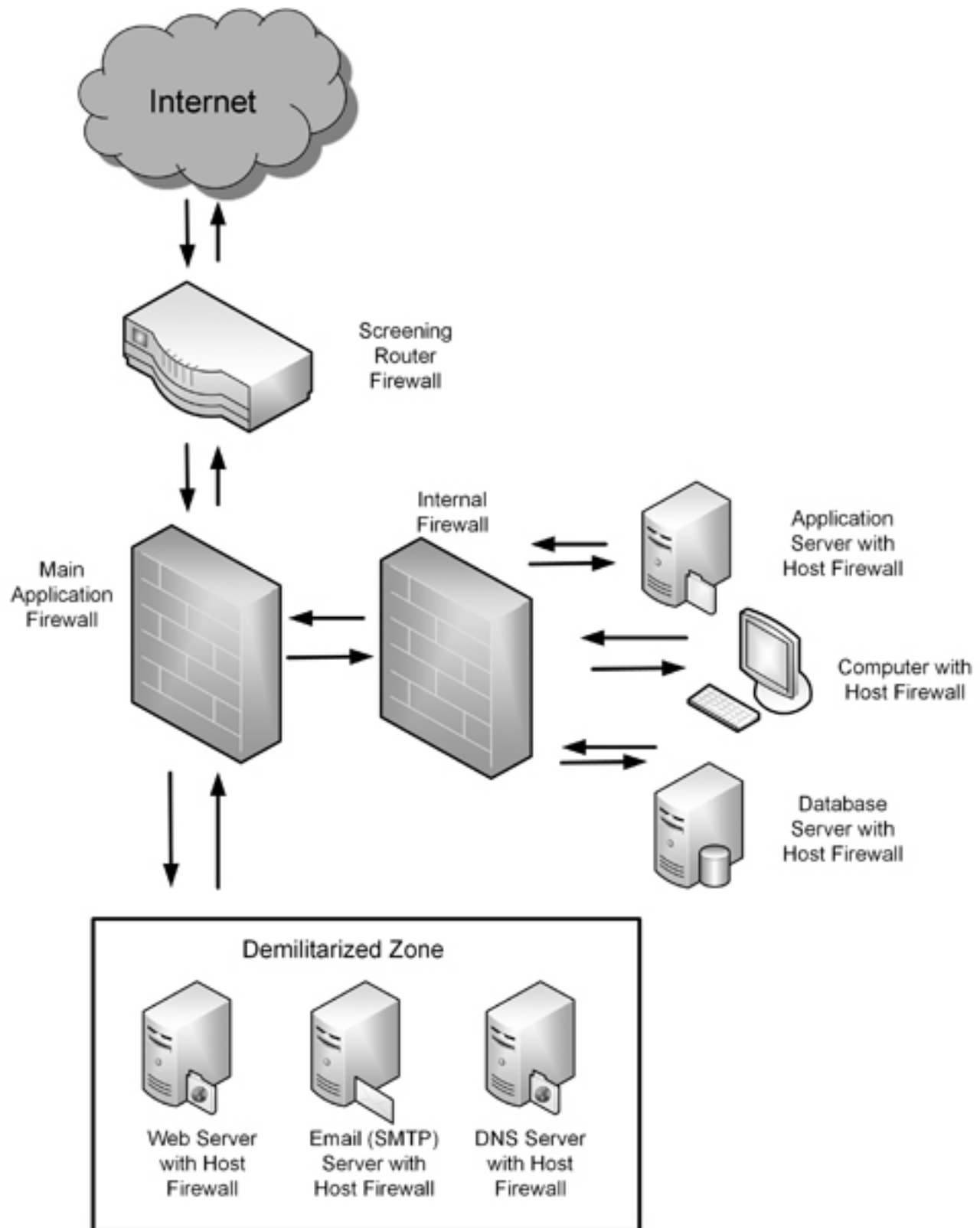


FIGURE 8.8 A Firewall Architecture for Defense in Depth

STATS BOX 8.1: SECURITY POLICY VIOLATIONS

Even when security is a top priority for organizations, employees can often find ways to not follow or violate security policies, such as by encrypting email or bypassing security controls such as firewalls, restricted access, or automatic logoff systems. In a survey of more than 700 senior IT and business decision makers in the United States and Canada, DataMotion found that three quarters of employees violate security policies at least occasionally (Hutton 2015).

Rendering Data Unreadable: Encryption

Encryption, also known as *cryptography*, is the use of mathematical algorithms to convert a message or data into scrambled information that makes it unreadable. The original message is called **plaintext**. The converted or unreadable text is called **ciphertext**. When the ciphertext is converted back to plaintext, this is referred to as **decryption**. The algorithm used to convert the message is called the **cipher**. The **encryption or decryption key** is information known only by the proper users of the encryption tool.

The ciphers used in [Learning Activity 8.6](#) are very simplistic. Ciphers used in encryption are much more complicated and use complex algorithms (not simply adding numbers and letters). The strength of an encryption technique is related to the length of the key. This is usually expressed in the number of bits the key has. The larger the size of the key, the more secure the encryption. This is because larger keys are harder to break since there are more combinations of bits possible. Today, keys in commercial use are 256 bits or longer. It is estimated that with advances in technology, a 64-bit key can be broken in a day or less. Understandably, a 256-bit, or even 1024-bit, key is much more secure.

[LEARNING ACTIVITY 8.6](#)

Breaking the Encryption

Security technologies are unlikely to be able to prevent all unauthorized access to data, applications, and systems. One way to provide additional protection for important data is through encryption. Before we discuss encryption in depth, let us explore what makes data unreadable.

Part 1

Given the plaintext a b c d e f g h I j k l m n o p q r s t u v w x y z and the resulting ciphertext b c d e f g h I j k l m n o p q r s t u v w x y z a, what is the cipher?

Part 2

Using the cipher, convert the words “computer lab closed.”

Part 3

Using the following cipher and your personally selected keys below, convert the text “Fun for Spring Break.”

Key selection:

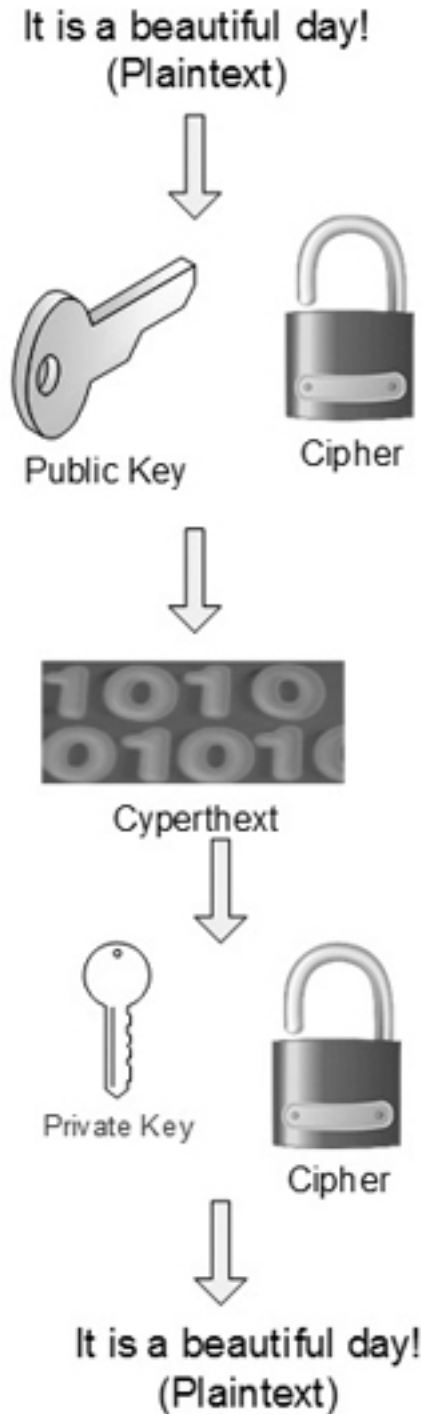
1. Pick a number from 1 to 5.
2. Pick a sign (+ or–).
3. Pick a symbol (!,@,#,\$,%,^,&,*).
4. Use this cipher to encode: new letter = original letter (sign selected) number, spaces replaced with symbol selected.
5. Compare your results with classmates.

Types of Cryptography

There are two main types of cryptographic systems used today: asymmetric or symmetric, as shown in [Figure 8.9](#). The systems are based on whether the same key is issued to encrypt and decrypt the data. In **asymmetric encryption**, two keys are used. The public key is used to encrypt messages. It is sent to any person or system with whom one wishes to exchange encrypted messages. Using the public key, anyone can encrypt messages for

the intended recipient, who will then use his or her private key to decrypt those messages. The public key and the private key are linked (forming a **key pair**), but only the recipient has the private key. This is also called *public key cryptography*, since one of the keys can be shared with anyone (public).

Asymmetric Encryption



Symmetric Encryption

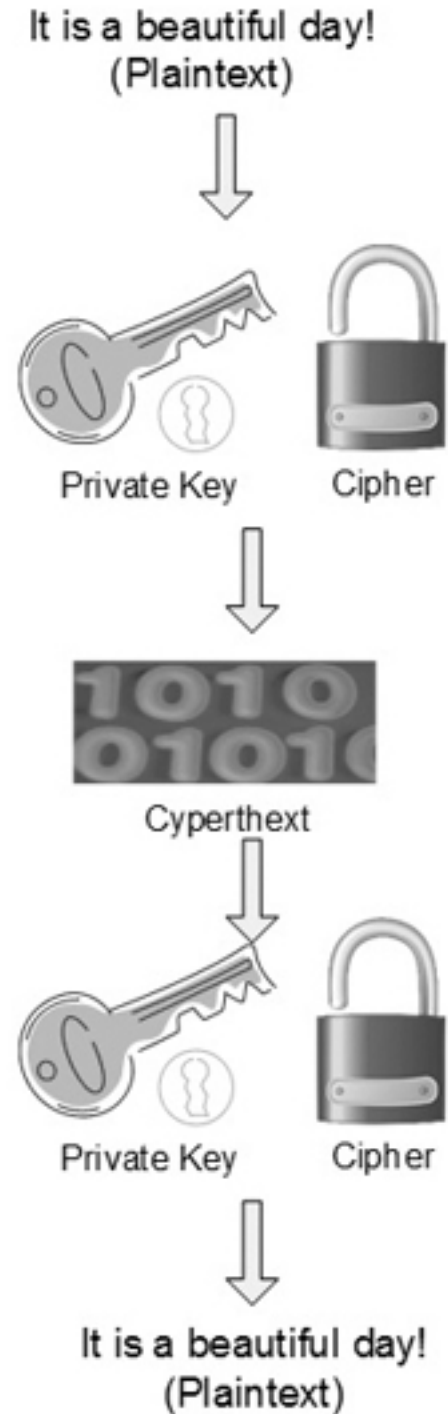


FIGURE 8.9 Symmetric versus Asymmetric Encryption

In **symmetric encryption**, the same key is used to encrypt and decrypt data. In this case, individuals have to be very careful with whom they share their encryption keys because these individuals or companies will also be able to decrypt their messages. It is very efficient, but it requires that both parties know the key and no one else. The problem is therefore how to distribute the key without having it intercepted by others. This is why both types

of encryption are often used together, with public key encryption used to distribute a secret key to a party you wish to interact with. Once the secret key is received, it can be used for symmetric encryption, since both parties know it. Finally, it is important to realize that encryption can be used for more than transmission of data. It can be used to protect data on servers and computers. For example, you could encrypt your data on your personal computer so that no one could access it without the proper key.

Encryption has many applications for securing data and transmissions. One of them is the **virtual private network (VPN)**. A VPN is a connection that makes use of an open wired network such as the Internet but that provides a secured channel through encryption and other security features. It is often used for employees to securely connect to their organizations from remote locations. VPNs function through the use of encryption. When the employee wishes to connect to the company's internal network, she requests a VPN connection. After inputting secret information, the employee's computer establishes an encrypted session with the company's server. (This is called a *handshake*.) Once both computers share the secret key (which is only for that session), all transmissions are encrypted until the VPN connection is dropped.

Encryption is also used for protecting information in business transactions online. When you shop online and have to enter your credit card information, you typically look for the lock icon or the https:// in the URL to indicate that the site is secure. If you double-click on the icon, you will see the security certificate that was issued to the website by a certificate-issuing organization such as VeriSign. [Figure 8.10](#) shows a sample certificate located in the Internet options of a browser application. This certificate includes a public key, which is sent to your browser when you connect to this secure Web page. The browser can then generate a secret key and send it to the server using the public key encryption, since only the server can decrypt this information (via the private key). Once the server receives the secret key, your browser and the server can communicate securely using this secret key (called a *session key*). The transmissions will be encrypted until the current session is dropped.



FIGURE 8.10 Sample Security Certificate

Virus Protection

Viruses are one of the most prevalent security threats in organizations. You should not underestimate the amount of money involved in terms of support personnel time involved in fixing virus problems. Fortunately, today antivirus software has become very easy to use and to keep up to date. Recall that a virus has a signature: the bit pattern that represents the virus. Antivirus software looks for these signatures or variations of them in files and systems. If they are found, the software can remove the virus, quarantine the file, or delete the file. The software can even detect viruses in emails and files as they are loaded but before they are opened. Once a new virus is identified, it usually takes fewer than 24 hours for specialists to decode it and write a protection for it. But viruses

are easy to write, with several tools for writing viruses available online. Symantec, one of the leading providers of antivirus software, states that there are now more than one million computer viruses in existence.

Unfortunately, most antivirus programs are primarily reactive. They only detect existing viruses or ones that look similar to an old virus archived in the software's database. Newer virus protection tools, called **behavioral-based antivirus protection tools**, look for suspicious behaviors in programs instead of just a virus's signature. One of the most important protections, however, remains user education about updating software and not downloading unknown executable files to their computers.

Wireless Security

Because more and more individuals are connecting their devices to the Internet and connecting to their organizations via wireless networks, we need to briefly discuss the additional issues related to wireless security. In reality, all the security solutions discussed so far can be used in the wireless environment. However, because the wireless networks typically broadcast their communications over the "airwaves," they are more susceptible to security breaches since they can be intercepted without physical connections to the devices.

The best protection for wireless networks remains encryption. The standards for wireless encryptions are numerous, and the most popular ones in America are called WEP and WPA. **WEP, Wired Equivalent Privacy**, is an older encryption algorithm, which today can be easily cracked within minutes (with proper knowledge and software tools). **WPA, Wi-Fi Protected Access**, replaced WEP with a more powerful encryption algorithm. However, this has been replaced by WPA2, which provides an even more powerful encryption algorithm and is widely available in most routers. So when setting up a home wireless network, users should select WPA2 encryption if their devices support it. A further protection for home wireless networks is to disable the broadcasting of the network's ID (SSID). Only with knowledge of the network's name can someone find it and connect to it (along with the WPA2, WPA, or WEP encryption key information).

Security Policies

Most medium to large organizations today have security policies, which describe *what* the general security guidelines are for the organization. **Security policies** tend to be for internal use and include a number of **security procedures**, which are specific statements describing *how* to implement the security policies. For example, a security policy could be "All users must change their passwords every two months." One of its related security procedures could then describe steps to be taken to change one's password. Another procedure could involve an automated system to force users to change their passwords every two months, while an additional one could include actions that should happen if a user attempts to enter an unacceptable (not strong) password. A security policy should have clear goals and objectives, a detailed list of security policies and procedures, and a list of actions for the enforcement of procedures.

Even with the best policies and procedures in place and with the best security technologies available, an organization may not be well protected if its users and employees fail to follow the policies and procedures or fail to use the technologies properly. This is where security education and training become very important. Users must be made aware of the risks involved, the tools available, and the consequences of not performing the proper security behaviors that are asked of them. Refer to the book's website for several tips on how to secure your computer, network, and data properly.

[BUSINESS EXAMPLE BOX 8.2](#)

How to Respond to a Security Crisis

While certain individuals in an organization are more concerned about being hacked (usually a chief-level officer or a security person), many believe that it is unlikely to happen to them. But what if it does? How should a

company react? Organizations can learn from what happened to Heartland Payment Systems in 2008–9 and from how they reacted.

Heartland Payment Systems, a financial transaction company, discovered in late 2008 that their system, which contained the information of more than 600 million credit card holders, had been hacked. Unfortunately, the company did not have a security crisis plan in place. Fortunately, they were quick to act and hired a crisis response corporation. The first order of business? To develop a plan to deal with employees, Wall Street, the media, and the customers and to do it quickly as opposed to waiting weeks or months after the breach happened. The company decided that it was better to provide full disclosure about what happened and be transparent about what was being done to address the situation. The company and their consultant agreed on two key objectives: (1) to show that they were going above and beyond expectations in terms of responsibility and accountability to deal with the huge data loss and (2) to develop a leadership position on dealing with identity theft after the crisis was over.

To achieve their objectives, the officers of the company quickly announced what type of data was hacked and what was not, conducted a great number of media interviews, and contacted a large number of their customers directly. They also discussed the situation with influential financial bloggers and industry analysts, created a dedicated website, and communicated all this to their employees fully and clearly.

In the end, the company was mainly successful in handling the crisis. They then explored new security programs and formed a security group. They also shared some of their key lessons learned: “Be prepared,” “Have a war room,” and “Figure out how you can make a difference in a bad situation.”

Source: “Case Study: Credit Card Payments Company ‘Runs to the Light’ as Security Breach Puts Reputation and Profits in Jeopardy.” 2010. *PR News* 66(35).

[LEARNING ACTIVITY 8.7](#)

Where’s the Security?

Now that we have explored all the security threats and solutions, we need to see how they fit together. For this learning activity, you need to map the threats to security and the goals of information security to the security solutions available. Prepare a table that contains the following information:

1. *Column 1:* List all the main security threats discussed.
2. *Column 2:* List all the security solutions that can address each of the security threats you have identified. (There might be many solutions for each threat.)
3. *Column 3:* For each security solution in column 2, indicate which security goal is met by the security solution.

CHAPTER SUMMARY

In this chapter, we discussed the security of information. We first defined information security and described the threats to information security. We then discussed the technologies and solutions related to information security and concluded the chapter with a discussion of information security policies.

Here are the main points discussed in the chapter:

- There are three main categories of information security threats: denial of service, unauthorized access, and theft and fraud. Denial-of-service threats are those that render a system inoperative, limit its capability to operate, or make data unavailable. They include intentional acts, such as viruses, malware, and email bombings; careless behavior, such as a lack of backups; and natural disasters. Unauthorized access threats refer to someone accessing systems and/or data illegally. Theft and fraud threats are related to the loss of systems or data due to theft or fraudulent activities, including illegal downloading or copying of software and theft of data using small hardware devices.

- There are three main goals that security tools and policies are meant to address: confidentiality, integrity, and availability (CIA). Confidentiality involves making sure that only authorized individuals can access information or data. Integrity involves making sure that the data are consistent and complete. Availability involves ensuring that systems and/or data are available when they are needed. Two additional goals are authentication (or authenticity) and nonrepudiation. Authentication means making sure that the parties involved are who they say they are and that transactions, data, or communications are genuine. Nonrepudiation refers to making sure one cannot renege on his or her obligations—for example, by denying that he or she entered into a transaction with a Web merchant.
- Security solutions and tools (also called security controls) can be classified as preventive, detective, or corrective controls. The goal of preventive controls is to stop or limit the security threat from happening in the first place. The goal of detective controls is to find or discover where and when security threats occurred. The goal of corrective controls is to repair damages after a security problem has occurred. Security controls can also be classified as physical or logical. Physical access controls are those security solutions that involve protecting physical access to systems, applications, or data, whereas logical access controls include security solutions that protect access to systems, applications, or data by ensuring users or systems are authenticated and allowed to have such access. Physical access controls can include locks for laptops, locked computer rooms, and secured rooms for backup storage. Logical access controls include user profiles, biometrics, firewalls, encryption, virus protection, and wireless security.
- There are many security solutions. The security solution of user profiles requires users to be assigned profiles that consist of a user identification (self-selected or assigned by the organization) and a set of privileges. Biometrics use human traits and characteristics to recognize individuals to grant them access or to identify them among other individuals. Firewalls are computers or routers that control access in and out of the organization's networks, applications, and computers. Encryption, also known as cryptography, is the use of mathematical algorithms to convert a message or information into a scrambled message or information that makes it unreadable. Antivirus software looks for virus signatures (patterns) in files and systems to prevent them from being executed. Wireless security is mostly done through encryption such as WEP and WPA.
- Security policies describe what the general security guidelines are for an organization, including procedures, enforcement mechanisms, objectives, and also list actions for the enforcement of procedures.
- Risk management is the process of identifying, assessing, and prioritizing the security risks an organization may face and deciding whether to accept the risks, mitigate the risks, or share the security risks by buying insurance.

REVIEW QUESTIONS

1. Briefly explain the three main goals of security and the additional two discussed in the text.
2. What is a denial-of-service attack, and what kind of events can lead to such an attack?
3. Explain how unauthorized access threats can occur.
4. Define preventive security controls, detective security controls, and corrective security controls. Provide two examples of each.
5. What are the various purposes of biometrics and how do they work?
6. What is a firewall and how does it work?
7. What are the two types of encryption discussed in the chapter and how do they differ?
8. How does antivirus software work?
9. What are the key steps required for wireless security?
10. What are security policies and procedures, and how are they related?

REFLECTION QUESTIONS

1. What is the most important thing you learned in this chapter? Why is it important?
2. What topics are unclear? What about them is unclear?
3. For each of the following security threats, suggest one preventive, one detective, and one corrective security control.
 - A virus is affecting the organization's intranet.
 - A hacker accesses consumer data on the company's database server to commit fraud.
 - A disgruntled employee steals trade secrets from the company's computers.
 - A construction worker breaks the data communication and electrical cables coming into the company's building.
4. Which biometric technologies are better used for identification and which are better used for verification? Explain why.
5. Explain what happens when you request your antivirus software to scan your hard drive.
6. A friend wants to send you encrypted messages. She asks you to send her both your public and private keys. What should your response be? Why? What should you send her? How will you send it? Does it matter?
7. List at least three security threats that a firewall will not protect a company against. Explain why.
8. Is a virtual private network a network or a security tool? Explain.
9. What do you believe are the most serious security concerns for the different types of networking architectures discussed in [Chapter 7](#)?
10. If an organization decides to accept a security risk instead of trying to mitigate it, would this still be considered risk management? Why or why not?

ADDITIONAL LEARNING ACTIVITIES

Learning Activity 8.A1

Identify all the security threats individuals can face when using social networking sites such as Facebook, LinkedIn, Instagram, and others. Create a table that lists the threats, your estimate of how serious each threat is (low, medium, high), and a suggestion for how such sites should go about addressing these security threats.

Learning Activity 8.A2

Perform research on encryption software that individuals can use for emails, their hard drives, or even mobile devices. Create a table that lists the various features of each major vendor and the costs for individual users like you. Then select one of the products and try it. Be prepared to discuss the advantages and disadvantages of the product you selected both for you as a student and for businesses that might want to use it.

Learning Activity 8.A3

A popular public key encryption tool is PGP (Pretty Good Privacy). Developed by Phillip Zimmermann, it was offered on the Internet for free on the MIT website for a while but then became a commercial product. Today, one can still get freeware PGP at the PGP International website: <http://www.pgpi.org/products/pgp/versions/>

[freeware/](#). Install PGP and create your key pair. Then exchange encrypted email messages with your teammates and encrypt files on your hard drive. Discuss how this could or could not be used for business.

Learning Activity 8.A4

Read the Constellation Energy Group security case on the course website. Prepare a report answering the following questions. You may need to perform extra research on the topic.

1. What is the case about?
2. Explain what *converged security operations* means.
3. Explain what is meant by political, logistical, and cultural challenges to implementing converged security operations. Provide some examples.
4. What are the similarities and differences between security and risk management?
5. What do you believe are the most important factors that help make converged security possible at Constellation?

Learning Activity 8.A5

Read [Appendix I](#), which discusses how to implement a security plan for an organization. Select a local small business that has at least 10 employees and develop a security plan for this business.

Learning Activity 8.A6

Find your university's security policy and identify the main components of this policy. Be prepared to discuss the following:

1. What threats are referred to?
2. What security technologies are included in the policy?
3. Select one example each of a specific policy and a specific procedure.
4. Who is responsible for ensuring that you, as a student, follow the policy?
5. What happens if you do not follow the policy?

Learning Activity 8.A7

Compare and contrast the security policy you found in [Learning Activity 8.A6](#) with the templates for security policies provided by the SANS organization: <http://www.sans.org/security-resources/policies/>.

Learning Activity 8.A8

Read the article by A. S. Horowitz, "Top 10 Security Mistakes," *Computerworld* (July 9, 2001): <http://www.computerworld.com/article/2582953/security0/top-10--security--mistakes.html>. Briefly explain each of the 10 mistakes. Then answer the following questions:

1. Where do we stand today on these security mistakes?
2. Why have we not improved more?

Learning Activity 8.A9

As computing technology changes, so do the threats to the security of information. Research the current state of threats, including spear-phishing and advanced persistent threats. Create a table with four columns. The first column should contain the name of the new threat. The second column should contain a definition of this new threat. The third column should identify how this threat builds on existing threats discussed in this chapter. Finally, column four should list what makes this threat different than existing threats discussed in this chapter. Be prepared to discuss these findings in class.

REFERENCES

- Davis, M. A. 2014. "Research: 2014 Strategic Security Survey." *InformationWeek*, May 1. http://reports.informationweek.com/abstract/21/12509/Security/Research:-2014-Strategic-Security-Survey.html?cid=smartbox_techweb_analytics_7.300005661
- Hutton, M. 2015. "Annual DataMotion Survey Reveals Employees Violating Security and Compliance Policies and Major Mobile Vulnerabilities." *DataMotion*, March 4. <http://www.datamotion.com/2015/03/annual-datamotion-survey-reveals-employees-violating-security-compliance-policies-major-mobile-vulnerabilities/>.

FURTHER READINGS

- APWG. 2014. Phishing Activity Trends Report, 4th Quarter 2014. <http://www.antiphishing.org/resources/apwg-reports/>.
- Berinato, S. 2004. *Anatomy of a Fraud*, *CSO Security and Risk*, October 1. <http://www.csoonline.com/article/2117911/fraud-prevention/anatomy-of-a-fraud.html>.
- Brandel, M. 2010, July 12. "Are You Listening?" *Computerworld* 44(14): 13. <http://www.computerworld.com/article/2550654/enterprise-applications/are-you-listening-.html>.
- Scarlet, S. D. 2005. "Death to Phishing." *CSO Security and Risk*, October 1. <http://www.csoonline.com/article/2119357/malware-cybercrime/death-to-phishing.html>.
- Toonkel, J. 2011. "SEC Said to 'Sweep' Advisory Firms for Social-Media Info." *Investment News*, February 14. <http://www.investmentnews.com/article/20110214/FREE/110219962/sec-said-to-sweep-advisory-firms-for-social-media-info>.
- Weise, J., and C. R. Martin. 2001. *Developing a Security Policy*, *Sun Microsystems*. <http://www.smps.reading.ac.uk/~swsellis/tech/solaris/performance/doc/blueprints/1201/secpolicy.pdf>.

Phishing Resources

<http://www.antiphishing.org>

<http://www.spamlaws.com/phishing.html>

GLOSSARY

Active content: Executable files on websites.

Antivirus software: Programs that look for virus signatures or variations of them in files and systems.

Application-level firewall: A firewall that verifies access to applications by requiring users to log into the firewall before they can access applications inside the organization (from outside).

Asymmetrical security warfare: One party must do everything to protect itself, while the other party (the attacker) only needs to find the one security weakness.

Asymmetric encryption: A type of encryption that uses two keys: a public key for encrypting and a private key for decrypting.

Audit logs: Software programs that can scan for unexpected actions to detect potential hackers.

Authentication: A process by which the identity of a transacting party is verified.

Authentication (biometrics): A type of security that matches the individual with his or her stored biometric data.

Availability: System and/or data are available when needed.

Backdoors: Ways for hackers to reaccess the compromised system at will.

Behavioral-based antivirus protection tools: Programs that look for suspicious behaviors in programs instead of just a virus's signature.

Behavioral biometrics: Biometrics that use human behaviors.

Biometrics: Technologies that use human features to recognize individuals and grant them access.

Cipher: An algorithm used to encrypt and decrypt plaintext.

Ciphertext: An encrypted (unreadable) message.

Confidentiality: Making sure that only authorized individuals can access information or data.

Corrective controls: Controls meant to repair damages after a security problem has occurred.

Decryption: Converting ciphertext back to plaintext.

Decryption key: A key used to convert the unreadable text into its original form.

Defense in depth: Multiple layers of security protections in place.

Denial-of-service threats: Threats that render a system inoperative or limit its capability to operate, or make data unavailable.

Detective controls: Controls meant to find or discover where and when security threats occur.

Dictionary attack: When all words of several dictionaries in multiple languages are tested as passwords with numbers before and after the words.

Disaster recovery: Procedures and tools to recover systems affected by disasters and destruction.

Distributed denial-of-service attacks (DDOS): When many computers are being used for DOS attacks.

DNA recognition: A type of security that analyzes segments from an individual DNA.

Dynamic firewall: Manages the requests as they occur, deciding on both denials and permissions as they arrive.

Dynamic signature recognition: A type of security that analyzes not only the signature but how it is written using pressure points.

Ear recognition: A type of security that analyzes the shape of the ear.

Email bombing: Sending a large number of requests, emails, or synchronization (SYN) messages to fill a target's mailboxes, systems, communication ports, or memory buffers with the intent of blocking legitimate messages from entering the systems or overloading the system to make it crash.

Encryption: The application of a mathematical algorithm to a message or information that scrambles that message or information to make it unreadable.

Encryption key: A key used to convert the text into an unreadable form.

External firewall: A firewall used to protect access to the internal network and computers of the organization.

Facial recognition: A type of security that analyzes facial features or patterns (faceprints).

Finger geometry recognition: A type of security that analyzes 3D geometry of the finger.

Fingerprint recognition: A type of security that analyzes ridges and valleys (minutiae) on the surface tips of human fingers.

Firewall: A computer or a router that controls access in and out of the organization's networks, applications, and computers.

Firewall appliance: The hardware and software to perform firewall function.

Gait recognition: A type of security that analyzes the walking style or gait of individuals.

Hactivism: A type of hacking in which hackers that try to find information that, if revealed, will advance human causes.

Hand geometry recognition: A type of security that analyzes geometric features of the hand, such as length of fingers and width of the hand.

Host firewall: A firewall installed on a computer.

Identification (biometrics): Identifying an individual from an entire population of individuals with stored biometric data.

Information security: A set of protections put in place to safeguard information systems and/or data from security threats such as unauthorized access, use, disclosure, disruption, modification, or destruction.

Integrity: When data are consistent and complete.

Internal firewall: A firewall used inside an organization, between departments or divisions.

Iris/retina recognition: A type of security that analyzes features (eyeprints) in the iris or the patterns of veins in the back of the eye (retina).

Key pair: A linked public key and private key.

Keystroke capture programs: Software that logs all information entered into a computer.

Keystroke recognition: A type of security that analyzes the rhythm and patterns of individuals' keystrokes on keyboards.

Knowledge (in security access): When an individual needs to know something to gain access.

Logical access controls: Security solutions that protect access to systems, applications, or data by ensuring users or systems are authenticated and allowed to have such access.

Nonrepudiation: Making sure a party cannot renege on obligations—for example, by denying that he or she entered into a transaction with a Web merchant.

Odor recognition: A type of security that analyzes an individual's odor to determine identity.

Packet-level firewall: A firewall that controls access by looking at the source and destination addresses in data packets. Also called *a screening level firewall*.

Packets: Small units of data that flow through networks, allowing for the transmission of messages.

Password crackers: Software used to recover forgotten passwords.

Personal firewall: A firewall installed on a given personal computer.

Physical access controls: Controls that involve protecting physical access to systems, applications, or data.

Physiological biometrics: Using physical traits to identify individuals.

Plaintext: Original message before it is encrypted.

Possession: When an individual owns a form of identification.

Preventive controls: Controls meant to stop or limit the security threat from happening in the first place.

Principle of least privilege: A form of access control in which users are only given permission to access the minimum amount of information required to complete their jobs.

Risk management: The process of identifying, assessing, and prioritizing the security risks an organization may face and deciding whether to accept, mitigate, or share the security risks.

Rootkits: Software that allows hackers to have unfettered access to everything on the system, including adding, deleting, and copying files.

Security: Protection against security threats.

Security levels: The layers of protection technologies and policies used to secure stored information.

Security policies: Statements describing what the general security guidelines are for an organization.

Security procedures: Specific statements describing how to implement the security policies.

Security threats: Broadly categorized as denial of service, unauthorized access, and theft and fraud.

Smurfing: When a hacker uses an innocent third party to multiply the messages being sent to the intended target.

Sniffer: Software that monitors transmissions, capturing unauthorized data of interest.

Social engineering: Tricking individuals into giving out security information. Sometimes called *phishing*.

Software ports: Applications installed and running on a computer.

Spamming: Sending emails to many individuals at once, sending unsolicited commercial email to individuals, or targeting one individual computer or network and sending thousands of messages to it.

Spoofing: Pretending to be someone else (or another computer) to enter a system or gain attention.

Spyware: A form of virus that logs everything users do on their computers, unbeknownst to them.

Static firewall: A firewall that has predetermined ways of dealing with transmission requests.

Static signature recognition: A security measure that compares scanned or ink signatures with stored signatures.

Stealth virus: A more advanced virus that changes its own bit pattern to become undetectable by virus scanners.

Symmetric encryption: A form of encryption where the same key is used to encrypting and decrypting data.

Target-of-opportunity threats: Threats (such as viruses) sent out to find any victim possible.

Theft and fraud threats: Threats related to the loss of systems or data due to theft or fraudulent activities.

Traits: Physical or behavioral human characteristics needed to gain access to systems or data.

Trojan horses: Viruses embedded into a legitimate file.

Unauthorized access threats: Individuals who access systems and/or data illegally.

User profile: Assigned profiles that consist of a user identification, a password, and a set of privileges.

Virtual private network (VPN): A connection that makes use of an open wired network such as the Internet but that provides a secured channel through encryption and other security features.

Virus: A computer program designed to perform unwanted events.

Virus hoaxes: False virus alerts sent and resent by individuals.

Virus signature: Bit patterns of the virus that can be recognized.

Voice recognition (speaker recognition): A security measure that analyzes voice to determine the identity of a speaker; different from speech recognition (determining *what* is being said).

Wi-Fi Protected Access (WPA): A recent and powerful encryption algorithm for wireless security.

Wired Equivalent Privacy (WEP): A protocol that uses encryption established via a preshared key known to the router and the wireless device or computer on a wireless network.

CHAPTER 9

PROTECTING THE CONFIDENTIALITY AND PRIVACY OF INFORMATION

LEARNING OBJECTIVES

By reading and completing the activities in this chapter, you will be able to

- Understand the various threats to information privacy
- Identify technologies and solutions used to protect the confidentiality and privacy of information
- Explain how information privacy is a component of the PAPA ethical framework
- Discuss the relationship between information privacy and information security

CHAPTER OUTLINE

- [Focusing Story: Privacy and Smartphones](#)
- [Learning Activity 9.1: Finding Mindy](#)
- [Information Privacy Threats](#)
- [Data Collection](#)
- [Learning Activity 9.2: Concern for Information Privacy](#)
- [Learning Activity 9.3: Privacy Pizza](#)
- [Consequences of Privacy Violations](#)
- [Technologies and Solutions for Information Privacy](#)
- [Learning Activity 9.4: Surveillance Societies around the World](#)
- [Learning Activity 9.5: Privacy Policy Creation](#)
- [Learning Activity 9.6: Why Your Advisor Can't Talk to Your Parents](#)
- [Government Information Privacy Regulations](#)
- [Privacy and Ethics](#)
- [Learning Activity 9.7: PAPA, Privacy Policies, and FERPA](#)
- [Ethical Decisions](#)
- [Learning Activity 9.8: Making Ethical Decisions](#)
- [Relationship between Security and Privacy](#)
- [Chapter Summary](#)
- [Review Questions](#)
- [Reflection Questions](#)
- [Additional Learning Activities](#)
- [References](#)

- [Further Readings](#)
- [Glossary](#)

Privacy of information is the confidentiality of the information collected by organizations about the individuals using their services (Van Slyke and Bélanger 2003). It can also be defined as one's ability to control information about oneself (Bélanger, Hiller, and Smith 2002). From an individual's perspective, it refers to a desire to control or influence data about oneself (Bélanger and Crossler 2011). Privacy of information is a very important concept for individuals and organizations alike. Many students may have faced issues with the privacy of their information when friends posted something about them on Facebook or Twitter without their prior approval. This may have been just for fun or may have caused some tensions between friends. However, as students move to the workplace, they will realize that organizations need to be even more keenly aware of information privacy concepts, since workers, professionals, and managers have access to and deal with great amounts of information on a daily basis. Therefore, everyone has to be concerned not only about their own information privacy but also about the privacy of information of others, including customers, employees, business partners, students, parents, children, and more.

FOCUSING STORY

Privacy and Smartphones

Most students today have smartphones. Depending on the settings on these devices, it is likely that location information is associated with every picture taken. The following video demonstrates how this happens and the possible implications. Please watch the video and answer the questions below.

<https://www.youtube.com/watch?v=N2vARzvWxwY>

FOCUSING QUESTIONS

1. What could people do with the information that is available on the pictures?
2. Who should educate people about this?
3. What else could be geo-tagged on your phone?
4. Why would all consumers not disable this feature?
 - Is there a reason not to?
 - What is the trade-off?

LEARNING ACTIVITY 9.1

Finding Mindy

Students often wonder if information privacy is really as much of a problem as the media tries to convey. In order to start looking into an answer for this question, let us see how information privacy can affect the lives of individuals. Please read the following story and be prepared to discuss the questions in class.

After a long week of school, Mindy was eager to get home, grab a snack, and relax in front of the computer. Signing on with her screen name SftBallGr116, she noticed Jimmyg114 was online, whom she met a month ago in a sports chat room.

SftBallGr116:

Hey you! I think I'm being stalked LOL!

Jimmyg114:

LOL really, why?

SftBallGr116:

Well I thought this car was following me on my walk home today. But I think it was just my imagination LOL

Jimmyg114:

Haha someone's paranoid! Better stop giving out your info online.

SftBallGr116:

No way. I don't do that. I've heard the terrible stories.

Jimmyg114:

Anyway didn't you have a game today?

SftBallGr116:

Yeah and we won again. 3 in a row!

Jimmyg114:

Nice, who did you guys play?

SftBallGr116:

The Warriors. They were pretty good.

Jimmyg114:

What is your team called?

SftBallGr116:

We are the Newtown Hawks. We just got new uniforms. I love them.

Jimmyg114:

Really what do they look like?

SftBallGr116:

They are blue and white with an awesome hawk logo on the front.

Jimmyg114:

Nice, what position do you play?

SftBallGr116:

Third base. We play them again for our homecoming in 2 weeks. My parents and friends are all coming. It is a big game. Well I have to get going. My parents will be home any minute and I was supposed to do the dishes. LOL

Jimmyg114:

LOL ok catch you later.

Later, Jimmyg114 went to the member's menu to search for her profile. He began to write everything down he knew about SftBallGr116 so far.

Name: Mindy

Birthday: July 19, 1996

Age: 13

Location: Maryland

Hobbies: softball, jogging, skiing, hanging out at the mall

Besides this information, he knew she lived in Newtown because she had just told him. He knew she stayed by herself until 6:00 p.m. every evening until her parents came home from work. He knew she played softball on Thursday evenings on the school team, and the team was named the Newtown Hawks. Her favorite number, 19, was printed on her jersey. He knew she was in the eighth grade at Newtown High School. This information had been gathered over the past couple weeks.

By Tuesday, Mindy forgot about the car following her.

Her game was well under way when she noticed a man she had never seen before staring at her. This startled her at first. Occasionally she would glance over at him, and he would smile. He seemed harmless. When the game finished, he wandered around, watching Mindy as she talked with her coach. Mindy began to walk home and the man followed quietly behind her. Keeping a safe distance, the man watched Mindy walk into her house. He now knew her exact location.

FOCUSING QUESTIONS

1. How much of the information provided by Mindy to Jimmy14 would you consider *private*?
2. How much of that information would be available online if Mindy did not interact with Jimmy14?
3. What types of personal information do you as a student care about protecting normally? Are you going to be more careful?
4. What potential risks do Mindy and her family now face?

Source: This story circulated on the Web at a certain time period in the mid-2000s. We do not know the author of the story.

Information Privacy Threats

There are many possible threats to information privacy—for example, dealing with collection and unauthorized secondary use of data, improper access to data, and errors in data (Smith, Milberg, and Burke 1996). Inaccuracies or **errors in data** can have serious impacts on individuals—for example, those applying for jobs or loans. **Improper access to data** deals more with the security of information, as discussed in the previous chapter with the security threat of unauthorized access. The information privacy threats of data collection and unauthorized secondary use, however, are worth discussing in more depth.

Data Collection

The collection of data from individuals is not a new concern, and the concept of privacy has been explored and discussed for centuries. One of the major differences today, however, is that as communications and information have been digitized, it has become easier and faster to collect ever-increasing amounts of information. Specifically, with the advent of advanced information and communication technologies, the **data collection threat** means that data can be collected, aggregated, and analyzed at a faster pace and in larger volumes than ever. Of a greater concern sometimes is the fact that data can be collected without anyone's awareness—for example, through the use of cookies. **Cookies** are small text files that store information on your computer about you or your computer when you browse or enter information into certain websites.

Another hidden data collection approach is **clickstream data**, which tracks online browsing behaviors. The tracking is done by software that looks at the IP address of the computer connecting to a site, identifying what page the computer connected from, what page it goes to after the current one, how often it connects to this site, and whether actual purchases are made from this site. Thorough analysis of this data can then give marketers an indication of successful and unsuccessful online ads, referring sites, and other information on the preferences of each user. Customized ads can also be delivered to the consumer's screen. Interestingly, it's likely no one would

agree to be followed in his or her buying decision process in a physical retail store. Imagine someone walking with you and observing you as you stroll through a Wal-Mart and look at various products! Yet online tracking of consumers is a regular occurrence.

The proliferation of data sources, tools to manipulate these data, and online sites collecting data in today's interconnected society leads to more data being available and to individuals being increasingly concerned about the privacy of their information. Current technology allows easy loading of information from online forms directly into databases. For companies, this is a major advantage, since the data are loaded immediately (faster) and accurately (no transcribing errors and no problems dealing with unreadable writing; Van Slyke and Bélanger 2003). However, as more information is being stored online, consumers are becoming increasingly concerned with losing control of how their information is being collected and used.

Information privacy is also an important concern for corporations. The increased ability to store consumer information makes corporations targets for hackers trying to gain access to the vast amount of consumer information that they store, causing an increase in the number of breaches that companies are experiencing. For example, customers who shopped at Target during December of 2013 provided their credit card information to Target. Hackers then attacked Target to gain access to this information (McGrath 2014). As more information continues to be collected and accessible via the Internet, it is unlikely that these trends will change any time soon.

[LEARNING ACTIVITY 9.2](#)

Concern for Information Privacy

A number of reports and studies relate the various concerns that individuals and organizations have about information privacy. For this learning activity, search the Internet for statistics on the level of concern either individuals or organizations have about sharing information electronically. Note any benefits reported as trade-offs that might overcome these concerns for sharing information. Be prepared to discuss your findings in class.

Secondary Use of Information

Unauthorized secondary use of information refers to the use of data for purposes other than those for which they were originally collected. For example, you enter your information on a website to register for the warranty of your new digital camera, but then the company uses your information to send you marketing ads about its other products. Information privacy refers to having some level of control over these potential secondary uses of one's personal information. *Function creep* is another term used to refer to data being used for other functions beyond those purposes for which they were collected. Often, individuals are given the option to opt in or opt out of secondary use on websites. When you **opt in**, you have to specifically state that you agree that your data can be used for other purposes, often to receive special deals or information from partner companies. When you **opt out**, you have to make sure you tell the company you do not want your data shared with others or used for other purposes. The trick is that sometimes you have to click a box to opt out and sometimes you have to unclick one. If you forget, by default you are agreeing to let the companies share or use your information.

In summary, when information collection and use are not regulated, individuals have the responsibility of protecting their own (or others') information, particularly in the United States. However, it is often the case that individuals are not aware of the risks or do not know how to protect their own information. Often, people make a choice to give this information because it provides convenience or personalization of one's online experience. These preferences do vary around the world.

[LEARNING ACTIVITY 9.3](#)

Privacy Pizza

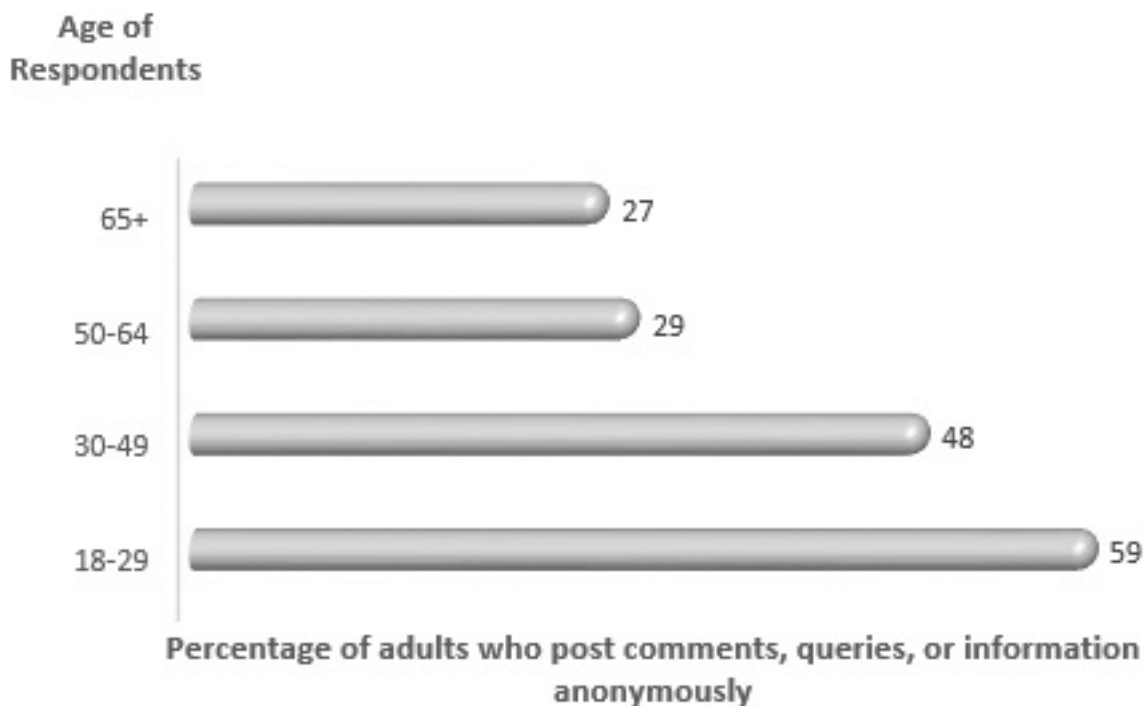
Your instructor will present a video titled *Privacy Pizza* in class or may direct you to the course website for you to watch the video individually before class. As you watch the video, make notes on the types of information and

technologies that are discussed and/or used in the video. The *Privacy Pizza* video can also be found at <https://www.aclu.org/ordering-pizza>. Be prepared to answer the following questions:

1. Do you think access to the various types of information identified is regulated or not?
2. For the technologies identified, are the technologies widely available today?
3. How likely is it that a pizza shop/company can use such technologies?
4. What can someone do to avoid this situation from happening to him or her?

STATS BOX 9.1: ANONYMITY ONLINE

As more opportunities to interact and discuss topics online emerge, remaining anonymous to various people has become an important step that some want to take. Different age groups are believed to post comments anonymously online. The Pew Internet and American Life Research Center studied this question by surveying 607 adults and found that indeed there are some differences, as can be seen from the figure below (Madden 2014).



Source: Based on data from Madden, M. 2014. *Public Perceptions of Privacy and Security in the Post-Snowden Era*, <http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/>.

Consequences of Privacy Violations

Individual Consequences: Identify Theft

The issues faced by Mindy in [Learning Activity 9.1](#) are very serious, since her physical well-being could have been at stake. Others, including adults, elderly parents, and small business owners, can also face serious consequences when people take their personal information for fraudulent activities. This is the concept of **identity theft**.

Identity theft cases have been increasing substantially in recent years. The Javelin Strategy and Research Center (<https://www.javelinstrategy.com>) reports that there were more than 12 million identity theft victims in 2014 in the United States. Their studies also show that as the ability to pay for products electronically using smartphones has emerged, the likelihood of having money stolen where the transaction occurs has also increased. In addition to these high-tech methods of identity theft, it is important to protect yourself from low-tech methods of identity

theft as well, including the stealing of wallets, mail, and other physical documents that contain people's personal information. As seen in the previous chapter, transmitting information online is relatively secure, but as new mobile technologies are emerging, this is changing. Furthermore, what happens after the information is received by local organizations can sometimes not be as secure. Identity theft can have several negative consequences for individuals, including financial, social, and emotional impacts.

Students are often concerned that their data are being stolen from the Web when they acquire some goods or services online. In reality, as stated in the previous paragraph, the risks are greater that fraudsters or identity thieves access large amounts of information from unsecured databases. Often, individuals who illegally access these data then resell it on the black market. It is difficult to have precise numbers on the size of this market, but various researchers and centers have identified the value of your information on the black market. How much would you be willing to pay for the following?

- A valid credit card number with a security code
- Valid bank account details, including the PIN (personal identification number)
- A valid Social Security number
- A completely new (valid) identity

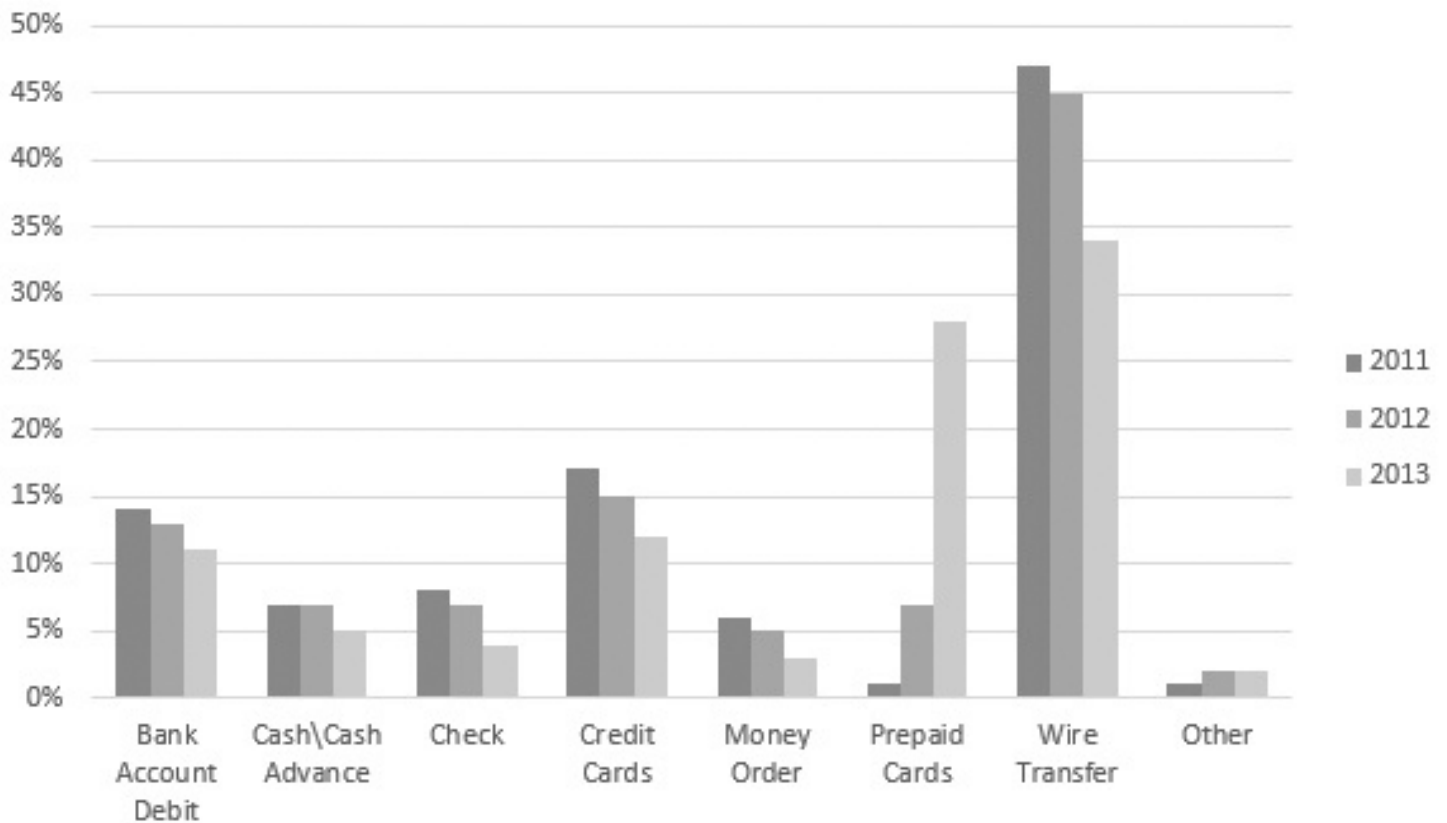
The best way for individuals to protect themselves from identity theft is to follow basic security guidelines and common sense. The Identity Theft Resource Center (<http://www.idtheftcenter.org>), a not-for-profit organization, has been created to help identity theft victims and offers very useful information about protection against identity theft and what to do if it happens to you.

The following are some examples of the recommended actions:

- Do not use your Social Security number unless it is absolutely needed.
- Shred everything that has any data about you.
- Place outgoing mail at the post office or locked collection box.
- Password protect financial accounts with strong passwords and two-factor authentication, if available.
- Really check the statements you receive.
- Request photo identification when someone asks for your information, and do not give it out over the phone, Internet, or mail unless you initiated the contact.
- Destroy digital data by going beyond a simple delete.
- Limit the information provided on your checks.
- Request your free annual credit report and check it.

STATS BOX 9.2: FRAUD TYPE FROM IDENTITY THEFT

Every year, the Federal Trade Commission (FTC) collects information on identity theft complaints and on fraud committed with someone else's identity in the United States. The figure below shows the types of fraud that are committed this way, computed from FTC complaint data. As can be seen, wire transfer fraud is by far the most common type of fraud being committed. This involves stealing money by intercepting the electronic communications between two financial institutions, such as banks. Other large categories of fraud include credit cards, bank account debits, and most recently, prepaid cards.



Types of Fraud Committed through Identity Theft

Source: Based on data published by the Federal Trade Commission, available at <https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2013/sentinel-cy2013.pdf>.

Organizational Consequences: Company Reputation

For organizations, information privacy violations also have serious consequences. There are, however, two sides to the issue here. Organizations have the responsibility of protecting their customers' data, but they are sometimes the ones infringing on the privacy of their clients.

If organizations fail to protect the privacy of their customers' information, then their reputations can suffer. There are many examples of companies' reputations being at stake. In December 2013, right in the midst of the Christmas shopping season, Target reported that as many as 40 million credit and debit card numbers, along with the cards' expiration dates and CVVs (card verification values), had been stolen. As the investigation unfolded, it turned out that information of as many as 70 million people was actually stolen. This resulted in a lower stock price and lost sales for Target as people decided to take their Christmas shopping elsewhere (McGrath 2014).

Similar things have happened to other companies over the years. For instance, TJX Co., owner company of approximately 2,500 retail stores, including T.J. Maxx, Marshalls, Winners, and HomeSense, among others, reported it had experienced a serious (and extended) breach of its databases, exposing information on more than 45.7 million credit and debit cards. The same year, Talves, a subsidiary of the Canadian Imperial Bank of Commerce (CIBC), lost a backup hard drive that contained personal information on approximately 470,000 clients, including addresses, signatures, names, dates of birth, social insurance numbers, and financial information (Stewart 2007; Charters 2008). In both cases, many customers stopped doing business with these companies.

STATS BOX 9.3: THE BLACK MARKET FOR STOLEN IDENTITIES

Identity theft is an increasingly prevalent issue because of the value of people's information. However, this information cannot be sold through traditional business channels. Therefore, a black market has emerged for

people's information, with different values for different pieces of information. The table below shows what the value of different stolen information is worth.

Stolen Information	Value
Credit card	\$0.50 to \$20.00
Email account	\$0.50 to \$10.00 per 1,000 accounts
Scan of passport	\$1.00 to \$2.00
Cloud account (command and control centers)	\$7.00 to \$8.00
Gaming account	\$10.00 to \$15.00
Social network	\$2.00 to \$12.00 per 1,000 followers
Hotel reservation/train ticket/airline ticket	10% of asking price
Online gift card	50% to 60% of nominal value

Source: Symantec. 2014. *Underground black market: Thriving trade in stolen data, malware, and attack services*. <http://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services>.

The costs of privacy breaches can be enormous for the companies involved. First, they may lose current and future customers. Second, they have to repair the breaches. And third, they have to compensate customers for their potential identity theft issues. In order to deal with the privacy breach, Target had to pay \$10 million to settle a class-action lawsuit, with breach victims eligible to receive as much as \$10,000 each (though this likely won't happen after the lawyers take their cut of the lawsuit; Riley and Pagliery 2015).

Finally, but not least, privacy breaches in organizations can directly impact the organization if the information that is leaked concerns the organizations' patents, trade secrets, or other intellectual property.

Technologies and Solutions for Information Privacy

Now that we understand the broad concepts of information privacy threats, it is important to further discuss the particular roles that technology can play in both infringing on information privacy and protecting one's information privacy. One technology that we will discuss is cookies. Some of the tools that we describe in this section, however, are more like approaches to information privacy rather than tools. For example, a privacy policy on a website is more about the content and whether it is applied properly than about technology to create a policy. Similarly, privacy seals and government regulations toward privacy are ways to protect you online, but they are more like tools and techniques than they are technologies.

Cookies and Cookie Managers

Websites often use **cookies**, small text files located on your computer, to temporarily (or sometimes for as long as you have your computer) store information about you, your accounts, and your computer. Information is stored in a cookie every time you enter information and are asked, "Do you want this to be remembered?" Cookies provide convenience to individuals. Because the information is stored on the computer, you do not have to retype all the account information or addresses or even remember your password to access a website that has stored information in the cookie file. Information not typed in can also be stored in cookies. For example, the website can record information such as your IP (Internet Protocol) address, the domain name of your computer, the length of time you stay on a specific Web page, and so on. When the user accesses one of the addresses in the address range of the website that stored the cookie, the browser transmits all the information retained in the cookie to the

server of the website the user is currently browsing. Any item used to personalize your experience on the Web uses a set of cookies. Examples of cookies are shown in [Figure 9.1](#).

Web site	Hits	Accessed Date	Modified Date	Created Date	Size	User	Filename	Status	Ad	Domain
addthis.com	9	5/23/2011 2:49:29 ...	5/23/2011 2:49:29 ...	5/23/2011 2:49:29 ...	401	france belanger	france_belanger@addthis[1].txt	Active	Unkno...	addthis.com
adms.com	3	5/23/2011 2:48:24 ...	5/23/2011 2:48:24 ...	5/23/2011 2:48:24 ...	285	france belanger	france_belanger@adms[1].txt	Active	Unkno...	adms.com
atdmt.com	2	5/23/2011 2:44:51 ...	5/23/2011 2:44:51 ...	5/23/2011 2:44:51 ...	193	france belanger	france_belanger@atdmt[2].txt	Active	Unkno...	atdmt.com
cnet.com	10	5/23/2011 2:44:56 ...	5/23/2011 2:44:56 ...	5/23/2011 2:44:42 ...	692	france belanger	france_belanger@cnet[2].txt	Active	Unkno...	cnet.com
com.com	2	5/23/2011 2:49:18 ...	5/23/2011 2:44:50 ...	5/23/2011 2:44:50 ...	95	france belanger	france_belanger@com[1].txt	Active	Unkno...	com.com
crowdscience.com	1	5/23/2011 2:44:57 ...	5/23/2011 2:44:57 ...	5/23/2011 2:44:57 ...	93	france belanger	france_belanger@crowdsien...	Active	Unkno...	crowdscience.com
doubleclick.net	5	5/23/2011 2:49:21 ...	5/23/2011 2:49:21 ...	5/23/2011 2:49:21 ...	123	france belanger	france_belanger@doubleclick...	Active	Unkno...	doubleclick.net
download.cnet.com	5	5/23/2011 2:47:37 ...	5/23/2011 2:44:57 ...	5/23/2011 2:44:57 ...	390	france belanger	france_belanger@download.c...	Active	Unkno...	cnet.com
eloqua.com	2	5/23/2011 2:48:35 ...	5/23/2011 2:48:35 ...	5/23/2011 2:48:35 ...	188	france belanger	france_belanger@eloqua[2].txt	Active	Unkno...	eloqua.com
google.com	5	5/23/2011 2:47:37 ...	5/23/2011 2:44:38 ...	5/23/2011 2:44:38 ...	354	france belanger	france_belanger@google[3].txt	Active	Unkno...	google.com
google.com/verify	1	5/23/2011 2:44:26 ...	5/23/2011 2:44:26 ...	5/23/2011 2:44:26 ...	130	france belanger	france_belanger@google[2].txt	Active	Unkno...	google.com
imworldwide.com/cgi-bin	2	5/23/2011 2:44:51 ...	5/23/2011 2:44:51 ...	5/23/2011 2:44:51 ...	226	france belanger	france_belanger@imworldwi...	Active	Unkno...	imworldwide.com
maxa-tools.com	5	5/23/2011 2:47:37 ...	5/23/2011 2:46:59 ...	5/23/2011 2:46:59 ...	363	france belanger	france_belanger@maxa-tool...	Active	Unkno...	maxa-tools.com
nisoft.net	6	5/23/2011 2:49:20 ...	5/23/2011 2:49:20 ...	5/23/2011 2:49:20 ...	375	france belanger	france_belanger@nisoft[2].txt	Active	Unkno...	nisoft.net
scorecardresearch.com	1	5/23/2011 2:44:53 ...	5/23/2011 2:44:53 ...	5/23/2011 2:44:53 ...	115	france belanger	france_belanger@scorecardre...	Active	Unkno...	scorecardresearch...
tynt.com	1	5/23/2011 2:45:01 ...	5/23/2011 2:45:01 ...	5/23/2011 2:45:01 ...	92	france belanger	france_belanger@tynt[1].txt	Active	Unkno...	tynt.com
webroot.com	17	5/23/2011 2:48:36 ...	5/23/2011 2:48:36 ...	5/23/2011 2:48:18 ...	1,051	france belanger	france_belanger@webroot[1]...	Active	Unkno...	webroot.com

FIGURE 9.1 Cookies Identified with IECookiesView (NirSofer; see [Table 9.1](#))

In terms of technologies to deal with cookies, there are many options. The simplest option is the settings you use on your Internet browser. The privacy settings allow you to state whether or not you allow cookies and what types of cookies should be automatically accepted. If you set your computer to be superprivate, most cookies will not work, and then many websites will not allow you to use their pages. If you set it your privacy settings too low, then most information about you and your computer will be stored and can be used by websites. The right balance depends on your privacy preferences. Different operating systems and browsers have different ways to deal with cookies. One organization, [AboutCookies.org](http://www.aboutcookies.org) (<http://www.aboutcookies.org>) shows you different ways to control or delete cookies from your computer.

There are also **cookie managers** that can be downloaded for free or for a fee. These give you more details about which cookies are stored and what is stored in them and allow you to delete them. [Table 9.1](#) shows you sample cookie managers, but many more exist on the Web. Finally, many new antivirus, antispysware, and other security programs automatically scan for and delete unnecessary cookies.

TABLE 9.1 Sample Cookie Management Tools

Name	Description	Creator and Link
Cookie Crusher	Cookie manager	The Limit Software: http://download.cnet.com/CookieCrusher/10006576.html
Cookie Monster	Cookie manager	AMPsoft: http://www.ampsoft.net/utilities/CookieMonster/
Cookie Pal	Cookie manager	Kookaburra Software: http://www.kburra.com/cpal.h
IECookiesView	Cookie Manager for Mozilla and Internet Explorer browsers	NirSofer: http://www.nirsoft.net/utills/iecookies.html
Maxa Cookie Manager	Freeware cookie manager	Maxa Research: http://www.maxa-tools.com/cookie.m

LEARNING ACTIVITY 9.4

Surveillance Societies around the World

We discussed privacy as having consequences for individuals and organizations. Privacy can also have global aspects as well. However, the concern for privacy and how it influences people's decisions is different in various countries. Visit the EMC Privacy Index (<http://www.emc.com/campaign/privacy-index/index.htm>) and explore the different infographics available. As you do so, be prepared to answer the following questions:

1. In what contexts are people most willing to trade their privacy? Least willing?
2. In which countries are people most willing to trade their privacy for services? Least willing?
3. What is a paradox, and how does it affect people in different information-sharing contexts?

LEARNING ACTIVITY 9.5

Privacy Policy Creation

This activity will allow you to explore the contents of privacy policies. Based on the following scenario, create an appropriate policy.

Scenario: Two of your best friends from class have asked you to join them in a new venture. They are starting to sell customized, high-quality, university-branded apparel to fellow students and mostly to wealthy alumni. They want you to be the chief technology officer, and you have enthusiastically joined with them. As you oversee the development of the website for the company, which you are outsourcing, you have been asked to provide a privacy policy regarding your handling of customer data. This policy will be on the website at the bottom of the pages in small print.

Activity

1. Go to one of these sites (or another tool that you find online) to help generate a privacy policy:
 - a. [PrivacyPolicies.com](http://privacypolicies.com/): <http://privacypolicies.com/>
 - b. Free Privacy Policy: <http://www.freeprivacypolicy.com>
2. Bring your resulting policy to class (if the activity is performed before class).
3. Be prepared to discuss how you created your policy and which decisions you had to make.

Privacy Statement or Policy

Most serious companies who do business online have privacy policies. A **privacy policy** is a statement that describes what the organization's practices are with respect to the privacy of its customers. In general, most privacy policies include some or all of the following information:

- What data are collected
- How the data are collected
- What the organization is doing with the data
- Why it is collecting the data
- What other companies it may or may not share the data with
- What actions the company is taking to protect the data
- How you can access the data the company has about you and how you can fix errors
- Whether you can opt out

The information contained in the privacy policies of companies usually follows the **fair information practices principles (FIPPs)** set forth by the Federal Trade Commission (FTC) and a number of other organizations. These principles are derived from a number of studies, guidelines, and reports coming from a variety of countries. The FIP principles provide guidance for how to deal with personal information and include (1) notice/awareness, (2) choice/consent, (3) access/participation, (4) integrity/security, and (5) enforcement/redress. [Table 9.2](#) shows how the FIP principles can be mapped to what privacy policies include.

TABLE 9.2 Mapping Fair Information Practices to Privacy Policies

Fair Information Practices	Privacy Policies
Notice/awareness	What data we are collecting How the data are collected What we are doing with the data Why we are collecting the data Which other companies we may or may not share the data with
Choice/consent	How you can (or cannot) opt out of us collecting these data about you
Access/participation	How you can access the data we have about you
Integrity/security	What actions we are taking to protect the data
Enforcement/redress	How you can fix errors in our data about you

It is important to note that privacy policies, like the privacy seals we will discuss below, are considered self-regulation mechanisms for information privacy. This means that most companies are not legally required to have a policy. **Self-regulation** is often an attempt by industry leaders to avoid government regulations. In this case, businesses do not want the government to impose privacy rules they would have to follow. Instead, they suggest that privacy policies provide sufficient protection for individuals. Do you think this is true? Well, the first question you should ask is, who reads privacy policies? Research clearly shows that most individuals never read privacy policies on websites. Now that you know what policies contain, do you feel protected? What would you do if a company failed to follow its own policies? The **Federal Trade Commission (FTC)** is in charge of ensuring that privacy policies are respected. However, there is no “privacy policy police.” It is up to consumers to make complaints to the FTC in the United States. With enough complaints about a particular site, the FTC will investigate. So if you find that a company fails to follow its own policy, you must turn to the FTC with your complaint in the United States or the privacy and data protection regulators of European countries, the European Commission or the EU Commission Data Protection Working Group. Companies dealing with customers in Europe have to be aware that the privacy laws are more stringent there than in the United States. To allow international business to prosper, however, a Safe Harbor program was developed so that companies in the United States can certify their practices with the U.S. Department of Commerce if they host or use European customers’ data in the United States. More details on this program can be found at the Safe Harbor page at [Export.gov: http://www.export.gov/safeharbor/](http://www.export.gov/safeharbor/).

BUSINESS EXAMPLE BOX 9.1

Privacy and Facebook

Which students are not on Facebook? Not many, right? Everyone seems to be on Facebook. Why? It’s easy to communicate with so many people, so fast, from anywhere, and at any time. It’s a great place to share pictures and keep in touch. It’s addictive. Facebook is currently the most commonly used social networking site by adults.

Facebook likes to collect information on their users because it is the company’s business model. Using profiles, Facebook is able to offer targeted marketing for companies. Facebook clearly says that it does not provide the information directly to its clients but rather uses its access to your information to provide targeted advertising for its clients. Think about the information available: what you like; where you shop; when you date; when you break up; when someone in your family gets a job, gets fired, or gets married; and so on. So is information privacy an issue on Facebook? Some say, “Yes, but I don’t care.” Others say, “No, not at all.” And few, very few say, “Yes, and I quit.” Where do you stand?

Let us look at some of the complaints against Facebook. In 2006, Facebook released a newsfeed application that displayed changes to a friend’s page directly to your computer without you having to access his or her page. In 2007, Facebook released an application called Beacon that showed information on your page (available to all your friends) when you performed actions on partner sites, such as what movie you rented on Netflix or what you

bought on eBay. Following class actions and a settlement, Facebook discontinued this application but launched a similar program called Connect, which is intended to have better privacy settings.

In spring 2010, Facebook changed settings to allow private information from users to be displayed to all users irrespective of the initial choice of keeping this private, including job title, music preferences, school attended, and home city. The information is also shared with selected business partners of Facebook through the “instant personalization” application. After complaints, Facebook offered ways to control this setting (opt out), but many users never changed them. It is apparently not an easy task to change the settings. As a result, European Union regulators filed complaints against Facebook, alleging that users did not have effective control over their information. The Federal Trade Commission also started to investigate and later asked the company to simplify privacy controls for users (which the company did) and to provide more opt-in rather than opt-out options (which the company did not do).

In 2014, Facebook began battling a class-action lawsuit in Vienna due to its privacy practices. The primary goal of the class-action lawsuit is for Facebook to provide fundamental privacy rights such as simplifying privacy policies, providing users with more information about how their information is used, and limiting how long ad-click data are retained.

Sources: Cowan, J. 2010. “Why We’ll Never Escape Facebook.” *Canadian Business* 83(10): 28–33; Menn, J. 2010. “Technology and Society: Virtually Insecure.” *Financial Times*, July 28: 7; Gelles, D., and M. Palmer. 2010. “Facebook in Privacy Action.” *Financial Times*, July 8:16; “Getting Personal. But Too Personal? Facebook’s Mark Zuckerberg on What Information People Should Share—and Who Gets to Decide.” 2010. *Wall Street Journal*, July 7; Hamaker, C. 2010. “Facebook Fans Pay Price in Privacy.” *Rural Telecommunications* 29(4): 8; Lenhart, A., K. Purcell, S. Smith, and K. Zickhur, 2010. “Social Media & Mobile Internet Use Among Teens and Young Adults.” *P. I. a. A. L. Project*; Lyons, D. 2010. “Facebook’s False Contrition: A Business Built on Your Data.” *Newsweek* 155(23); Lyons, D. 2010. “The High Price of Facebook: You Pay for It with Your Privacy.” *Newsweek* 155(22); Best, J. 2014, “Facebook Forced to Respond to Privacy Complaints of 25,000 Europeans.” *ZDNet*, August 21. <http://www.zdnet.com/article/facebook-forced-to-respond-to-privacy-complaints-of-25000-europeans/>.

Privacy Seals

Privacy seals offer companies another attempt at self-regulation regarding privacy of consumers and a way to reassure consumers about transacting with them online. The way it works is that some company or organization, such as the Better Business Bureau, develops a seal program with a **security seal**—a logo that companies can post on their website if they follow certain rules, such as BBBOnline. There are several **seal programs** that businesses can participate in to show their commitment to trustworthiness (i.e., this website can be trusted). These seals are also called **reputation seals** and are issued by such sites as TRUSTe (<http://www.TRUSTe.com>) and WebTrust. Security seal programs assure consumers that the website follows a set of security procedures protecting their data; examples include those offered by VeriSign (<http://www.verisign.com>) and McAfee Secure (<https://www.mcafeesecure.com/>). Privacy seals ensure that the website follows certain privacy guidelines, such as ESRB Privacy Online (<http://www.esrb.org/privacy/>). Even general trust seals often deal directly with privacy. For example, TRUSTe states to consumers, “Certified companies that display our privacy seal demonstrate compliance with our Certification Standards and their commitment to privacy protection, instilling confidence and trust in users of their products and services” (<http://www.TRUSTe.com>). Seals are supposed to instill consumer confidence in the website, but studies have shown that even experienced Web users are less familiar with privacy and security seals than with security technologies (Cheskin 1999). In general, only 25% of consumers seem to recognize seal features on websites (Harris Interactive 2001), and many users will acquire goods or services independent of whether trust seals are present or not (Bélanger et al. 2002). There are many other seal programs, some specific to other areas of the world, such as TrustUK for the United Kingdom and eTICK for Australia.

LEARNING ACTIVITY 9.6

Why Your Advisor Can't Talk to Your Parents

Legislation exists to protect information privacy of individuals in a number of specific cases, such as individuals' health and financial information, as well as information about children and students. The purpose of this activity is to allow you to explore how your information privacy is protected and to better understand the difference between legitimate and inappropriate uses of information.

1. Go to the Family Educational Rights and Privacy Act (FERPA) website for students: <http://www.ed.gov/policy/gen/guid/fpco/ferpa/students.html>. FERPA protects the privacy of student education records. This link is available on the book's website.
2. Read the information on the main page. Pay particular attention to the types of information covered by FERPA and individuals to whom protected information can be released.
3. Answer the following questions and be prepared to discuss them in class:
 - a What types of information are protected under FERPA?
 - b Under what conditions may school officials provide protected information to parents? In your opinion, how do these conditions relate to the concept of "owning" your personal data?
 - c Why do you think FERPA was created? What problem did it solve?
 - d Compare the protections afforded by FERPA to the privacy policies you examined in [Learning Activity 9.5](#). What elements do they have in common? How are they different? Which has stronger protections?

Government Information Privacy Regulations

Even though information privacy is largely our responsibility as individuals, there are specific situations where governments have created regulations to protect information privacy. There are actually many such regulations throughout the world. For example, the **Data Protection Directive** regulates how personal data are processed and protected in the European Union. In the United States, there are many specific privacy laws. Some that students might be more familiar with include the **Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLBA)**, which regulates use of private information by financial institutions; the Family Educational Rights and Privacy Act (FERPA) discussed in [Learning Activity 9.6](#); the **Children's Online Privacy Protection Act of 1998 (COPPA)**, which prevents websites from collecting personally identifiable information from children without parental consent; and **HIPAA, the Health Insurance Portability and Accountability Act**, which protects your medical information (and requires you to sign a form at the doctor saying you are aware of their privacy practices). [Table 9.3](#) describes a few of these specific privacy protection regulations. Note that there are many more privacy regulations around the world that are not included in the table.

TABLE 9.3 Sample Privacy Regulations

Law	Description	Source
Children's Internet Protection Act of 2001 (CIPA)	Regulates access to offensive content over the Internet on school and library computers	http://www.fcc.gov/guides/childrens-internet-protection-act
Children's Online Privacy Protection Act of 1998 (COPPA)	Prevents websites from collecting personally identifiable information from children without parental consent	https://www.ftc.gov/enforcement/reform-proceedings/childrens-online-privacy-protection-act
Electronic Communications Privacy Act of 1986 (ECPA)	Regulates access, use, disclosure, interception, and privacy protections of electronic communications	https://epic.org/privacy/ecpa/
Family Educational Rights and Privacy Act (FERPA)	Protects the privacy of student education records	http://www2.ed.gov/policy/gen/guid/fpco/ferpa/students.html

Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLBA)	Provides regulations to protect consumers’ personal financial information held by financial institutions	https://www.ftc.gov/tips-advice/bsecurity/gramm-leach-bliley-act
Health Insurance Portability and Accountability Act (HIPAA)	Provides regulations to protect personal health information held by covered entities and gives patients an array of rights with respect to that information	http://www.hhs.gov/hipaa/index.h

BUSINESS EXAMPLE BOX 9.2

HIPAA and Identity Theft

As discussed in this chapter, **HIPAA** was enacted to protect personal health information that health organizations hold and to give patients an array of rights with respect to that information. While HIPAA was not meant to provide identity theft protection, one case actually led to HIPAA being used to prosecute a health care worker who used his access to health information to steal identities and use them for his own personal gain. Richard Gibson was employed by the Seattle Cancer Care Alliance, where he took personally identifiable information from patients, including name, Social Security number, and date of birth, to fraudulently obtain credit cards that he then used to purchase electronics for about \$9,000. Once this was discovered, he was investigated and prosecuted for failing to safeguard the privacy and integrity of patients’ health information. He was sentenced in late 2004 to 16 months in federal prison. The company he worked for was not found responsible for the employee’s actions, although in many cases, employers can be held responsible for criminal activities their employees perform.

Source: Annulis, B. D. 2005. “Identity Theft Case Creates New HIPAA Concerns for Hospitals.” *Health Care Strategic Management* 23(1): 11–12.

Privacy and Ethics

As discussed at the beginning of the chapter, information privacy and confidentiality are not new issues, but the increased use of technology has created new concerns about the use of data, and not only information privacy concerns. In the mid-1980s, Mason (1986) suggested that the increased use of information technologies, which was labeled the Information Age, would lead to four major concerns about the use of information: privacy, accuracy, property, and accessibility (PAPA). [Table 9.4](#) shows the **PAPA framework**. The framework can be used by managers to consider areas of concern about information they handle in their organizations.

TABLE 9.4 PAPA Ethical Framework: For Students

PAPA Component	Description	Questions to Ask You
Privacy	How the confidentiality of the data collected about you is maintained	• What information about you must you reveal? • What information should others be able to know without your permission? • How is your information protected?
Accuracy	Whether the data about you is what it is supposed to be and does not include errors	• Who is responsible for the accuracy of your information? • Who is accountable for errors about your information? • How do you remedy errors about your information?
Property	Who owns the data about you	• Who owns your information? • Who has the legal rights to your information?

Accessibility

Who has access to the information systems and the data that they hold about you

- How is the distribution of your information
- Who can have access to your information?
- Which companies can have access to your information?
- What safeguards are in place when someone

Source: Mason (1986).

LEARNING ACTIVITY 9.7

PAPA, Privacy Policies, and FERPA

This activity is meant to bring together various concepts you have learned throughout the chapter. First, you must review the privacy policies you created earlier in this chapter and the information on FERPA regulations you read earlier. Answer the following questions and be prepared to discuss them in class:

1. How is each element of the PAPA model addressed in the privacy policy? Are any aspects of PAPA not addressed? Which ones (if any)?
2. How is each element of the PAPA model addressed by FERPA? Are any aspects of PAPA not addressed? Which ones (if any)?
3. Explain how the conditions under which a university can disclose information to parents relate to the property element of PAPA.

Ethical Decisions

LEARNING ACTIVITY 9.8

Making Ethical Decisions

The following scenarios describe some decisions that have ethical issues. For each question, state what decision you would make and why you would make that decision. Be prepared to discuss your answers in class.

1. You need some special software for a school project. The software is available in the school's computer labs, but going to the lab is inconvenient. You can purchase the software at the bookstore, but your friend has the software and is willing to loan you the installation DVDs. Would you borrow the DVDs?
2. One of your coworkers is using his work computer for his part-time business. You become aware of this. Should you report your coworker?
3. You are the chief information officer for your company. As part of your duties, you are in charge of safeguarding data about your customers. The vice president for marketing is interested in trading information about your customers with another company. (In exchange, your company will receive information about the other company's customers.) The marketing VP thinks this trade will increase your company's revenue. Should you provide the customer information?

“A man without ethics is a wild beast unleashed on the world.” This quote from the French writer Albert Camus nicely sums up the importance of ethics. While philosophers may argue about the definition of ethics, at its core is the idea of doing the right thing—standards of behavior that tell us how we should act. Since decision making is choosing among alternatives, ethical decision making is considering standards of conduct when making choices.

Ethical decision making requires work, as doing the right thing often does. The work is worth the effort. If you always strive to make ethical choices, you will be a success. Many authors have proposed various procedures for making ethical decisions. One that we like comes from the Ethics Resource Center. It incorporates the PLUS set of questions to keep you on track (<https://www.ethics.org/eci/research/free-toolkit/decision-making-model>). The PLUS model questions whether an alternative

- [P] is consistent with organizational policies, procedures, and guidelines
- [L] is acceptable under applicable laws and regulations
- [U] conforms to universal values such as empathy, integrity, and justice
- [S] satisfies your personal definition of what is good, right, and fair

Keeping the PLUS questions in mind, follow these steps (adapted from <https://www.ethics.org/eci/research/free-toolkit/decision-making-model>):

1. Define the problem.
 - a. Why do you need to make a decision? What outcome do you want from the decision?
 - b. Does the current situation violate any PLUS criteria?
2. Identify alternatives.
 - a. Try to identify three or more alternatives.
3. Evaluate the alternatives.
 - a. What are the positive and negative consequences that flow from each alternative? Consider “positive” and “negative” from the perspective of those impacted by the decision.
 - b. How probable is it that those outcomes will occur?
 - c. Consider whether each alternative will create or resolve any violations of the PLUS criteria.
4. Make the decision.
5. Implement the decision.
 - a. Minimize negative consequences to the greatest extent possible.
 - b. Communicate the reasoning behind the decision to those affected by the decision.
6. Evaluate the decision.
 - a. Did the decision improve the situation that led to the need for the decision?
 - b. Were any new problems created by the solution?
 - c. Are any PLUS considerations resolved or introduced by the new situation?

If you keep the following in mind throughout the decision-making process, you will be much more likely to make ethical decisions:

 - Who are the stakeholders for this decision or its outcomes? Try to think broadly about this. Often, stakeholders may not be readily apparent.
 - Could someone be damaged by this decision? If so, consider whether there are alternatives that can reduce this harm. Sometimes your decisions will harm people; tough decisions often do. However, by considering the impact on others and trying to develop ways to minimize the harm, you will often be able to soften the blow.
 - What alternatives are available? How do the outcomes from those alternatives impact each stakeholder group? For each alternative, consider which option
 - Produces the greatest good and the least harm
 - Best respects stakeholders’ rights
 - Leads you to act as the type of person you want to be
 - How can you implement the decision with the greatest attention to stakeholders’ concerns? Decisions often have uncomfortable outcomes. This applies to ethical decisions as well. The way in which you carry out the decision can have a significant impact on the level of harm to any individual stakeholder.

While information systems cannot make you an ethical decision maker, they can help reduce some of the extra work that sometimes comes from ethical decision making. For example, suppose you are tasked with cutting expenses for your company. A spreadsheet can help you analyze various alternatives for doing so. Information

systems also contain the data and information you may need for developing and analyzing alternative courses of action.

Ethical decision making is worth the effort. Leadership requires followers, and if you always strive to make ethical decisions, the people you lead will trust you to have their interests in mind, even when making difficult decisions. When those you lead trust you, you can be a great leader.

Relationship between Security and Privacy

In the [previous chapter](#), we discussed information security. After reading this chapter on information privacy, you should realize that these concepts are very much related in practice. Security is the protection of information against threats such as unauthorized access to data, falsification of data, or denial of service. A company can provide every security protection possible against these threats to your information without necessarily having the intent of protecting the confidentiality of your information. Thus information privacy is different than information security, even if these concepts are often used interchangeably.

CHAPTER SUMMARY

In this chapter, we discussed information confidentiality and privacy. We first described the threats to information privacy and the consequences of privacy violations for individuals and organizations. We then discussed the technologies and solutions related to information privacy. We concluded the chapter with a discussion of the PAPA framework and of the relationship between security and privacy.

Here are the main points discussed in the chapter:

- There are four main categories of threats to information privacy: data collection, unauthorized secondary use of data, improper access to data, and errors in data.
- We identified several technologies used to infringe on and/or protect information privacy, such as cookies, cookie managers, privacy statements and policies, trust seals, and government regulations.
- Information privacy is one of the four components of the PAPA ethical framework, which includes privacy, accuracy, property, and accessibility. The framework can be used to identify concerns about the use of information.
- Information privacy and information security are related concepts, since it is mandatory for the information to be secured before it can be private. The reverse is not necessarily true, since information that is protected from a security standpoint can still be shared with others, infringing on the privacy of the information.
- Ethical decision making considers standards of behavior when making decisions.

REVIEW QUESTIONS

1. Explain briefly the four main threats to information privacy.
2. What is the difference between opt-in and opt-out options in privacy policies?
3. What are some of the possible consequences of privacy violations?
4. What are cookies, and what should individuals do about them?
5. What is the purpose of privacy policies or statements? Who regulates them?
6. What are the fair information practice principles? What is their purpose?
7. What are privacy seals, and what is their purpose?
8. Briefly describe some of the key regulations protecting information privacy in the United States.
9. What is the PAPA framework? Explain its components. What is its purpose?

10. Describe the PLUS approach to ethical decision making.
11. What is the difference (if any) between information privacy and security?

REFLECTION QUESTIONS

1. What is the most important thing you learned in this chapter? Why is it important?
2. What topics are unclear? What about them is unclear?
3. Are there any overlaps between the information privacy threats discussed in the chapter and the components of the PAPA framework?
4. How are privacy policies, cookies, and privacy seals related?
5. Imagine a well-known online retailer reveals that a hacker successfully accessed the personal information of 500 of its consumers. Is this a threat to privacy or security for the consumers? Explain.
6. Give examples of five types of data that could be stored in a cookie set up by your university when you browse the main student pages.
7. What is the difference between information privacy and information security? Can one exist without the other?
8. Why are data collection and secondary use of information threats to information privacy?
9. Can businesses be victims of identity theft? Why or why not?
10. When should organizations consider trust seals when they design a website?
11. How can information and communication technologies help make ethical decisions?

ADDITIONAL LEARNING ACTIVITIES

Learning Activity 9.A1

This activity requires you to complete a case analysis regarding information privacy. The case may be accessed through your university website, the Ivey Business School business case website (<https://www.iveycases.com>), or the Harvard Business School case website (<https://cb.hbsp.harvard.edu/cbmp/pages/home>), or it may be provided to you by your instructor.

Paine, L., and Z. Phillips. 2006. "CASE: ChoicePoint (A)." *Harvard Business School Case*, February 10. Product number: #9-306-001.

Learning Activity 9.A2

This activity allows you to explore two privacy seal programs in greater depth. First, visit five websites and note which privacy seals are common to the websites. Identify trends. Do better sites use particular seals? Then select the two most popular privacy seals and find their websites. Identify the requirements and costs for organizations to participate in each of the two seal programs and create a comparison table that includes whether a fee is charged (high/low), policies for affixing the seal, disclosures required, consumer redress options, and any other important information.

Learning Activity 9.A3

This activity requires you to listen to an interesting series of broadcasts on information privacy presented on the National Public Radio's *All Things Considered* program called "The End of Privacy." Listen to each segment and then write a short essay on one of these questions:

1. Is privacy still possible? Why?
2. Is real-time tracking a concern for privacy or a security advantage? Why or why not?
3. Is social networking worth the privacy risks? Why or why not?
4. Can online information about you come back to haunt you? How?
 - October 26, 2009—Online Data Present a Privacy Minefield (7 minutes, 49 seconds)
 - <http://www.npr.org/templates/story/story.php?storyId=114163862>
 - October 27, 2009—Is Your Facebook Profile as Private as You Think? (5 minutes, 47 seconds)
 - <http://www.npr.org/templates/story/story.php?storyId=114187478&ps=rs>
 - October 28, 2009—Digital Bread Crumbs: Following Your Cell Phone Trail (7 minutes, 50 seconds)
 - <http://www.npr.org/templates/story/story.php?storyId=114241860>
 - October 29, 2009—Digital Data Make for a Really Permanent Record (7 minutes, 46 seconds)
 - <http://www.npr.org/templates/story/story.php?storyId=114276194>

Learning Activity 9.A4

Select two websites you regularly transact with or send information to. Obtain their privacy policies and map them to the fair information practices and privacy policy contents as done in [Table 9.2](#). Do all privacy policies include the proper content? Explain.

Learning Activity 9.A5

Investigate two of the laws discussed in this chapter in greater depth (COPPA, HIPAA, FERPA, etc.). Draw a table that shows how each law addresses the fair information practices principles.

Learning Activity 9.A6

Much of the discussion in this text focused on laws and individual behaviors related to privacy that were very United States-centric. Research laws and privacy behaviors for individuals in another part of the world (e.g., Europe, Asia, Africa, and South America). Compare the privacy laws and behaviors of individuals to those discussed in this chapter. How are they the same? How are they different?

Learning Activity 9.A7

Find three examples of websites that ask you to provide personal information and discuss the reasons why you would. Then find three examples of websites that you would not want to provide with personal information and discuss why.

Learning Activity 9.A8

Compare and contrast the information privacy threats discussed in the chapter with the components of the PAPA framework. Identify any overlaps and differences.

Learning Activity 9.A9

Think of a time when you had to make a decision that was unclear from an ethical perspective. Apply the PLUS model to the decision. Prepare a two-page reflection paper that comments on the following:

- Why the decision was unclear ethically
- The effectiveness of the PLUS model

REFERENCES

- Bélanger, F., and R. E. Crossler. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems." *MIS Quarterly* 35(4): 1017–42.
- Bélanger, F., J. S. Hiller, and W. J. Smith. 2002. "Trustworthiness in E-Commerce: The Role of Privacy, Security, and Site Attributes." *Journal of Strategic Information Systems* 11(3/4): 245–70.
- Charters, D. 2008. "Addressing Privacy Breaches." *CMA Management* 81(9): 34.
- Cheskin. 1999. "eCommerce Trust Study." Cheskin Research and Studio Archetype/Sapient, January. <http://experiencecurve.com/articles/ecommerceTrustCheskin.pdf>.
- Harris Interactive. 2001. "Why Some Companies Are Trusted and Others Are Not: Personal Experience and Knowledge of Company More Important than Glitz." *PR Newswire*. <http://www.prnewswire.com/news-releases/why-some-companies-are-trusted-and-others-are-not-personal-experience-and-knowledge-of-company-more-important-than-glitz-72260317.html>.
- Madden, M. 2014. "Public Perceptions of Privacy and Security in the Post-Snowden Era." *Pew Internet Life and Society Project*, November 12. <http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/>.
- Mason, R. O. 1986. "Four Ethical Issues of the Information Age." *MIS Quarterly* 10(1): 5–12.
- McGrath, M. 2014. "Target Data Breach Spilled Info on as Many as 70 Million Customers." *Forbes*, January 10. <http://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers>.
- Riley, C., and J. Pagliery. 2015. "Target Will Pay Hack Victims \$10 Million." *CNN Money*, March 19. <http://money.cnn.com/2015/03/19/technology/security/target-data-hack-settlement>.
- Smith, H. J., S. J. Milberg, and S. J. Burke. 1996. "Information Privacy: Measuring Individuals' Concerns about Organizational Practices." *MIS Quarterly* 20(2): 167.
- Stewart, R. 2007. "Commentary: Legal Effect of Revealing Private Information in the US and Abroad." *Information Systems Management* 24(4): 343.
- Van Slyke, C., and F. Bélanger. 2003. *Electronic Business Technologies*. New York: John Wiley & Sons.

FURTHER READINGS

- Anti-Phishing Game: Used to be at Carnegie Mellon University but is being commercialized by Wombat technologies. Students can still play the demo game at the following website: Wombat Interactive Training Modules, http://wombatsecurity.com/antiphishing_phil/index.html.
- Bélanger, F., and J. S. Hiller. 2006. "A Framework for E-government: Privacy Implications." *Business Process Management Journal* 12(1): 48–60.
- Kugler, L. 2010. "The Smart Paranoid's Guide to Using Google: Here Are down-and-Dirty Details on How to Maintain Your Privacy While Using Google's Myriad Services." *Computerworld*, May 25.
- McGarry, C. 2014. "5 Privacy Fixes Your Facebook News Feed Needs by New Year's," *Macworld*, December 5. <http://www.macworld.com/article/2855596/5-privacy-fixes-your-facebook-news-feed-needs-by-new-year-s.html>.

GLOSSARY

- Accessibility:** Refers to who has access to the information systems and the data that they hold.
- Accuracy:** When data are what they are supposed to be and do not include errors.
- Children's Internet Protection Act of 2001 (CIPA):** A law that regulates access to offensive content over the Internet on school and library computers.
- Children's Online Privacy Protection Act of 1998 (COPPA):** A law that prevents websites from collecting personally identifiable information from children without parental consent.
- Clickstream data:** Tracking of online browsing behaviors.
- Cookie manager:** A software application that allows you to view which cookies are stored on your computer and what's in them and gives you the ability to delete them.
- Cookies:** Small text files located on your computer to store information about you, your accounts, and your computer.
- Data collection threat:** A privacy threat resulting from the fact that data can be collected, aggregated, and analyzed at a faster pace and in larger volumes than ever, without individuals' awareness.
- Data Protection Directive:** A law that regulates how personal data are processed and protected in the European Union.
- Electronic Communications Privacy Act of 1986 (ECPA):** A law that regulates access, use, disclosure, interception, and privacy protections of electronic communications.
- Errors in data:** A privacy threat where there are inaccuracies in data.
- Fair information practices principles (FIPPs):** Guidelines for how to deal with personal information, which include notice/awareness, choice/consent, access/participation, integrity/security, and enforcement/redress.
- Family Educational Rights and Privacy Act (FERPA):** A law that protects the privacy of student education records.
- Federal Trade Commission (FTC):** A government agency responsible for (among other things) ensuring that privacy policies are respected.
- Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLBA):** A law that provides regulations to protect consumers' personal financial information held by financial institutions.
- Health Insurance Portability and Accountability Act (HIPAA):** A law that provides regulations to protect personal health information held by covered entities and gives patients an array of rights with respect to that information.

Identity theft: Using another person's personal information for fraudulent activities.

Improper access to data: A privacy threat where unauthorized individuals have access to one's private information.

Opt-in: A privacy option where individuals state they agree that their data can be shared with others or used for other purposes, often to receive special deals or information from partner companies.

Opt-out: A privacy option where individuals must state that they do not want their data to be shared with others or used for other purposes.

PAPA framework: A framework that identifies four major categories of concerns about the use of information: privacy, accuracy, property, and accessibility.

Privacy: One's ability to control information about oneself.

Privacy policy: A statement that describes what the organization's practices are with respect to the privacy of its customers.

Privacy seal: A seal that a business can post on its website to show its commitment to privacy.

Property: Refers to who has ownership of the data.

Reputation seal: A seal that a business can post on its website to show its commitment to trustworthiness.

Seal program: A program offered by an organization that posts a set of rules that companies must follow to be a part of the seal program.

Security seal: A seal that a business can post on its website to show its commitment to security.

Self-regulation: An attempt by industry leaders to avoid government regulations by suggesting (rather than requiring) that companies have privacy policies—for example, with privacy seals and privacy policies.

Unauthorized secondary use of information: A privacy threat resulting from the use of data for purposes other than those for which they were originally collected.

CHAPTER 10

DEVELOPING INFORMATION SYSTEMS

LEARNING OBJECTIVES

By reading and completing the activities in this chapter, you will be able to

- Explain the benefits of a software development methodology
- List and describe the phases in the traditional systems development life cycle
- Compare and contrast the traditional systems development life cycle with alternative methodologies
- Explain factors that influence the decision to build custom software or purchase commercial, off-the-shelf software
- Define open source software
- Describe major outsourcing models
- List the benefits and risks of outsourcing

CHAPTER OUTLINE

- [Focusing Story: The \\$6 Billion Software Bug](#)
- [Time, Cost, and Quality](#)
- [Learning Activity 10.1: Determining Requirements](#)
- [Software Development Methodologies](#)
- [Traditional Systems Development Life Cycle](#)
- [Learning Activity 10.2: Advantages and Disadvantages of the SDLC](#)
- [Alternative Methodologies](#)
- [Learning Activity 10.3: Comparing the Methods](#)
- [Build or Buy Decision](#)
- [Learning Activity 10.4: How Open Source Software Impacts Build versus Buy](#)
- [Using Open Source Software in Business](#)
- [Learning Activity 10.5: What to Outsource](#)
- [Outsourcing Information Systems](#)
- [Chapter Summary](#)
- [Review Questions](#)
- [Reflection Questions](#)
- [Additional Learning Activities](#)
- [References](#)
- [Glossary](#)

In this chapter, you will gain a basic understanding of the software development process. In addition, the chapter will help you learn about alternatives to building software from scratch. Outsourcing information systems are also discussed.

FOCUSING STORY

The \$6 Billion Software Bug

In August 2003, the largest power blackout in North American history hit the northeastern United States and southeastern Canada. More than 50 million people lost power, some for up to two days. At least 11 people died as a result of the blackout. Total cost: \$6 billion. Investigators concluded that the initial problem started when a power line in Ohio sagged and hit an overgrown tree. Normally, this is an isolated incident. When such an incident occurs, alarm systems alert power systems operators of the problem so they can take appropriate steps to make sure that the problem remains isolated. Unfortunately, in this case, a software bug caused the alarm system to malfunction. This started a cascade of errors that led to more than 50 million people losing electrical power. The lack of power also led to water supply problems and the shutdown of major transportation systems, including railroads and airlines. Gas stations could not dispense fuel. Cell phone service was interrupted (although wired phones continued working).

While lack of proper maintenance was the root cause of the blackout, without the software bug, the impact would have been small and limited to relatively few people. With the software error, tens of millions of people were affected, and there were billions in economic costs.

There are many other examples of the serious consequences of faulty software:

- In 2013, the Patient Protection and Affordable Care Act (Obamacare) went live, and as millions of Americans accessed the newly created exchange websites, the websites crashed and became nonresponsive. As a result, millions of dollars had to be spent to get the websites working properly.
- In 2005, Toyota recalled more than 150,000 Prius hybrids to fix software that caused the gasoline engine to shut down unexpectedly.
- In 2004, a software error disrupted communication at Los Angeles International Airport's air traffic control system; 800 flights were disrupted. Fortunately, there were no midair collisions, although there were several near misses.
- From 1985 to 1987, software errors in the Therac-25 radiation therapy device allowed the device to deliver lethal doses of radiation to patients. At least five patients died.
- In 1990, an error in the control systems of AT&T's long distance switches left 60,000 people without long-distance service.

FOCUSING QUESTIONS

1. Have you ever experienced software that did not operate correctly? What consequences did you experience?
2. What can be done to limit software errors?
3. Why is it important to catch software errors early in the development process?

Time, Cost, and Quality

Every software development project faces a tension among time, cost, and quality. This reality, which applies to all sorts of projects, is known by several names, including the *project triangle*, the *engineering triangle*, and the *design triangle*. The basic idea is that there are trade-offs among the three dimensions. The three constraints are as follows:

- *Time*: How long will the project take to complete?
- *Cost*: What resources are required to complete the project?
- *Quality*: How well does the completed project meet user requirements?

Some versions of the triangle substitute *scope* (what is done as part of the project) for quality. Scope and quality are closely related, especially when considering an overall project. Quality is related to user requirements, and increasing the scope of a software development project adds new requirements that need to be met. So increasing the scope of a project also makes it harder (more costly and/or longer in duration) to meet quality goals.

There is an old saying: “You want it fast, good, and cheap? Pick any two.” Increase the speed with which a project is delivered and you will have to compromise on either quality or costs. Decreasing the cost requires a longer completion time or accepting lower quality. It is important to understand these trade-offs when making software development decisions. Typically, one of the three constraints is fixed (for example, you may have a strict budget or delivery date). As a result, the other two constraints must be managed against each other. For example, if you have a fixed budget, moving to an earlier delivery date requires changes in quality or scope. You can learn more about this in relation to project management in [Appendices J](#) and [K](#) on funding and managing projects.

LEARNING ACTIVITY 10.1

Determining Requirements

Determining system requirements is a major step in the software development process. One method for uncovering requirements is to interview the intended users of the software. Suppose that a club you belong to wants to create a system for keeping track of members. Get in pairs. One of you will act as the interviewer who is trying to discover requirements. The other will act as the user. Document at least 10 requirements for the system.

Software Development Methodologies

Developing software is a complex, time-consuming, and costly endeavor. Because of this, it is often useful to have a framework for planning, structuring, and controlling software development projects. Such frameworks are commonly called **software development methodologies**. These methodologies provide discipline to the software development process by defining processes, roles, and deliverables related to software development. Typically, the methodologies break down software development into phases, each of which has its own set of processes, roles, and deliverables. In some methodologies, the deliverables of one phase provide the inputs for the next phase.

Most large organizations have a standard software development methodology that is used across the organization, although many organizations may allow different methodologies for particular projects. For example, a Web-based system development project may follow a different methodology than a transaction processing system (TPS) development project.

The main reason to use a formal software development methodology is that it provides discipline by clearly defining how the project should proceed, what work should be done, how that work should be done, and what outputs should be produced. Having a standard methodology in an organization also allows individuals to more easily join a project in progress. The standardized roles, processes, documentation, and deliverables make it easier for a new team member to become familiar with what has been done on the project. It also makes it easier for the new member to find relevant information.

Traditional Systems Development Life Cycle

Traditionally, many systems development projects have followed a semisequential, phased approach, which is typically called the **systems development life cycle** (SDLC). The SDLC provides a disciplined approach to systems development. Projects follow a well-defined set of phases that have related objectives, processes, and

deliverables. The traditional SDLC is sometimes called the *waterfall method*, since the results of one phase flow as inputs into the next phase. It is important to realize that there are many different versions of the “traditional” SDLC. The differences boil down to how the phases are divided; some versions have more phases than others. The versions with fewer phases collapse multiple phases from the more complex versions into a single phase. In this chapter, we present a relatively typical version with five phases, as shown in [Figure 10.1](#). Note the dashed feedback lines on the left-hand side of the diagram. Sometimes you need to go back and refine an earlier phase based on new information that emerges.

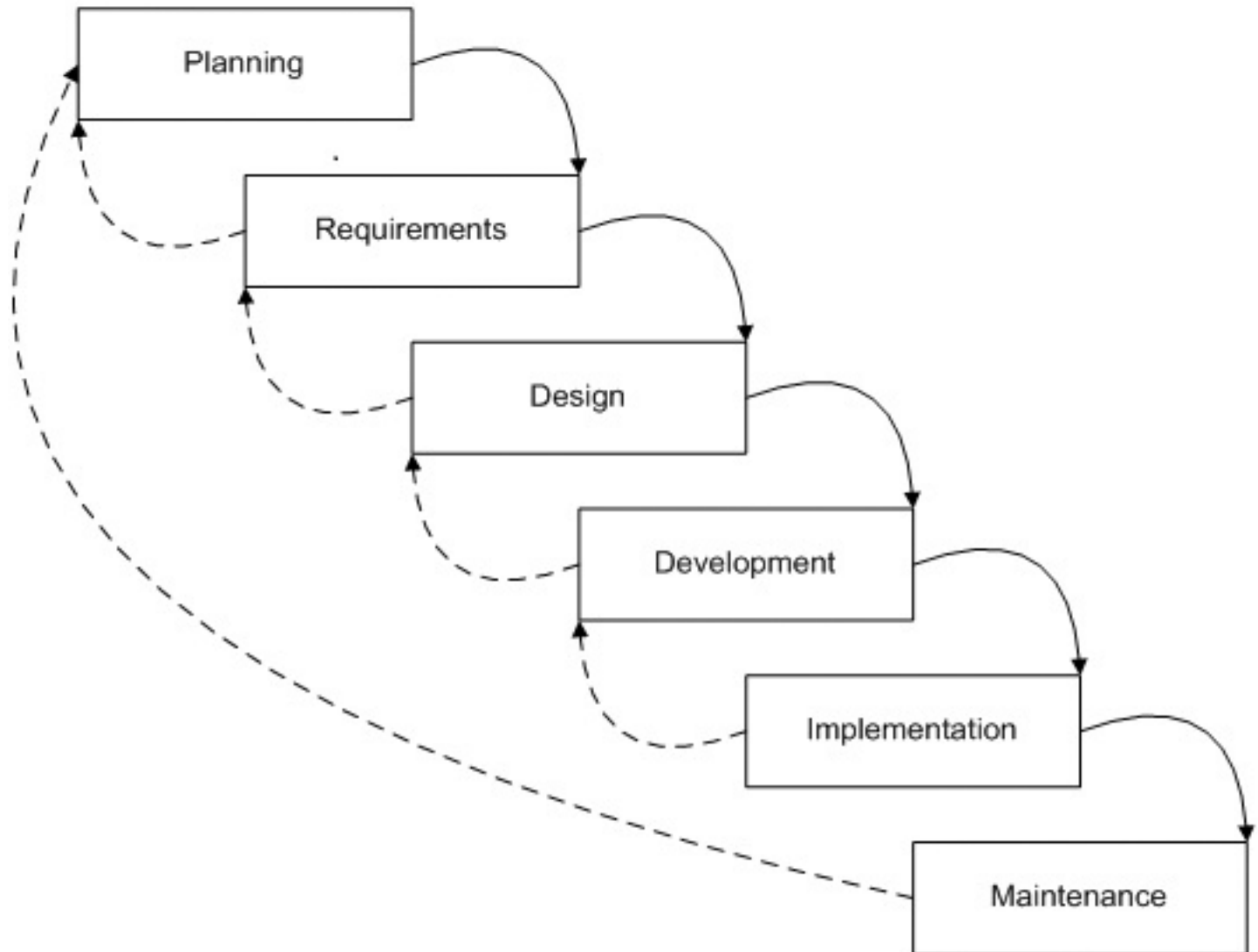


FIGURE 10.1 Traditional Systems Development Life Cycle

Planning Phase

The goal of the planning stage is to define the overall goal and scope of the system and determine the feasibility of the project. Essentially, you want to answer the question “Why build the system?” In addition, you need to establish whether the project is feasible. There are several different aspects to feasibility:

- *Technical feasibility* concerns whether the proposed system can be completed from a technical standpoint. It is important to consider whether the system fits with the existing technical infrastructure.
- *Economic feasibility* relates to whether the proposed system is affordable and worth the investment.
- *Organizational feasibility* concerns whether the project fits with the organization’s existing strategies and practices. If the system does not fit with current ways of operating, the organization needs to determine what needs to be

changed and whether these changes are feasible. Organizational feasibility should also consider whether the organization has access to the human resources necessary to complete the project.

- *Legal feasibility* concerns whether the proposed project violates any laws or regulations.
- *Ethical feasibility* considers whether the system fits within the ethical guidelines and practices of the organization and its industry.

The major deliverables of the planning phase are the feasibility analysis, project initiation document, and the project management plan. The project initiation document specifies the high-level goals of the system and describes the business case for the system. (A business case describes the system and why it is needed.) The feasibility analysis results are often included in the business case. The project management plan documents the scope of the project, identifies major tasks and resources, and describes any interrelationships with other projects.

Requirements Phase

The goal of the requirements phase is to uncover and document the functions that the system should provide and desired levels of performance. In other words, in the requirements phase, the task is to figure out and document what the system should do. There are two types of requirements: functional and nonfunctional. **Functional requirements** describe how the system should interact with users and other systems. An example of a functional requirement is “The system shall allow customers to look up the price of a product.” **Nonfunctional requirements** are related to constraints on the system—for example, how well it should perform. An example of a nonfunctional requirement is “The system shall be available at least 23 hours per day.”

Requirements elicitation involves gathering requirements from various stakeholders and is a primary task in the requirements phase. Gathering the requirements for a system is often a difficult, time-consuming, and error-prone process. To make things worse, requirements may change during the process. Despite the difficulties, it is very important to fully understand the system’s requirements; they form the foundation for the rest of the development project.

The output of the requirements phase is a specification of the system’s functional and nonfunctional requirements. Typically, this takes the form of a set of requirements statements (sometimes called *system shall* statements) or a set of use cases, in either text or diagram form. A *system shall* statement simply defines a requirement, such as “The system shall allow teachers to enter student grades.” A **use case** describes a sequence of actions that results in an outcome for some actor. An actor can be a user or another external system. [Figure 10.2](#) shows a use case diagram. (Use case diagrams are part of the Unified Modeling Language, which was developed as a standard way to specify models related to software systems.)

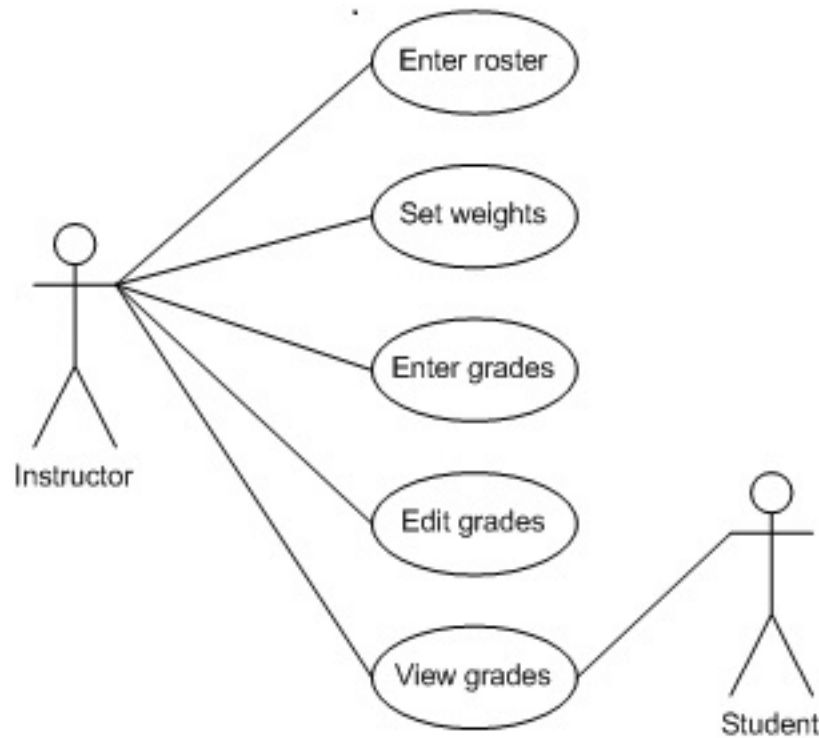


FIGURE 10.2 Use Case Diagram Example

It is important to understand that requirements should specify *what* the system must do but not *how* the system should meet the requirements. This allows the system designers flexibility in the design of the system, which is covered in the next phase.

Design Phase

The main goal of the design phase is to describe in detail how the system will meet the requirements specified earlier. The requirements form the foundation of the system design. The focus here is on *how* the system will satisfy the requirements, although there are elements of the design phase that still deal with what the system is intended to do. These elements are known as the *logical system design*, which includes abstract models of what the system is intended to do. An example of such a model is the database diagram we saw in [Chapter 5 \(Figure 5.4\)](#). In addition to the database model, the user interface and business rules enforced by the system need to be designed. The design phase also specifies the plans for implementing and testing the system. The system design document is a major deliverable of the design phase. This document describes, in detail, the system requirements, operating environment, database design, user interface, and processing logic. Other deliverables include an implementation plan and a training plan.

Development Phase

During the development phase, the outputs of the design phase are converted into the actual information system. This is the phase in which the system is actually constructed. The software is written, databases are created, and any necessary hardware is installed. It is often necessary to integrate the new system with existing information systems; if needed, the integration occurs during the development phase. System testing is a critical part of the development phase. Testing occurs both during the development of the software and when the entire system is complete and integrated. Software testing is a complex, time-consuming, but critical aspect of systems development. It is necessary to thoroughly test the system prior to actual implementation. Errors are very expensive to correct when they are not discovered until after the system is implemented. The errors may also lead

to business disruptions. The development phase's deliverables include the application software, data and files for testing, and documentation on how the software components interact with one another and external systems.

Implementation Phase

The goal of the implementation phase is to make the system operational in a production environment. One important implementation phase activity is to notify users of the rollout of the new system. This notification should include the implementation schedule, differences in work processes and responsibilities brought about by the new system, and the process for obtaining technical support for the new system. User training is also an important activity in this phase. Often, it is also necessary to convert data from the existing system into the new system. For example, a new product cataloging system might need to have data from the old system migrated into the new system. Finally, it is a good practice to have a postimplementation review that documents the project to date and makes recommendations for improvements for future projects. The main deliverable of the implementation phase is the system itself, installed and running correctly. The postimplementation review report is another deliverable from this phase.

There are four common approaches to system migration:

- *Direct changeover (also called immediate changeover)*: At a specific point in time, the old system is no longer used and is replaced by the new system. While this has the advantage of being rapid, it is very risky. If the new system has problems, the functions available in the old system are also unavailable.
- *Parallel operation*: Both the old and new systems operate for some period of time. The parallel approach is less risky than direct changeover but also takes longer and is more expensive. The parallel approach is necessary for systems that cannot be taken out of service while changing from the old to the new system.
- *Phased implementation*: The new system is implemented in stages. This approach is an attractive compromise between direct and parallel approaches. However, it is best suited for systems that have clear modules that can be implemented in a phased manner. Systems with significant interdependencies between modules are not suitable for phased implementation.
- *Pilot operation*: The new system is implemented in a business unit (such as a store or department) or location (such as a state or country). The initial pilot is followed by other pilot changeovers or a full changeover to the new system. Each pilot changeover must use one of the other approaches.

Maintenance Phase

The final phase in the SDLC is the maintenance phase. This is usually the longest, most costly phase of the life cycle. It is not unusual for more than half of the total system cost to occur in the maintenance phase. The goal of this phase is ensuring that the system operates properly to meet current needs. This involves fixing any problems that are uncovered and may also involve modifying or adding to the programs to meet new needs. In addition, the system may be modified to improve performance or take advantage of new technologies. For example, an online ordering system may be modified to allow customers to order from their smartphones.

Although we presented the SDLC as a very linear process, where one phase follows the next in an orderly fashion, reality is rarely so neat. During the systems development process, it is often necessary to revisit an earlier phase when new needs arise or problems are discovered.

[LEARNING ACTIVITY 10.2](#)

Advantages and Disadvantages of the SDLC

The traditional SDLC has been around for a long time (which is why it is called “traditional”) and has been used successfully for many systems development projects. However, it is not without its drawbacks. With a partner,

research the SDLC approach and develop a list of three advantages and three disadvantages to the traditional SDLC. Be prepared to share your list.

As you discovered in [Learning Activity 10.2](#), there are advantages and disadvantages to the traditional SDLC. These drawbacks led to the development of alternative methodologies. In the next section, we describe several of these alternative approaches.

STATS BOX 10.1: STANDISH CHAOS REPORT

Cancelled information technology (IT) projects and incorrect software cost the global economy billions of dollars each year. The Standish Group's CHAOS Report provides data on the failure rates of IT-related projects. Project outcomes are divided into three categories. Successful projects are delivered on time and on budget and meet requirements. Challenged projects are late, are over budget, and/or do not meet some requirements. Failed projects are cancelled before they are completed or are delivered but not used. For 2013, 16.2% of the IT projects studied were successful, while 52.7% were challenged, and 31.1% failed. This is a slight improvement over the first CHAOS Report, which found that only 16% of IT projects were successful, while 53% failed. There are many causes for software failure. In some cases, the initial estimates of the costs, resources, and delivery date are unrealistic. Other causes include misunderstanding requirements, "feature creep" (expanding requirements), and inadequate testing. The costs of these failures are staggering. One estimate puts the global price tag of IT failure at more than \$3 trillion (<http://www.zdnet.com/article/worldwide-cost-of-it-failure-revisited-3-trillion/>).

Alternative Methodologies

Prototyping

Prototyping is an approach to deal with aspects of a full methodology; it is not a complete, stand-alone methodology. In a prototyping approach to systems development, you begin with an initial investigation of the main requirements of the system. It is not necessary to have a full understanding of all requirements. After the initial investigation, a small-scale mock-up of the system (called the **prototype**) is built and reviewed by stakeholders. The stakeholders point out flaws, which reveals new or misunderstood requirements. The prototype is refined and reviewed. This cycle repeats until the stakeholders are satisfied that all requirements are met. Then the full system is implemented. Some prototypes are "throwaway" prototypes, which means that they are not intended to be part of the final system; their purpose is to uncover requirements and problems. Sometimes, however, prototypes become part of the final system. This is known as *evolutionary prototyping*.

Increased stakeholder involvement is a major benefit of the prototyping approach. The stakeholders know the particular business area addressed by a system much better than the systems developers, and having them involved throughout the development process can lead to systems that better meet their needs. In addition, stakeholder involvement may increase satisfaction with the final system. Prototyping is also potentially more effective for uncovering system requirements. This is especially important when requirements are unclear, ambiguous, or difficult to define. In some cases, a prototyping approach may be less expensive than a traditional SDLC approach.

There are also drawbacks to the prototyping approach. Prototyping can lead to poorly designed systems that do not perform well when scaled up for actual use. It is also difficult to estimate how many iterations are required, which makes it difficult to estimate costs and schedules. Usually, prototyping results in less-well-documented systems, which may cause problems later (for example, when the system needs to be revised or integrated with new systems). Finally, nonfunctional requirements (such as performance requirements) are difficult to establish using prototypes.

Prototyping is best for systems that require extensive user interaction and for which the analysts have some understanding of the business issues to be addressed, especially when functional requirements are not well understood. Prototyping is less well suited for systems that have well-defined requirements, when nonfunctional requirements are especially important, or when future scalability is important.

Rapid Application Development (RAD)

As the name implies, rapid application development (RAD) is intended to develop systems more quickly than traditional methods. It is an iterative method that uses rapid development of prototypes rather than engaging in extensive up-front planning. RAD typically breaks software development projects into smaller chunks in order to reduce overall project risk. This also facilitates making changes as the project's requirements emerge. The focus is usually on filling organizational needs rather than creating technically perfect systems.

Active user involvement is a key aspect of RAD. The idea is to work with users to determine high-level requirements and then build a prototype based on those requirements. Developers review the prototype with the users, who provide feedback. The prototype is refined based on the feedback. This process continues until the full system is developed. Interestingly, some of the same methods used in the traditional SDLC approach can also be applied in RAD. The RAD process is illustrated in [Figure 10.3](#).

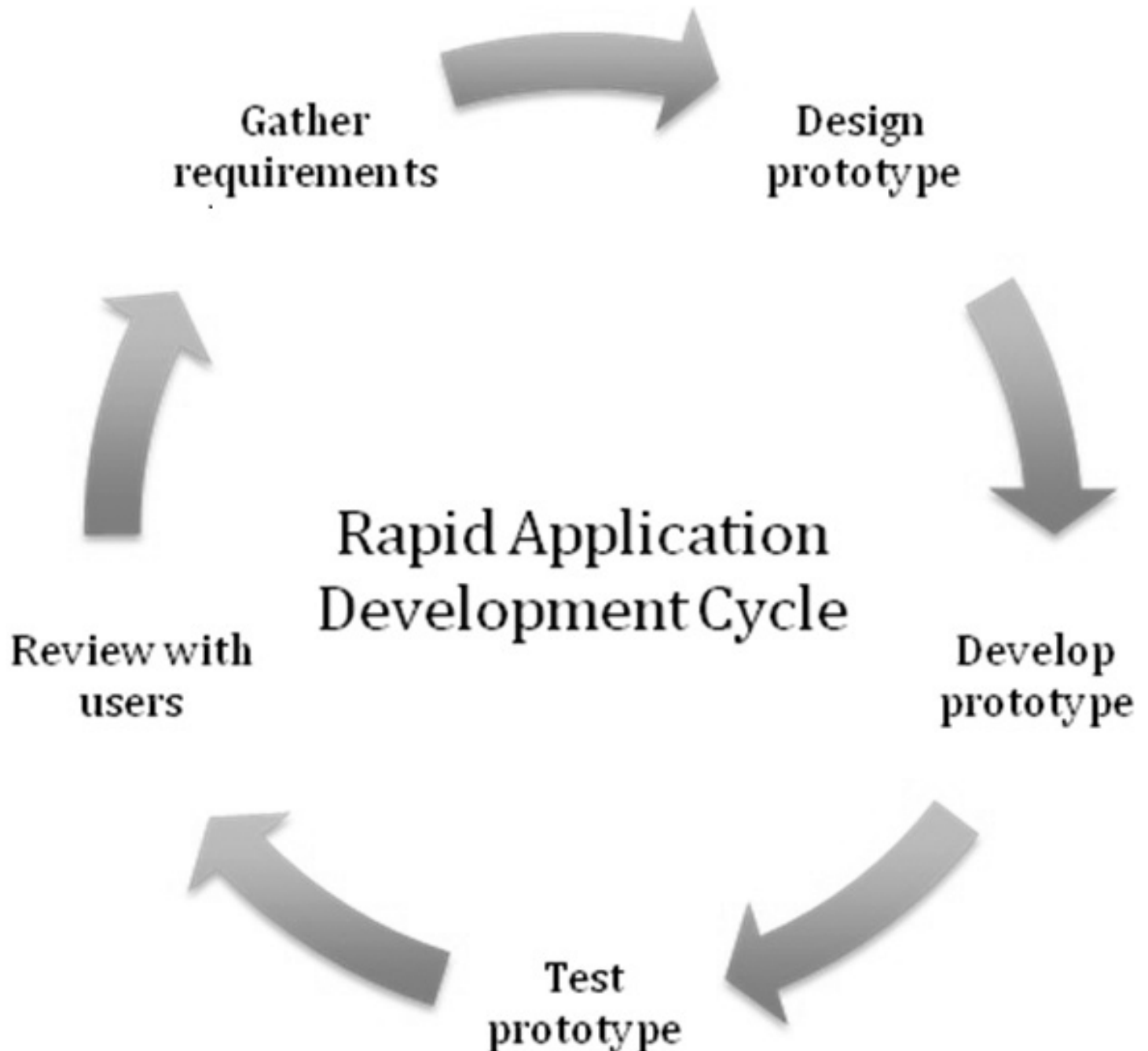


FIGURE 10.3 Rapid Application Development (RAD) Cycle

Development tools are integral parts of a RAD system. Computer-aided software engineering (CASE) tools, for example, automate many software design and development tasks. Tools for quickly developing graphical user interfaces are often included in a RAD environment. These tools allow developers to build user interfaces by dragging and dropping interface elements onto a screen instead of having to write the software code.

In addition to delivering systems more quickly than the traditional SDLC, RAD often results in lower costs as well. Because user involvement is such an important aspect of RAD, systems developed using RAD often have greater buy-in from users. RAD also facilitates evolving requirements well. However, the speed of RAD may result in lower-quality software. Because users often want more and more features, “feature creep” may be more likely with RAD. Since there is less focus on nonfunctional requirements, systems may not perform well when scaled to more users or greater volumes of processing.

RAD is best suited for smaller-scale projects with well-focused organizational objectives and committed users. RAD does not work as well for very large projects or systems where performance and quality are critical. For example, you might not want to use RAD for a safety-critical system such as an air traffic control system.

Spiral Model

The spiral model, which is shown in [Figure 10.4](#), is basically an iterative version of the standard “waterfall” SDLC. It is a risk-driven model, which focuses on reducing project risk by identifying risks and ways to reduce those risks throughout the development process (Boehm 1988). Think of the development process as trips around the spiral. For each trip, you would perform the same steps:

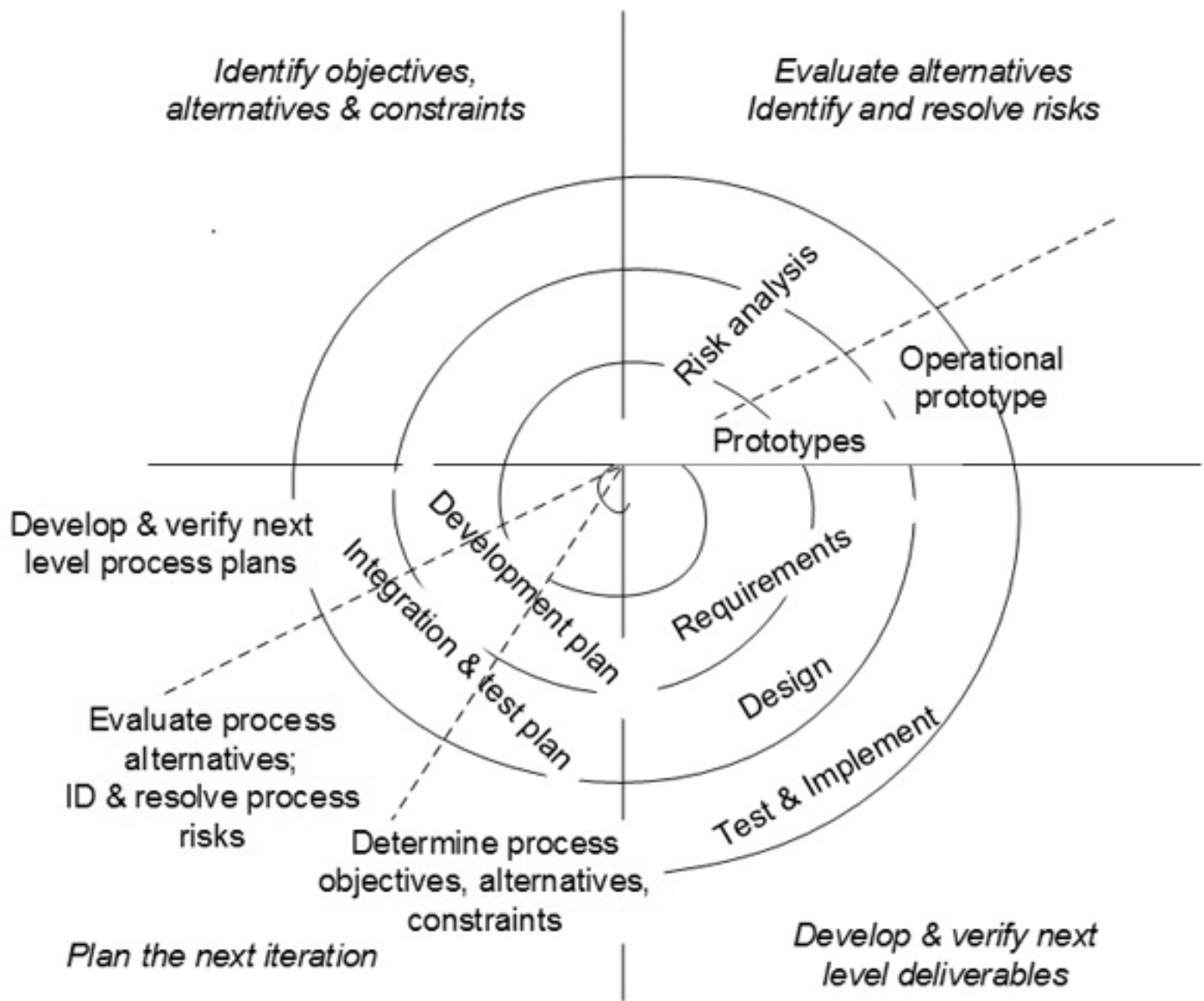


FIGURE 10.4 Spiral Model

Adapted from <http://www.maxwideman.com/papers/linearity/spiral.htm>

- *Identify objectives, alternative approaches, and constraints:* Objectives correspond to the requirements we discussed earlier. They may include both functional and nonfunctional requirements. In addition, alternative means of achieving the objectives are identified. These might include different designs, purchasing the system, and so on. Constraints would include time, resources, costs, and the systems with which the new system must interact.
- *Evaluate the alternatives and identify and resolve risks:* Identifying potential risks is important. These risks are associated with project uncertainties. Developing effective methods for reducing these uncertainties is critical. For example, prototyping may help reduce risks related to misunderstanding functional requirements.
- *Develop and verify the deliverables from this iteration:* The prototype (or other deliverable) from the current iteration is developed and evaluated. Evaluation includes making sure that the prototype meets the current requirements. In early iterations, this may simply be a proof of concept. In later iterations, verification may include detailed testing.
- *Plan the next iteration:* Determine what should be accomplished in the next iteration. Also determine the resources needed.

The spiral model's focus on risk and risk reduction is a major advantage over other methods when developing critical systems. The approach also involves users throughout the process, which can build user commitment to the project. The spiral model allows developers to incorporate other approaches, such as the traditional SDLC

and prototyping, when appropriate for individual iterations. Like RAD, the spiral model considers evolving requirements. Effectively using the spiral model requires highly skilled project managers. In addition, it is often difficult to know when to stop. Although originally intended to run for four cycles, there is a temptation to keep going to add more features.

The spiral model is most appropriate for critical systems, where there is a high priority on minimizing risk. It is less appropriate for projects where risk avoidance is not critical and when costs are especially important.

This is just a sampling of some of the more common systems development methodologies. There are many others. Several of these fall into the category of agile development methodologies. *Agile development* occurs in self-managed, cross-functional teams whose members include information systems professionals and user representatives. Rather than being process oriented, agile methods are people oriented. Agile methods emphasize multiple iterations and continuous feedback from user representatives. Many specific methodologies fall into the family of agile methods. These include extreme programming (XP), which uses frequent releases with short development cycles, and Scrum, which features work “sprints” of one to several weeks, at the end of which the development team meets with stakeholders to assess progress and plan what needs to be done next. As software and its uses continue to evolve, we expect that software development methodologies will do the same.

LEARNING ACTIVITY 10.3

Comparing the Methods

Pick one of the alternative software development methodologies described in the chapter. Compare it with the traditional SDLC. Find at least three ways in which they are similar and three ways in which they are different. Be prepared to share your answers.

BUSINESS EXAMPLE BOX 10.1

App Developers Needed!

You may be aware of companies that only make apps and are very successful at doing so. As the vast majority of consumers own smartphones, the majority of their time is spent using apps specifically designed for their phones, as opposed to visiting sites through the mobile Web browser. This results in an increased demand by organizations for people to design apps for them. Unfortunately, there are not enough app developers available to meet this growing need. In fact, in a survey of 228 application development managers for enterprises, 85% reported that they had a backlog of between 1 and 20 mobile applications. Half of the managers reported that their backlog was between 10 and 20 applications. Furthermore, it can take up to a year to get an app into production. This has resulted in companies not being able to generate as much revenue as they otherwise would if they could create more apps for the marketplace and do so in a timely manner.

Sources: <http://techcrunch.com/2014/04/01/mobile-app-usage-increases-in-2014-as-mobile-web-surfing-declines/>; <http://www.zdnet.com/article/enterprises-we-need-more-mobile-app-developers/>; <https://www.outsystems.com/blog/2014/10/new-mobile-trend-statistics.html>.

As you can see, there are many different methods for developing systems; choosing the correct methodology depends on many factors. However, developing a system from scratch is not the only option available when an organization needs a new system. It may be preferable to buy rather than build the system. This choice is the topic of the next section.

Build or Buy Decision

When the need arises for a new software-based system, managers face a long-standing decision: whether to create the software or purchase existing commercial, off-the-shelf (COTS) software. This decision is complex and costly if you get it wrong. On the surface, it may seem like it is always preferable to purchase an existing system rather than going through the time, cost, and effort of creating a new system. However, the decision is not that easy. Often, the COTS software will need significant customization in order to meet business needs. In these cases, it

may be more effective to build a new system. In between the extremes of custom and COTS software lie hybrid approaches. These hybrid approaches involve modifying COTS software to better fit organizational needs or combining COTS components to create the desired solution.

Custom-built software is software that is built from scratch using a few commercially obtained components. The main benefit of the custom approach is that the resulting system will likely be a better fit with business requirements. As a result, the custom system may be used to create a competitive advantage. In addition, the organization will have greater control over adding or modifying functions after the initial system is implemented. However, custom solutions usually take much longer and are more costly to develop than COTS or hybrid solutions. In addition, custom solutions are more prone to errors, which can further increase costs and time to delivery.

COTS software is a complete (or nearly complete) solution obtained from a third party. Examples range from office productivity systems to ERP systems. Often, COTS software is less expensive than custom or hybrid approaches. COTS software may also be higher quality, especially if it is a widely used system. Usually (although not always), COTS-based solutions can be provided in a much shorter time frame than custom or hybrid solutions. There are downsides to COTS software, however. First, COTS software often requires changing existing business practices to fit the COTS software. Second, companies are largely at the mercy of the vendor or consultants for support, including enhancements and fixes. In addition, a financially weak vendor may be unable to provide proper support or maintenance. In extreme cases, the vendor may go out of business.

Hybrid solutions may use components from different vendors to create the complete solution or may involve customizing COTS software by modifying programming code or adding small programs called *scripts*. In ideal cases, the hybrid solutions offer the best of custom and COTS approaches. The hybrid solutions usually better fit business requirements and existing processes but can be delivered less expensively and more quickly than custom solutions. However, hybrid solutions also suffer from some of the same drawbacks as custom-built systems and COTS solutions. In addition, it may be difficult to find the expertise necessary to modify or combine the COTS components. [Figure 10.5](#) provides an overview of some of the characteristics of the three approaches.

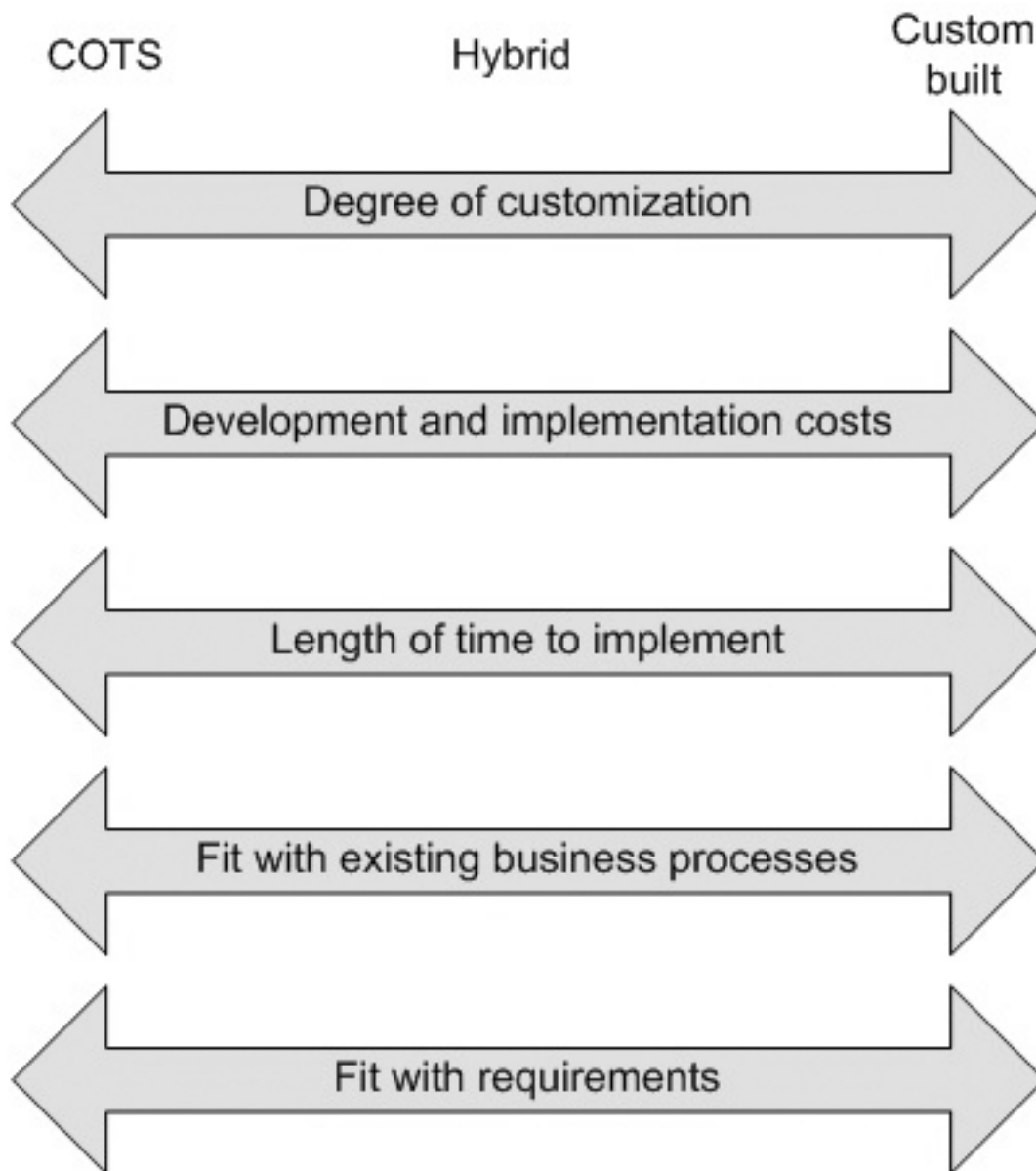


FIGURE 10.5 Comparing COTS and Custom Development

Source: Adapted from <http://www.baselinemag.com/c/a/Application-Development/Buy-vs-Build-Software-Applications-The-Eternal-Dilemma>.

When making the build versus buy decision, a number of questions must be addressed:

- *Is there COTS software that will meet the business's needs?* If the answer to this question is no, your choices are narrowed to custom development or a hybrid approach. If no COTS software can meet your organization's needs, you have to create the software or customize COTS software. In these cases, you may have the option of outsourcing the development or customization. (We discuss outsourcing later in this chapter.)
- *Will the software give your company a competitive advantage?* If COTS software is an option, the next question is to consider whether the system will give your company a competitive advantage. If so, the scale is tipped toward building custom software. If not, COTS software may be a better choice. To understand why, think about the example of a hotel chain. To such a company, a payroll system would not be likely to provide any competitive advantage. Payroll is a routine function, so it is a good candidate for COTS software. In contrast, having a custom system for analyzing the behaviors and preferences of frequent guests may give the company an advantage over its competitors and is therefore a better candidate for a custom-built system.
- *Does the COTS software fit with business processes?* COTS software will rarely match exactly with existing business processes. As a result, you will usually have to modify at least some business processes in order to use COTS software. Often, this is not a problem, but sometimes the changes necessary are so extensive that it may

be better to build a custom system. The key issue is whether it is practical to alter existing processes in order to fit the way the COTS software operates.

- *Does the COTS software fit with existing IT architecture and staff?* To be successful, COTS software must fit with your organization's existing IT. Here is a simplistic example. Suppose that your organization used only Windows-based PCs. Macintosh-only COTS software would not be a good fit with your existing IT. It is also important that your IT staff be able to support any COTS software you use. If the existing staff cannot provide support, you will need to either contract with an outside company for support, train your existing staff, or hire new staff. All of these add to the cost and complexity of implementing the COTS software.
- *Do you have the capability to create the required system?* There are times when an organization simply does not have the capability to create a system that meets requirements. In these cases, COTS software is often an attractive option. Outsourcing the development of the system is another option.
- *When is the system needed?* A COTS solution can almost always be implemented faster than a custom-built system. As a result, you should consider the "go-live" goal for the new system when making the build versus buy decision.
- *What is the total cost of ownership for each approach?* Finally, you should compare the total cost of ownership (TCO) for both approaches. The cost of purchasing or building the system is not the only cost you should consider. There are also support and maintenance costs, costs to integrate the system into the existing architecture, and costs related to enhancing the system in the future. One important point to keep in mind is that COTS systems usually are changed much more often than custom-built systems. When the vendor releases a new version of the software, you may incur additional costs related to deploying the new version. Of course, you could stay with the old version, but vendors often drop support for older versions, which may lead to problems.

[LEARNING ACTIVITY 10.4](#)

How Open Source Software Impacts Build versus Buy

Open source software is software that provides access to the program's code, which means that it can be freely modified. Often organizations must decide whether to build custom software or purchase a commercial software package. In pairs, discuss how open source software might impact the build versus buy decision. Prepare a bullet list of your findings.

[Using Open Source in Business](#)

Open source software is software that allows users to access the underlying source code for an application. Having the **source code** for a program allows users to modify the program's functions. The **source code** is the human-readable form of a software program. Typically, this source code is translated into computer instructions through a process called *compiling*. The compiled code is not in a form that is easily understood by a human. The licensing for open source software also allows users to modify the program, subject to some conditions. The Open Source Initiative provides a detailed definition for "open source" at <http://www.opensource.org/docs/osd>.

Open source software is usually available free of charge, although it is common for companies to distribute (for a fee) open source software along with support contracts or other enhancements. Open source software has been in existence for many years but has been largely unknown to the general population until recently. The rise of popular open source applications such as Mozilla Firefox (a Web browser), OpenOffice (a productivity suite), and operating and systems software such as the Linux operating system and Apache Web server have increased the awareness of open source software.

More recently, Google's open source Android operating system has been credited with a rapid rise in the number of smartphones running Android. According to the Nielsen Company, in the second quarter of 2009, Android-based phones accounted for only 1% of the new smartphone purchases in the United States. By November 2010, they accounted for more than 40%. By the end of 2014, more than 75% of the smartphones in use were running the Android operating system (IDC 2014). Some believe that Android's openness is one reason for its rapid rise. The fact that Android was open allowed many smartphone manufacturers to implement Android

on their handsets. The manufacturers were also able to modify Android to take advantage of their phone's specific features.

Businesses are adopting open source software for a variety of uses. For many years, the Apache Web server has held more than 50% of the U.S. Web server market. Most large organizations use Linux servers to some extent. According to the Linux Foundation, more than three-quarters of large organizations plan to add more Linux servers in the near future (Linux Foundation 2014). Open source is less popular for personal computer operating systems, with slightly more than 1% of personal computers using Linux. Open source for end users may be on the rise, however. The recent economic downturn has led some organizations to take another look at open source applications. In addition, many governments are actively promoting the use of open source alternatives to proprietary software among both governmental departments and citizens. Time will tell whether this trend continues.

Why would businesses use open source software? There is a variety of reasons. The most obvious is the potential cost savings. Most open source software can be acquired without charge. It is important to note that this does not mean that the software can be implemented without cost. There are ongoing costs associated with installation, support, and continuous training; these costs should not be ignored. Another reason businesses use open source software is to avoid being dependent on proprietary software vendors for ongoing development and support. For example, users of Microsoft Office are completely reliant on Microsoft for current developments (such as fixing errors or enhancing the software). With open source software, the larger community can carry out these functions. This means that continuous development and support are possible even if the creator of the software goes out of business. There is also some evidence that mature open source software is often more reliable than proprietary software. In addition, open source software is more likely to use open standards for things such as file formats. This reduces the reliance on any particular software vendor. Additional flexibility comes from the fact that users have the ability to modify the software as needed. This is not possible with proprietary software. (It should be noted that most users lack the technical skills necessary to modify software, which reduces the value of this benefit.)

One interesting aspect of open source software is that a community of volunteer programmers often does ongoing development. The structure of an open source development community is like an onion. Core developers are at the center, and passive users are at the outermost layer. The core developers do most of the programming for both the original creation and ongoing development. Core developers at outer layers report errors and request features and may also contribute fixes for the errors. Active users also report problems but do not contribute any programming code, and they often help less experienced users in community forums. Thus the community not only supports current users but also provides a platform for ongoing enhancements.

[LEARNING ACTIVITY 10.5](#)

What to Outsource

Outsourcing occurs when a company turns to an outside vendor to provide some service. While the definition of outsourcing is easy to understand, deciding what to outsource is much harder. For each of the following business scenarios, decide whether the system or operation should be outsourced. Explain your answer.

Organization	System/Function
1. Engineering company	Payroll and benefits management system
2. Regional beer brewery	Customer relationship management
3. University	Learning management system (e.g., Blackboard, Moodle)
4. Financial portfolio management company	Investment analysis software
5. Public radio station	Donor management system

Outsourcing Information Systems

Information technology **outsourcing** occurs when an organization goes to an outside company to provide IT services that were previously provided internally. (Outsourcing is not unique to IT. For example, some companies outsource the manufacturing of products that they sell.)

Outsourcing Models

There are many different outsourcing models. These differ in the degree of outsourcing and in what is outsourced. Some organizations contract with a service provider to provide all IT-related services. This is known as **full or complete outsourcing**. Full outsourcing allows an organization to focus on its core activities and may also reduce IT costs. Service providers may be able to provide services less expensively due to economies of scale.

In contrast, in **selective or partial outsourcing**, only certain aspects of IT are outsourced to a service provider. For example, AT&T recently outsourced the maintenance of its ERP system to Accenture. There are different approaches to deciding what to outsource. Under **process-based outsourcing**, an organization outsources a particular function or business process. Functions that are often outsourced include help desk support, payroll and benefits processing, and telecommunication services. Outsourcing specific functions is not new. For example, ADP has been providing payroll services to organizations for more than 50 years.

Personnel outsourcing is another form of outsourcing that has a long history. This form of outsourcing allows organizations to meet staffing needs without the long-term costs associated with hiring permanent workers. Bringing in temporary, contract-based workers may be effective when an organization needs specific expertise on a short-term basis or when the current workload is more than the internal IT staff can handle. In these cases, outsourcing can speed time to deployment for a system and avoid costs related to training the current staff.

Another approach is **project-based outsourcing**. As the name implies, this involves contracting with a vendor for a specific project. Since projects have specific start and end points, when the project is finished, the outsourcing engagement ends. Organizations outsource projects when they lack the internal resources necessary to complete the project. Earlier we mentioned outsourcing as an alternative for developing a custom system. This is an example of project-based outsourcing. When the system is developed and deployed, the outsourcing engagement ends. Interestingly, upgrades to the system may lead to future outsourcing engagements.

Application outsourcing involves a service provider handling activities related to a specific software application for a fee. There are different forms of application outsourcing. With application hosting, the client organization is responsible for operating the IT infrastructure associated with the application, but the client must purchase the software and pay any annual license or maintenance payments to the software publisher. Amazon's Web Services is an example of application hosting. Organizations can deploy applications on Amazon's systems. Amazon handles keeping the servers up and running but is not responsible for maintaining the application. This arrangement is often very cost effective, especially when there are demand spikes that may require additional server capacity. Software as a service (SaaS) provides on-demand Web-based access to an application on a per-use or per-user basis. [Salesforce.com](https://www.salesforce.com) is a well-known provider of SaaS. [Salesforce.com](https://www.salesforce.com) provides organizations with customer relationship management software for a monthly per-user fee. Different features lead to different fees. For example, a simple contact management currently costs \$5 per user per month, while a full CRM system costs \$125 per user per month. The SaaS model provides a large degree of flexibility and can be cost effective. The client organization does not have to worry about maintaining the software or the servers. SaaS also provides very good scalability. However, there are security and privacy concerns with SaaS.

Benefits and Risks of Outsourcing

Outsourcing, when done well, can result in a variety of benefits. A major benefit of outsourcing is that it can give organizations access to specific expertise not available in-house. There can also be cost savings with outsourcing.

These are normally associated with the vendor having lower cost structures, through either economies of scale or lower wage rates. Outsourcing also shifts employee-related fixed costs to variable costs. In addition, outsourcing may allow for more rapid delivery of projects through additional expertise and personnel and can be an effective means of managing capacity. It is generally easier to contract for additional capacity than to add it through other means. Selective outsourcing allows management to focus on core business activities. Finally, when outsourcing sites are spread across time zones, offshore outsourcing can lead to 24-hour productivity.

There are also risks associated with outsourcing. In some cases, outsourcing can lead to a loss of competencies within the organization. This is especially problematic when this loss is related to the core activities of the organization. There are also risks related to the outsourcing relationship. There is a risk of becoming dependent on the service provider, which can lower bargaining power in later negotiations. In addition, there is a danger that the vendor may behave opportunistically and take advantage of the organization's lack of expertise or inadequate monitoring. Risks from opportunism are especially high when the outsourcing contract is not well structured. Outsourcing may also hurt the morale of the remaining workforce. Finally, there are risks related to confidentiality. Outsourcing vendors must ensure that sensitive information is properly protected. This is both a technical and human problem. Even when the proper technical security measures are in place, the employees of the service provider can compromise confidentiality. The benefits and risks of outsourcing are summarized in [Table 10.1](#).

TABLE 10.1 Benefits and Risks of Outsourcing

Benefits of Outsourcing	Risks of Outsourcing
• Access to expertise not available in-house • Potential cost savings • Shifting fixed costs to variable costs • Effective way to manage capacity • Focus on core activities • Potential for 24-hour productivity	• Loss of internal competencies • Dependence on service provider (lowers bargaining power) • Opportunistic behavior by service provider • Lower morale of remaining workers • Compromises to confidentiality

BUSINESS EXAMPLE BOX 10.2

Reversing the Outsourcing Decision

In 2005, Houston, Texas-based utility Reliant Energy outsourced some of its IT jobs to Accenture. As a result, Reliant cut approximately one-third of its 340 IT jobs. In 2009, Reliant reversed this decision and began hiring IT workers so it could bring the outsourced work back in house. Neither Reliant nor Accenture would comment on the reason for the reversal.

While still relatively rare, there are numerous other examples of “backsourcing” (bringing a previously outsourced function back in house). In 2004, JPMorgan Chase cancelled a multibillion-dollar outsourcing contract with IBM. IBM lost another contract when the UK Automobile Association canceled a £50 million outsourcing contract. In both cases, mergers were cited as the reason for the backsourcing. Poor performance can also cause backsourcing. In 2005, Sears Roebuck cancelled a \$1.6 billion contract with Computer Sciences Corporation due to what Sears claimed was a failure to meet obligations. Another example of backsourcing comes from General Motors in 2012, which backsourced its IT from HP by hiring 3,000 HP workers who had been providing outsourced services to GM. This provided GM the ability to hire the expertise back into their company to provide the skills they lost when they chose to outsource their IT department.

Sources: <http://www.computerweekly.com/blogs/outsourcing/2013/04/insourcing---outsourcing-backsourcing.html>; <http://www.computerweekly.com/news/2240167895/General-Motors-recruits-3000-HP-IT-workers>; <http://www.reuters.com/article/2010/01/30/urnidgns852573c400693880002576ba006e69d-idUS96268580820100130>; <http://www.computerweekly.com/Articles/2007/09/24/226946/AA-cancels->

Making the Outsourcing Decision

The decision of whether to outsource is very complex and depends greatly on the particular set of circumstances. However, there are some consistent factors that should be considered (Grover and Teng 1993):

- *How mature is the IT system in question?* Systems that have been around a long time are better candidates for outsourcing. There are several reasons for this. First, if the system is mature, organizations are less likely to be able to gain a competitive advantage from the system. Second, it is easier to find competent vendors for mature systems. This also means that organizations are more likely to have a choice of vendors, which is helpful during negotiations both initially and in the future.
- *How significant is the system to the organization's competitive advantage?* One common reason for outsourcing is to allow the organization to concentrate on core activities. Outsourcing is more suitable for systems that do not provide a competitive advantage. There is also a greater risk of loss of control when you outsource strategic systems; problems with strategic systems usually have serious consequences.
- *How does the organization's IT capability compare with that of its competitors?* In cases where an organization has relatively weak IT capabilities, it may be better to outsource. This is particularly true if the organization is weak in IT related to the system in question.
- *Are there cost advantages to outsourcing?* Of course, the question of costs is also important. Even if there are no savings through outsourcing, it may still be a good idea if outsourcing allows the organization to focus on critical areas or if the organization lacks the necessary capabilities.

Geographic Considerations

Where to outsource is an important aspect of outsourcing. (Note that choosing a vendor is also important, but here we focus on location.) **Offshore outsourcing** involves using a vendor that provides services from a location outside the client organization's region. A U.S. computer manufacturer outsourcing technical support to India is an example of offshore outsourcing. This is often done to reduce costs. Developing countries have much lower wages than developed countries, so offshore outsourcing can be very cost effective. However, there may be a backlash to offshore outsourcing. This can result from customers being upset about jobs sent overseas. Resistance can also come from poor language skills or cultural differences. Language and cultural differences, along with distance, can make offshore outsourcing arrangements difficult to manage.

Nearshore outsourcing is similar to offshore outsourcing. The difference is that nearshore outsourcing occurs close to the client's home location. If a U.S. company outsources to a Canadian firm, this would be a nearshore arrangement. The reduced travel times may make management easier. Cultural and language differences may be reduced, but this is not always the case. A U.S. company outsourcing to Mexico may still face considerable language and cultural barriers. A nearshore arrangement often results when a company wants to gain some of the cost savings of offshore outsourcing while reducing some of the management, language, and cultural difficulties.

Onshore outsourcing is outsourcing to a firm located in the same country. Onshore outsourcing may offer significant cost savings while eliminating the cultural and language barriers of offshore outsourcing. In addition, onshore outsourcing is less likely to bring about a customer backlash, since the jobs are staying in the country. Cost savings result from differences in wage rates for different areas of a country. Wages in rural areas are often considerably lower than in urban areas. As a result, rural onshore outsourcing saves significant money over urban areas and is only slightly more expensive than offshore outsourcing.

CHAPTER SUMMARY

In this chapter, we discussed various approaches to developing information systems. We began by describing the time, cost, and quality tradeoff. Then we talked about different software development methodologies, including the traditional systems development life cycle and its alternatives. We also discussed the build or buy decision and advantages and disadvantages of using open source software. The chapter concluded with a discussion of outsourcing. Here are the main points discussed in the chapter:

- Software development methodologies provide discipline to the development process by defining processes, roles, and deliverables.
- The traditional systems development life cycle (SDLC) is a semisequential, phased approach. There are different versions of the traditional SDLC.
- The SDLC described in this chapter consists of five phases: planning, requirements, development, implementation, and maintenance.
- Alternatives to the traditional SDLC include prototyping, rapid application development, and the spiral model.
- The decision of whether to build custom software or purchase commercial, off-the-shelf software is complex.
- Open source software allows users to access the underlying source code for the application, which allows users to modify the program.
- Open source software is usually free, although some companies charge a fee for ongoing support.
- Outsourcing occurs when an outside organization provides IT services that were previously provided internally.
- Outsourcing models include full (complete), process-based, personnel, project-based, and application outsourcing.
- There are both benefits and risks associated with outsourcing.
- Factors affecting the outsourcing decision include the maturity of the system, the system's significance to the organization's competitive advantage, the organization's IT capability, and cost.
- Offshore outsourcing occurs when an organization receives services from a company outside the organization's geographic region.
- Nearshore outsourcing occurs when an organization receives services from a company within the organization's geographic region but outside its home country.
- Onshore outsourcing occurs when an organization receives services from a company in the same country.

REVIEW QUESTIONS

1. What is the major benefit of a software development methodology?
2. What aspects of software development does a methodology specify?
3. Name and briefly describe the phases of the systems development life cycle described in the chapter.
4. Name and briefly describe the aspects of feasibility described in the chapter.
5. Name and describe three alternatives to the traditional SDLC.
6. Name the advantages and disadvantages of each of the software development methodologies described in the chapter.
7. List the advantages and disadvantages of custom; commercial, off-the-shelf (COTS); and hybrid approaches to software.
8. List the main characteristics of custom-built and COTS software.
9. What are the main factors to consider when deciding whether to build or purchase software?
10. Define open source software.
11. What advantages does open source software offer to businesses?

12. List and briefly describe the outsourcing models presented in the chapter.
13. List the major benefits and risks of outsourcing.
14. What factors should organizations consider when deciding whether to outsource?
15. How do offshore, nearshore, and onshore outsourcing differ?

REFLECTION QUESTIONS

1. What is the most important thing you learned in this chapter? Why is it important?
2. What topics are unclear? What about them is unclear?
3. What relationships do you see between what you learned in this chapter and what you have learned in earlier chapters?
4. How is the traditional systems development life cycle related to systems theory? (Recall that you learned about systems theory in [Chapter 2](#).)
5. What is the difference between functional and nonfunctional requirements? Why are they both important? Which do you think is harder to determine? Why?
6. Your organization needs to build a system to help users carry out a business process that is very unique to your organization.
 - a. Should your organization build this system from scratch or use a COTS system? Why? What additional information would be helpful in making this decision?
 - b. Do you think this should be outsourced? Why? What additional information would be helpful in making this decision?
7. Commercial, off-the-shelf (COTS) software is often of higher quality than custom-built software. This is especially true if the COTS software is widely used.
 - a. Why might COTS software be of higher quality?
 - b. Why would this be more likely if the COTS software is widely used?
8. What ethical issues are related to the decision to outsource a function? Are these issues different for offshore, nearshore, and onshore outsourcing?
9. There have been several instances of software development companies making formerly proprietary software open source. (See http://en.wikipedia.org/wiki/List_of_formerly_proprietary_software for a partial list of proprietary software that has been shifted to open source.) Why would a software development company do this? What would the company potentially gain? What would it potentially lose?

ADDITIONAL LEARNING ACTIVITIES

Learning Activity 10.A1

Form groups of two or three:

- One of you (the explainer) will answer the following question: What are the possible consequences of incorrect or poorly stated requirements?
- When the first person finishes, the other person (the questioner) will seek clarification and provides her or his own ideas.
- Record and be prepared to share your answer.

Learning Activity 10.A2

You need to recommend a software development methodology for an upcoming project. From the methodologies presented in this chapter, choose a methodology for each of the following projects. Briefly provide the rationale for each choice.

1. A system for monitoring electrical surges in an electrical power grid. The requirements for the system are well understood. Users will be required to use the system.
2. A contact management system. The system's potential users are unsure of exactly what they want the system to do. Use of the system will be voluntary.
3. A relatively small order-tracking system. The objectives of the system are well known, and potential users very much want such a system.

Learning Activity 10.A3

For each of the following, recommend whether the organization should build or buy the system in question. Explain your recommendation.

1. A medium-sized company that sells roofing materials to contractors needs a system that will allow customers to check product inventory through a website.
2. A large (Fortune 500) retailer with a large, well-skilled IT department needs a system that will track the purchasing habits of its frequent customers.
3. A large (Fortune 500) defense contractor needs a system that will track payments to vendors.

Learning Activity 10.A4

For each of the systems described in [Learning Activity 10.A3](#), what additional information would be useful in making your recommendation? Explain why the information would help in the build versus buy decision.

Learning Activity 10.A5

Locate open source alternatives for each of the following:

1. Microsoft Access database management system
2. Microsoft Outlook (email)
3. Adobe Photoshop
4. [Salesforce.com](https://www.salesforce.com) customer relationship management system
5. iTunes media player

Learning Activity 10.A6

Find two examples of back sourcing (bringing back in house previously outsourced functions or personnel) other than the examples described in the chapter. Provide a brief (one-paragraph) description of each. Include the reason for the back sourcing in your description.

Learning Activity 10.A7

Find two examples of outsourcing (other than the examples from the chapter). Provide a brief (one-paragraph) description of the outsourcing arrangement. Include the reason for outsourcing in your description. Also indicate which outsourcing model best describes the example.

REFERENCES

- Boehm, B. 1988. "A Spiral Model of Software Development and Enhancement." *IEEE Computer* 21(5): 61–72.
- Grover, V., and J. T. C. Teng. 1993. "The Decision to Outsource Information Systems Function." *Journal of Systems Management* 44(11): 34–38.
- IDC. 2014. "Smartphone OS Market Share, Q4 2014." <http://www.idc.com/prodserv/smartphone-os-market-share.jsp>.
- Linux Foundation. 2014. "The Linux Foundation Releases Report Detailing Linux User Trends Among World's Largest Companies." <http://www.linuxfoundation.org/news-media/announcements/2014/12/linux-foundation-releases-report-detailing-linux-user-trends-among>.

GLOSSARY

Application outsourcing: An outsourcing arrangement that involves a service provider handling activities related to a specific software application.

Functional requirements: Describes how a system should interact with users and other systems.

Nearshore outsourcing: Using a vendor that provides services from a location close the client's location.

Nonfunctional requirements: Constraints on a system.

Offshore outsourcing: Using a vendor that provides services from a location outside the client organization's region.

Onshore outsourcing: Outsourcing to a firm located in the same country.

Open source software: Software that allows users to access the underlying source code for an application.

Outsourcing: An arrangement in which an organization contracts with a service provider to provide IT-related services.

Personnel outsourcing: An outsourcing arrangement in which a service provider places workers into an organization on a temporary contract basis.

Process-based outsourcing: An arrangement in which an organization outsources a particular function or business process.

Project-based outsourcing: An outsourcing arrangement that involves contracting with a service provider to complete a specific project.

Prototype: A small-scale mock-up of a system or a portion of a system.

Requirements elicitation: Gathering system requirements from various stakeholders.

Selective (partial) outsourcing: An outsourcing arrangement in which only certain aspects of IT are outsourced to a service provider.

Software development methodology: a framework for planning, structuring, and controlling software development projects.

Source code: Text-based computer programming language statements that can be read by humans.

Systems development life cycle (SDLC): A semisequential, phased approach to systems development.

Use case: Describes a series of actions that results in an outcome for an actor.

CHAPTER 11

INFORMATION-BASED BUSINESS PROCESSES

LEARNING OBJECTIVES

By reading and completing the activities in this chapter, you will be able to

- Explain what a business process is
- Perform business process modeling
- Discuss the impacts of technology on business processes
- Explain how business process improvement can be achieved with business process reengineering (BPR)

CHAPTER OUTLINE

- [Focusing Story: Improving Processes Is for Everyone!](#)
- [Learning Activity 11.1: How Many Steps in This Process?](#)
- [What Is a Process?](#)
- [Process Modeling](#)
- [Learning Activity 11.2: Model This!](#)
- [Technology and Processes](#)
- [Process Improvement](#)
- [Learning Activity 11.3: Informal Business Processes](#)
- [Learning Activity 11.4: Redesign This!](#)
- [Chapter Summary](#)
- [Review Questions](#)
- [Reflection Questions](#)
- [Additional Learning Activities](#)
- [References](#)
- [Further Readings](#)
- [Glossary](#)

FOCUSING STORY

Improving Processes Is for Everyone!

This book is about information, and many of our examples seem to showcase technology companies. However, when we talk about business processes, or the way things are done in organizations, everyone can benefit from improvements—even companies that are in basic manufacturing industries like the cement industry.

Cemex is a 100-year-old multinational cement corporation based in Monterrey, Mexico. For years, it functioned pretty much like every other cement company, with limited communication among its various plants, constant changes in order information (customers cannot pour concrete in bad weather), and difficulty confirming precise deliveries to customers due to weather, traffic, and labor problems. Needless to say, customer satisfaction is not always high in this industry.

When Lorenzo Zambrano, the grandson of Cemex's founder, was appointed CEO, he looked for ways to improve processes. To handle unpredictable demands and changing conditions, the company realized it needed better real-time communications. It therefore implemented a satellite communication system (which they called Cemexnet) to connect all its cement plants. It also linked all offices via satellite and the Internet and created a central office for coordination. This allowed plants to be constantly aware of fluctuating supply and demand. The second main aspect of the overhaul was to develop a new tracking, scheduling, and routing system (which the company called Dynamic Synchronization of Operations). This logistics application uses GPS transmitters in each delivery truck, allowing dispatchers to allocate trucks to the plants closest to where they are at a given time. With detailed information on traffic conditions, inventory, and the customers' location, trucks can be rerouted as needed. Finally, suppliers, distributors, and customers of Cemex can use an online application to check order status.

The results have been impressive for Cemex: decreased delivery time from 3 hours to 20 minutes (98% of the time), increased customer satisfaction, substantially increased net sales, decreased number of delivery trucks (35% decrease in the first year), and substantial cost savings overall (e.g., fuel, maintenance, and payroll).

FOCUSING QUESTIONS

Identify specific ways in which the new technologies at Cemex changed the following:

1. How customers do business with Cemex
2. How delivery truck drivers do their work
3. How office staff work at Cemex
4. How plant managers handle business at Cemex

Source: Kaplan, S. 2011. "Business Process Improvement at Concrete Co. Cemex." *CIO Magazine*, August 15. <http://www.cio.com/article/2441369/process-improvement/business-process-improvement-at-concrete-co--cemex.html>.

LEARNING ACTIVITY 11.1

How Many Steps in This Process?

The organization you work for sells university-trademarked items to various consumers. It has traditionally sold goods through the bookstore but is now going to sell items (clothing, memorabilia, etc.) online. In this activity, your group represents a team of managers assembled to identify all the steps involved in managing the inventory for supporting the sale of goods online. Identify all the steps and substeps necessary for this to occur. Make a list of all the steps you think of.

What Is a Process?

A **process** is a series of steps or tasks required to achieve a specific goal. In organizations, everything that happens is based on a series of processes or key activities. They are often called *business processes*, but they could more precisely be labeled *organizational processes*, since processes exist not only in businesses but also in government agencies, charities, schools, and other noncommercial organizations. [Figure 11.1](#) shows an example of a process: the process of acquiring materials needed for the production of an enterprise's main goods. It should be noted that

while the process appears to be linear, it is not necessarily the case, since several activities can take place at the same time (concurrently).

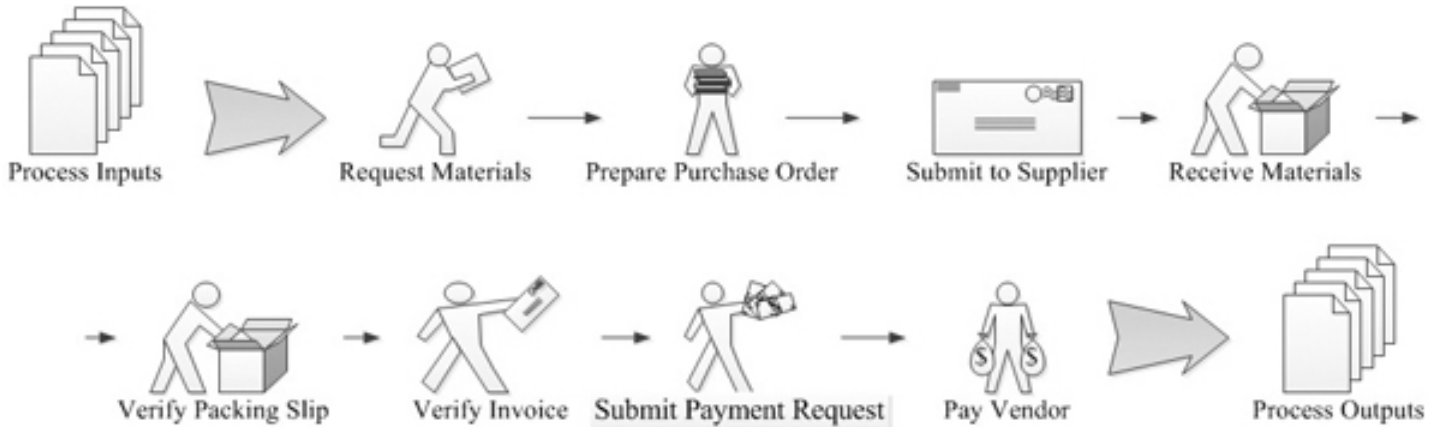


FIGURE 11.1 Example of a Process to Acquire Materials

Processes are not limited to one functional area of the organization. For example, in [Figure 11.1](#), it is likely that a production department will request materials, while an accounting department will pay vendors. This is an important point: processes extend across many organizational boundaries and tend to involve several individuals. Another key characteristic of processes is the **all-or-nothing concept**. This implies that a process needs to be completed or not done at all. Looking again at [Figure 11.1](#), requesting materials requires purchase orders, receiving materials, and so on. The process is not complete if there is no payment request or no payment made.

Every business process can usually be decomposed into several tasks, also called **subprocesses**. This is because processes usually require several decisions and actions to be made along the way. In general, there can be several levels of subprocesses, all the way down to specific activities or tasks. For example, in the process shown in [Figure 11.1](#), the subprocess of verifying the invoice involves viewing the invoice, viewing the ordering information, and comparing what was ordered with the charges. It can involve making sure that the proper discounts are given, which can require several steps (searching for discounts, comparing quantities, etc.). (See [Figure 11.2](#) for some possible subprocesses.)

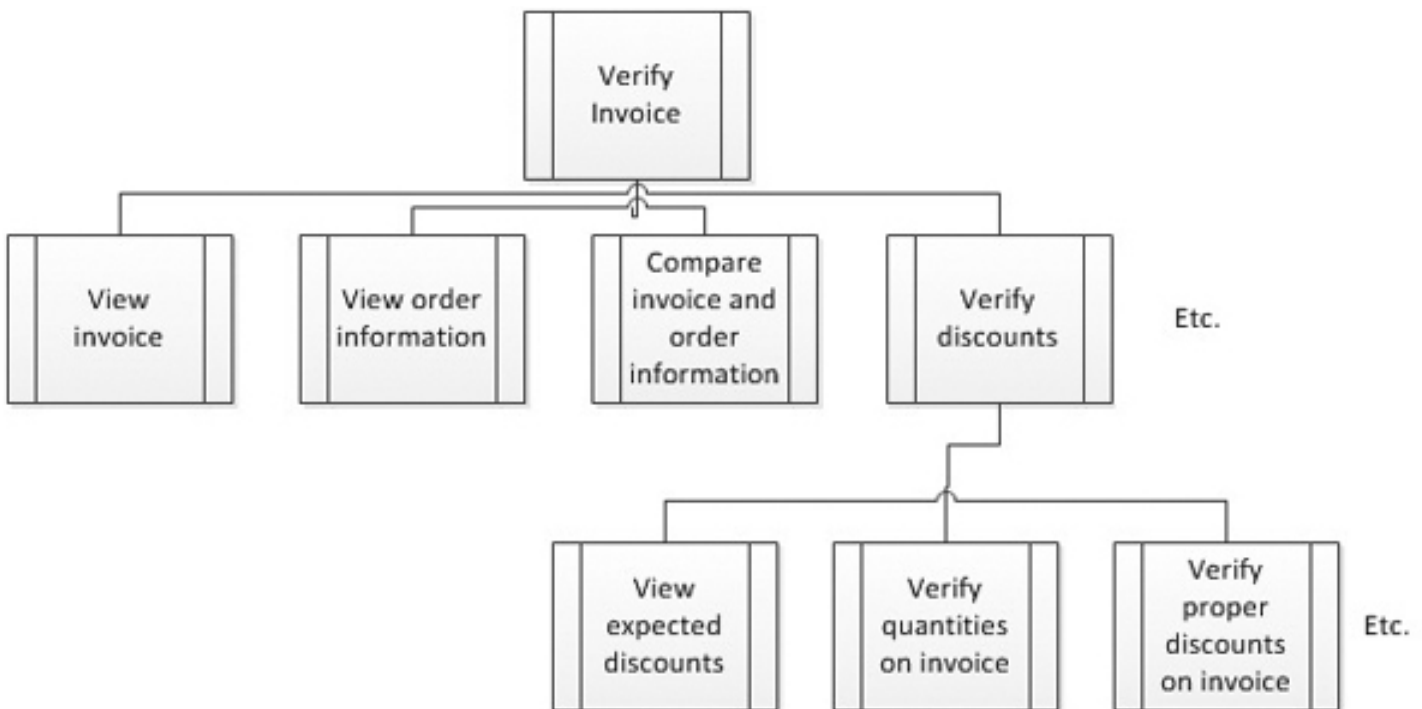


FIGURE 11.2 Examples of Subprocesses

Mapping the processes and subprocesses is called *process modeling*, which we describe in more detail below. There are many examples of processes you are familiar with even if you do not realize they are considered

processes. Think of course registration. What are the various steps involved? You need to identify the courses required for your program and the requirements for each course. You must then log into the registration system, enter your information, and make the requests. Next, you need to react to those requests that were denied. You can appeal them, try to force-add the course, or decide to take a different course. There are also processes for requesting transcripts, updating your personal information, or for instructors to enter grades, just to name a few.

Process Modeling

Process modeling is the mapping of processes and subprocesses used in an organization or division. Examine the process of acquiring materials needed for the production of an enterprise’s main goods in [Figure 11.1](#). Only the steps involved are identified. In process modeling, we need to expand the steps to identify when they are occurring and which decisions are involved. We must also recognize if there are any relationships between processes. The bottom line is that understanding which processes occur at different levels in the organization and how they interrelate is necessary to really understand how an organization works. [Figure 11.3](#) shows a process model for customers acquiring goods from a firm.

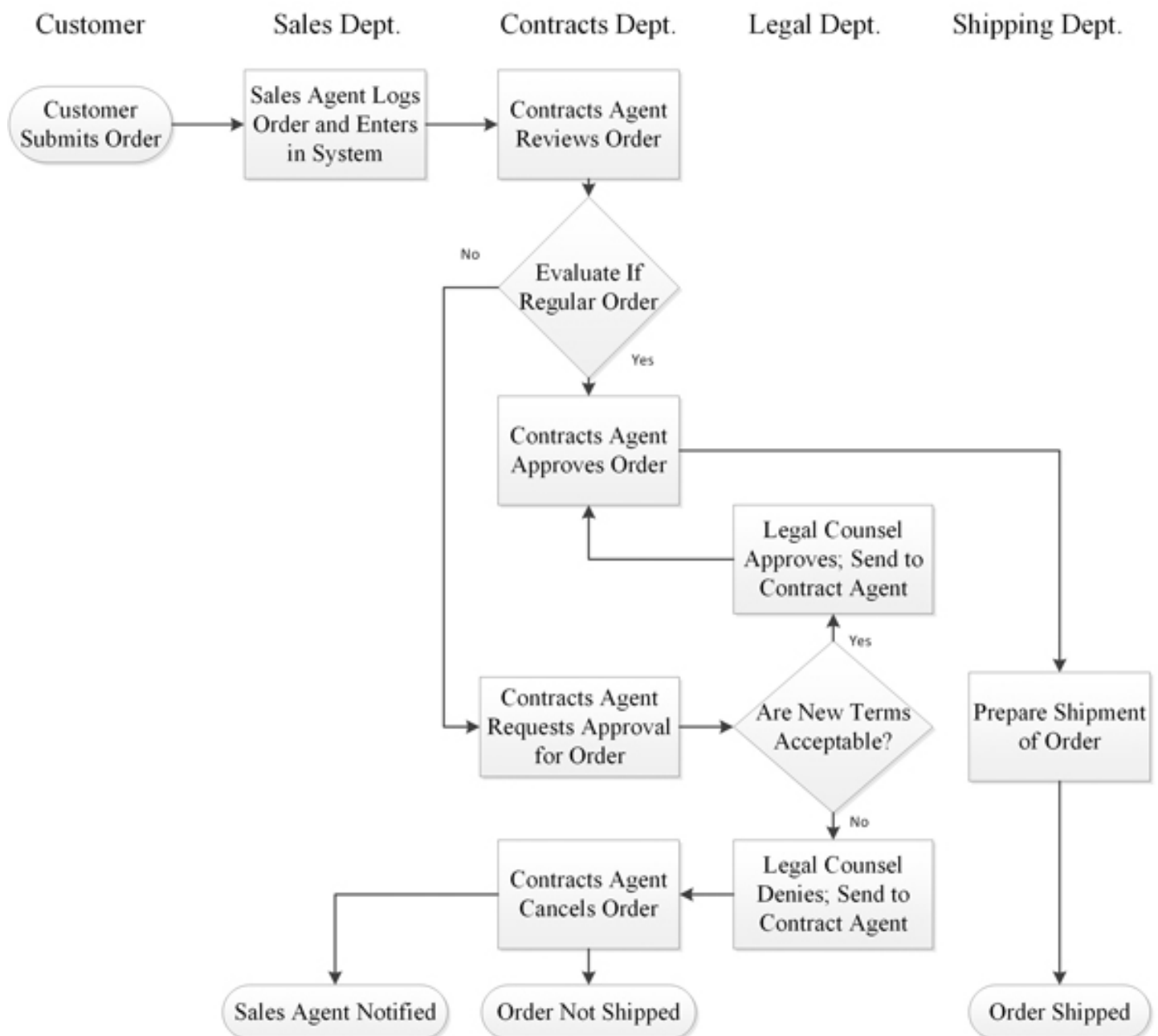


FIGURE 11.3 Process Model of a Process to Acquire Materials

A process model should clearly describe what happens as a process is performed. As analysts are modeling the processes, they should not analyze the process for improvements (yet); the goal is to describe the process as is. Process modeling can also be explanatory, in that the process modeling effort can identify the rationale for why processes are performed this way. Individual processes can be modeled, although organizations often model several processes simultaneously. Recall that processes are made of several subprocesses, which can also be modeled. As a result, process modeling usually results in “levels” of process models. [Figure 11.4](#) shows a refinement of the order entry subprocess from the process shown in [Figure 11.3](#).

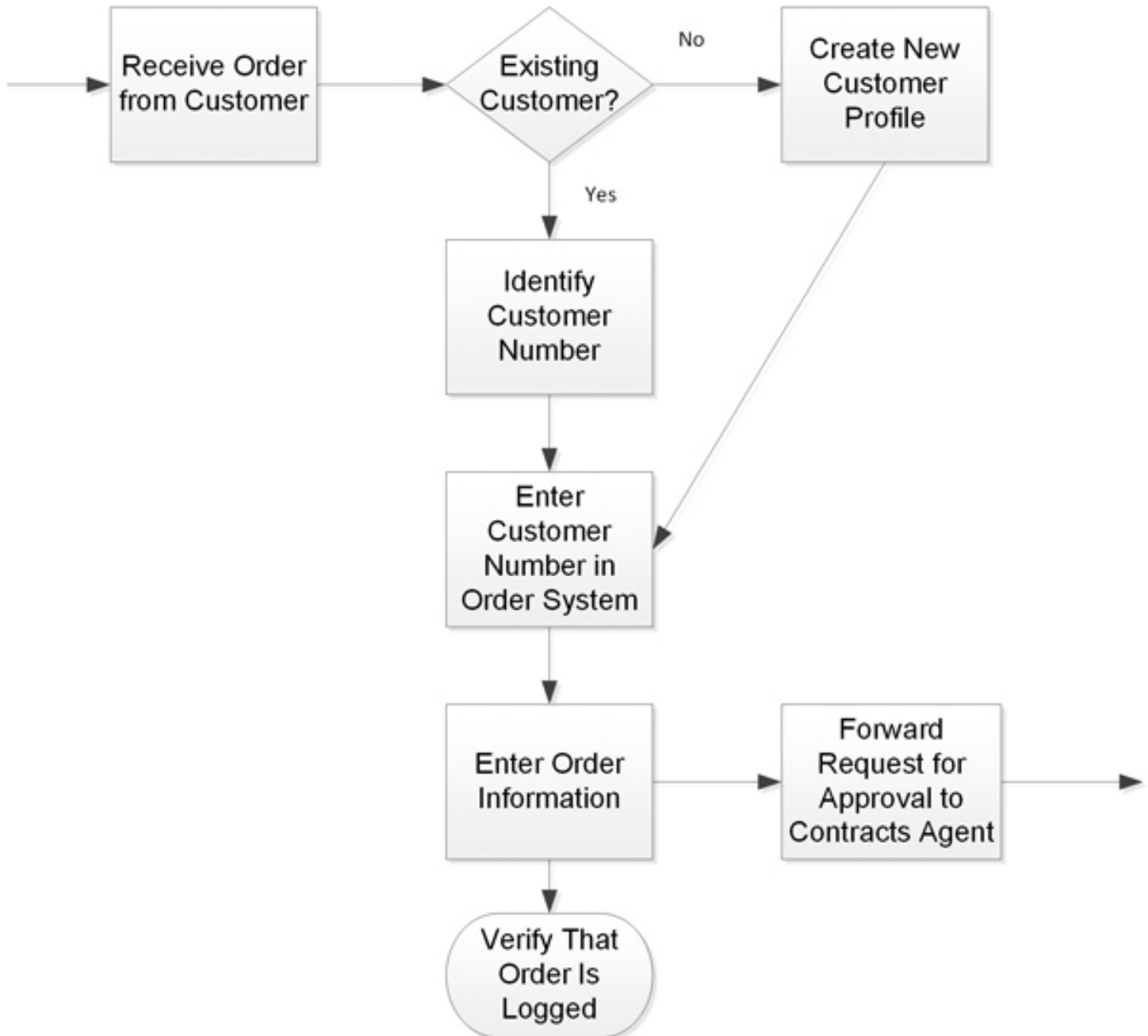


FIGURE 11.4 A Subprocess Model of Customer Goods Acquisition

[LEARNING ACTIVITY 11.2](#)

Model This!

Following up on [Learning Activity 11.1](#), your group of managers must now model the steps you identified in the inventory management process for your company. Make your process model as complete as possible.

Business Process Modeling Tools

There are many **process modeling tools** and software available to help analysts describe business processes and create business process models or diagrams. Mili et al. (2010) identify four types of such tools: traditional process modeling languages, object-oriented modeling languages, dynamic process modeling languages, and process integration languages. [Table 11.1](#) describes these various categories and shows some examples of these languages.

Analysts can become well versed in some of the languages presented in [Table 11.1](#), but to facilitate business process modeling, several companies have developed software specifically targeted at creating business process models. [Table 11.2](#) shows a few of the popular process modeling companies and software.

TABLE 11.1 Examples of Business Process Modeling Tools

Category of Modeling Tool	Description	Sample Languages
Traditional process modeling languages	Software engineering and information systems modeling languages mostly used in business process engineering	• Event-Driven Process Chain (EPC) • Role Activity Diagram (RAD) • Resource-Event-driven Process Chain (REPC) • Architectural Modeling Language (AMN) • Business Process Redesign (AMN)
Object-oriented modeling languages	Process modeling languages supporting the object-oriented approach to software development	• Object-Oriented Modeling Language (OORAM) • Enterprise Distributed Objects Computing (EDOC) • Unified Modeling Language (UML)
Dynamic process modeling languages	Process modeling language standards proposed by various—mostly industrial—organizations	• Workflow Process Definition Language (WPDL) • Business Process Modeling Language (BPML) • Web Services Business Process Modeling Language (WS-BPM) • Business Process Definition Language (BPDL) • Business Process Definition Language (BPDL) • Business Process Definition Language (BPDL)
Process integration languages	Process modeling languages for the purpose of integrating the processes of two or more business partners in electronic business	• RosettaNet • Electronic Business Language (ebXML) • Web Services Choreography Language (WS-CL)

Source: Mili et al. (2010).

TABLE 11.2 Sample Business Process Modeling Companies and Software Products

Company	Product	Address
Corel Corporation	DESIGNER Technical Suite X7	http://www.corel.com
CSG Systems Intec BPR Consulting and Process Modeling Software	Business Support Systems	http://www.csgsystems.com

Global 360	Open Text Cordys	http://www.opentext.com/what-we-do/process-management
Interfacing Technology	Enterprise Process Center	http://www.interfacing.com
KBSI, Knowledge Based Systems Inc.	Business Process Solutions (several)	http://www.kbsi.com/solutions-and-services
Microsoft Corporation	Visio Modeling Software	http://products.office.com/en-us/visio/
OpenText	Business Process Management	http://www.opentext.com/2/global/products/business-process-management.htm/
Oracle Corporation	Oracle Business Process Management	http://www.oracle.com/us/technologies/bpm
Silverrun BPM	Silverrun Modeling Tools	http://www.silverrun.com
Software AG	Business Process Analysis	http://www.softwareag.com

Technology and Processes

Business processes have existed since organizations started to organize work activities into tasks. Today, however, information technologies play an ever-increasing role not only in how business processes are performed, since technology is embedded in most work environments, but also in how business processes are modified or improved. We discuss business process improvement in the next section. Before we discuss how things can be done better, however, it is important to realize that technology not only enables new business processes but can also be a barrier or constraint to business process improvement.

Think about how much the tasks individuals perform in organizations are dependent on how the technology they use functions. It might be more efficient to input data a certain way, but the system will not let you do it. It could be useful to create a new report, but the system does not allow the data to be collated appropriately. This is even more apparent when we talk about legacy systems. Recall from the previous chapters that **legacy systems** are often older, large applications that may be mission critical. They are hard to replace and can be somewhat inflexible. In addition, they are often still used to support key business processes. Even if an organization creates a new, graphically friendlier interface to access information, what can be done with the information can be highly dependent on the type of data warehouse or application performing the back-office processing.

Process Improvement

Once business processes are properly modeled, they can be analyzed for improvement. Business process improvement is an important goal for managers, and it is often labeled **business process reengineering (BPR)**. BPR involves the redesign of business processes to improve how work is done, which of course means that BPR requires that business process modeling be done well first. It is important to realize that BPR often involves changing the way tasks are performed instead of just automating the tasks. It requires rethinking about what is done and how it is done (and even whether it should be done!). In one of their books on BPR, Michael Hammer and James Champy (2003) suggest that BPR involves the fundamental rethinking (really asking why an organization performs tasks in a certain way) and radical redesign of business processes (meaning that there is reinvention or re-creation, not just simple minor changes) in order to obtain dramatic improvements in performance (meaning that the goal is to achieve significant improvements for the organizations, whether in terms of cost, efficiency, satisfaction, or other important measures). There are usually four key areas for business process improvement: effectiveness, efficiency, internal control, and compliance. These goals are summarized in [Table 11.3](#).

TABLE 11.3 Typical Goals for Business Process Reengineering

Effectiveness	The extent to which the outputs of the process are obtained as expected
Efficiency	The average time it takes for the process to be completed
Internal control	The extent to which the information and data used in the performance of the process cannot be changed by error
Compliance	The extent to which the process follows the regulatory or statutory obligations of the organization

Summarizing our discussion so far, it is clear that BPR involves several phases, and just like our strategic planning process did in [Chapter 4](#), it starts with a clear vision of the goal of the redesign. It follows with an understanding of what the current processes are, how they work, who performs them, and who uses their outcomes. At the same time, redesign involves rethinking business processes, so analysts should not end up limiting themselves by focusing too much on how things are done as opposed how they should be done. Finally, a very important part of the redesign process is ensuring that there are measurements to make certain that improvements are indeed being made. As you can expect, the BPR effort is an iterative process in which what is done or found in later stages may result in the need to revisit earlier stages. [Figure 11.5](#) shows a sample BPR process.

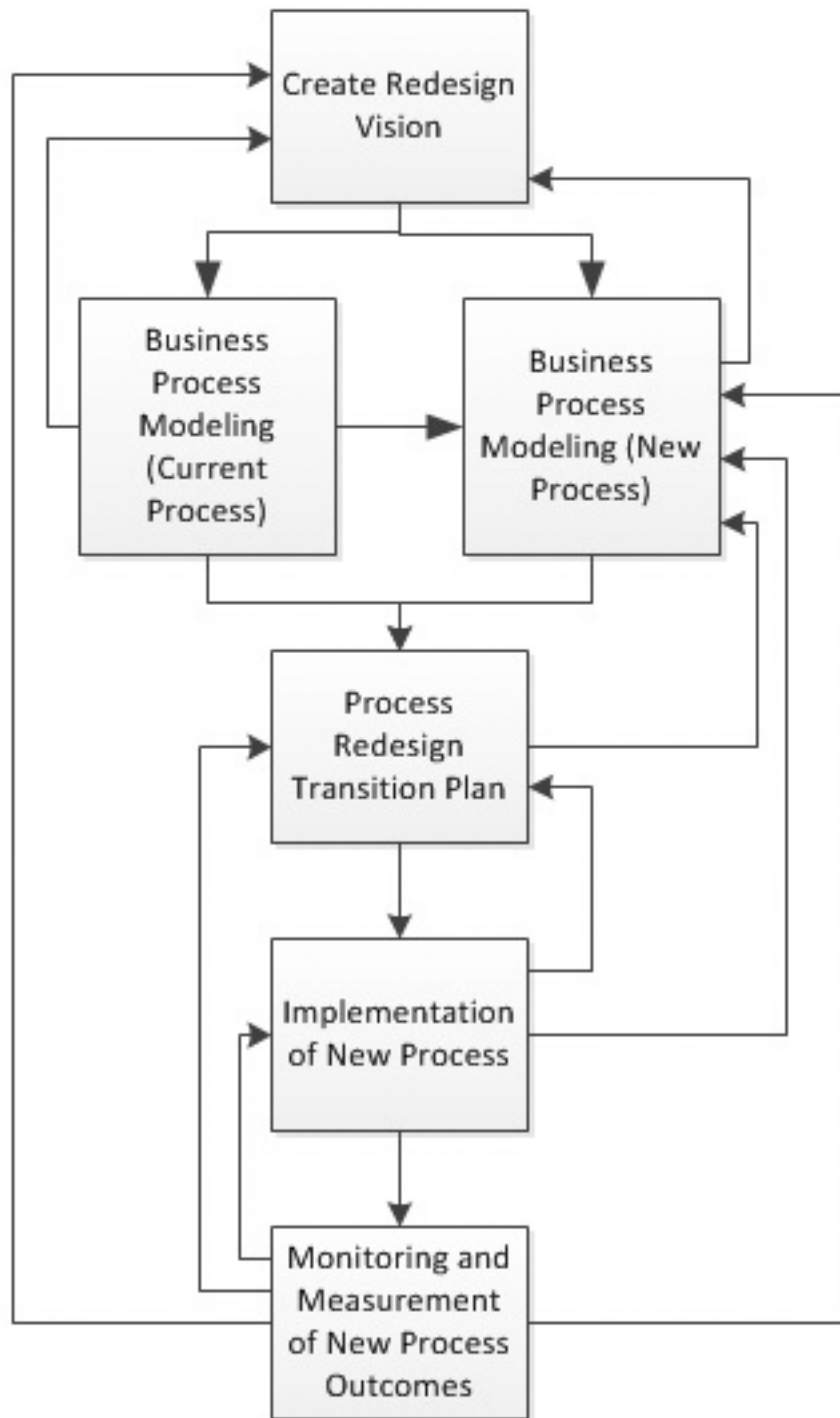


FIGURE 11.5 Business Process Redesign (Reengineering) Stages

Remember that, in the end, managers performing BPR need to ask themselves key questions such as the following:

- What are our key business processes?
- Do we have to execute each process?
- How can we use information technologies to perform these processes in better ways?
- What are the likely impacts of the business process redesign?

The result of a business process improvement effort should be a document that defines how the new business processes should or could be performed, indicating clear rules and guidelines that the processes must or should follow. For organizations, the results of a redesign of business processes are often streamlined ways of doing

business. [Figure 11.6](#) shows an example of the redesign of the business process from [Figure 11.4](#) after the organization offers online ordering.

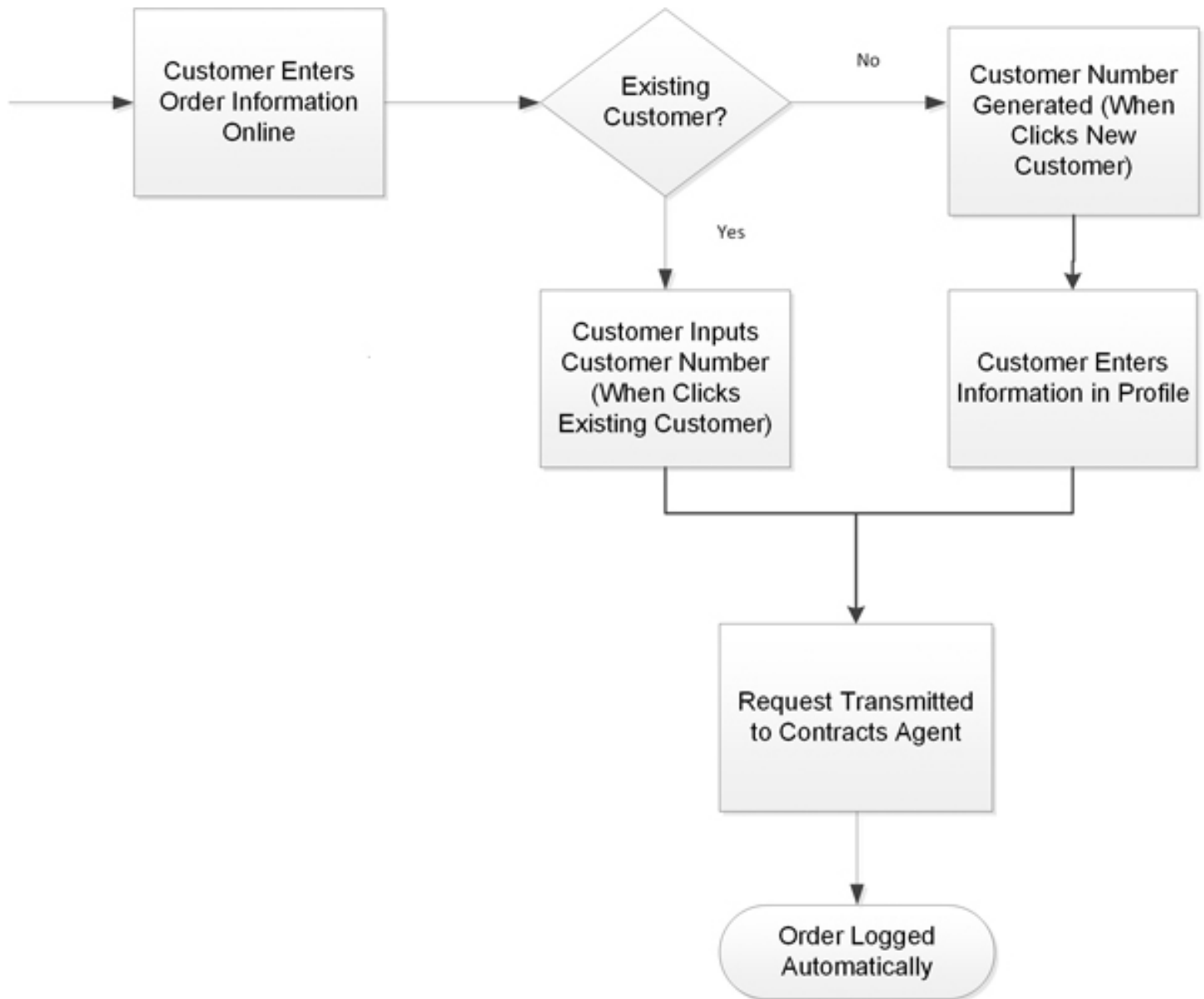


FIGURE 11.6 Online Ordering Redesign

LEARNING ACTIVITY 11.3

Informal Business Processes

In an organization, there are two types of business processes: official business processes and informal businesses processes. An official business process is one that has been documented and defined, as discussed in this chapter. An informal business process is a process that the business relies on but has not been properly documented. Based on these definitions, one could claim that an official business process is not the same as an informal process. For this learning activity, think about these definitions as you answer the following questions. Have your responses ready for discussion in class.

1. Is it true that these two processes are not always the same?
2. Why is that?
3. Which one should you model? Why?

Levels of Change

In [Chapter 4](#), we introduced the idea that information technology can be implemented in organizations for strategic purposes—in other words, to create competitive advantages. When new information technology (IT) is implemented, it can have differing effects on organizations depending on the role it plays in changing or supporting business processes. One way to categorize these impacts is whether they represent changes that automate, informate, or transform organizations (Dehning, Richardson, and Zmud 2003; Schein 1992).

- *Automate*, also called *first-order change*, involves using technology to perform a process more efficiently, often by replacing human labor with technology. It is usually fairly easy to justify because managers can quantify the benefits (e.g., reduced wages, reduced errors).
- *Informate*, also called *second-order change*, involves using technology to better inform people, which as a result can change how they perform business processes. Whenever people have to change how they perform business processes, it is more difficult to implement systems. Recall from our earlier discussions that people often resist technology implementations when they have to change their work habits.
- *Transform*, also called *third-order change*, requires a fundamental redefinition of the business processes, or how work is done. Obviously, since business process reengineering (BPR) involves the redesign of business processes, it is a third-order change. This is the most difficult level of change to deal with when implementing information systems.

[LEARNING ACTIVITY 11.4](#)

Redesign This!

This activity builds on what you have accomplished in [Learning Activity 11.3](#). Now that your team of managers has become more familiar with the inventory management system and has gained knowledge on business process improvement, your team should perform a redesign of the business process model you previously completed.

[BUSINESS EXAMPLE BOX 11.1](#)

ChoiceCare Physicians: Changing Access to Patient Records

Most students have gone to small doctors' offices where the receptionists and nurses have folders marked with different colors that contain tons of details about you, including a variety of paper charts. ChoiceCare Physicians, an eight-doctor private practice, is one of those offices that had a very large room specifically dedicated to storing all the charts and reports needed by doctors, nurses, and staff. When staff needed to access documents, they had to look for the charts that, depending on the situation, could be in a variety of locations. This was quite inefficient when patients called for results, with documents sometimes logged in the existing system and sometimes not because they were not yet completed. Similarly, insurance companies would request documents that were in different formats and locations. Staff had to spend a significant amount of time finding these different documents, if they could be found. In the end, it was easy to misplace a document, and it was very hard to find other documents.

To solve this situation, ChoiceCare implemented a document management system that allowed them to digitize all documents and store them together in one place. Staff personnel register every document in a digital format as the document is created, filled, or signed. When anyone (with proper access) needs a document, it can be easily accessed as needed. Since the documents are digitized, it is harder to lose them (with proper backup facilities) and easier to find them (since they can be indexed and/or searched). The system also avoids duplication of files for the same patient, since the document management system can flag a file that has a similar name.

Source: Health Management Technology. "Change Unmanageable Work-Flow Procedures." 2010, April. *Health Management Technology* 31(4): 18–19.

CHAPTER SUMMARY

In this chapter, we explained in greater depth what business processes are, how they can be modeled, and how organizations seek to improve business processes through business process reengineering (BPR). Here are the main points discussed in the chapter:

- A business process is a series of steps or tasks required to achieve a specific business goal of an organization.
- Business process modeling is the mapping of processes and subprocesses used in an organization or division. We demonstrated business process modeling with graphic models of a materials acquisition process and its subprocesses. Business process modeling helps us understand the various processes that occur at different levels in the organization and how they interrelate.
- Technology impacts business processes because it is embedded in how work is done in most work environments. Technology could be a constraint to business processes, especially when legacy systems are involved.
- Business process improvement can be achieved with business process reengineering (BPR), which involves the redesign of business processes to improve how work is done. BPR often involves changing the way tasks are performed instead of just automating the tasks. There are usually four key areas for business process improvement: effectiveness, efficiency, internal control, and compliance.

REVIEW QUESTIONS

1. Explain what a business process is and give an example from your school environment.
2. Identify some of the important characteristics of processes.
3. What is business process modeling, and what is the purpose of business process modeling?
4. Identify some of the important characteristics of a process model.
5. What kinds of tools are available for business process modeling?
6. How does technology impact business processes?
7. What is business process reengineering (BPR), and what does it involve?
8. What are the four key areas for business process improvement?
9. Briefly explain the main steps involved in performing business process redesign.
10. What are some of the results expected from a business redesign effort?

REFLECTION QUESTIONS

1. What is the most important thing you learned in this chapter? Why is it important?
2. What topics are unclear? What about them is unclear?
3. Identify all the processes a student encounters during the first week of class as a freshman.
4. How does the business process-related material in this chapter relate to the security topics in [Chapter 8](#)?
5. How does the business process-related material in this chapter relate to the privacy topics in [Chapter 9](#)?
6. Can all business processes be redesigned? Why or why not?
7. What are the similarities and differences between process modeling as discussed in this chapter and data modeling as discussed in [Chapter 5](#)?
8. Should informal business processes (representing how things are really done, even if they do not follow recognized or documented procedures) be modeled or just formalized business processes (those documented by the organization)?

9. What is an example of technology being a barrier to redesign in a school setting?
10. Why do you think business process reengineering is an important concern for CIOs?

ADDITIONAL LEARNING ACTIVITIES

Learning Activity 11.A1

This activity allows you to get some additional practice at business process redesign. First, you need to download the template of one of the business processes (your instructor will tell you which one) from Global 360: <http://www.global360.com/process-templates/>. In small groups, examine the template and then, with business process redesign in mind, modify the business process you downloaded to improve it.

Learning Activity 11.A2

This activity requires you to complete a case analysis regarding business processes. The case may be accessed through your university website, the Ivey Business School business case website (<https://www.iveycases.com>), or the Harvard Business School cases website (<http://cb.hbsp.harvard.edu/cbmp/pages/home>), or it may be provided to you by your instructor.

Raghu, T. S. 2010. "CASE: Creating a Process-Oriented Enterprise at Pinnacle West." *Ivey School of Business*, February 5. Product number: 910E02-PDF-ENG.

Learning Activity 11.A3

Examine [Figure 11.2](#), identify one of the subprocesses of the order entry process, and model it, as was done in [Figure 11.4](#) for the order entry part in the sales department.

Learning Activity 11.A4

Select one of the key processes needed at your school and model it. You can select one from the following list or you can identify another important process and model it:

- Class registration
- Final grade assignment
- Student enrollment
- Tuition payment
- Requesting transcripts

Learning Activity 11.A5

Use the process modeling tools in the Visio software to create your models in Learning Activities 11.A3 or 11.A4.

REFERENCES

- Dehning, B., V. J. Richardson, and R. W. Zmud. 2003, December. "The Value Relevance of Announcements of Transformational Information Technology Investments." *MIS Quarterly* 27(4): 637–56.
- Hammer, M., and J. Champy. 2003. *Reengineering the Corporation: A Manifesto for Business Revolution*. New York: HarperCollins.
- Mili, H., G. Tremblay, G. Bou Jaoude, É. Lefebvre, L. Elabed, and G. El Boussaidi. 2010, November. "Business Process Modeling Languages: Sorting through the Alphabet Soup." *ACM Computing Surveys* 43(1): 7–62.
- Schein, E. H. 1992. "The Role of the CEO in the Management of Change: The Case of Information Technology." In *Transforming Organizations*, edited by T. A. Kochan and M. Useem, 325–45. Oxford: Oxford University Press.

FURTHER READINGS

- IBM. 2015. "Business Processes." http://www-01.ibm.com/support/knowledgecenter/SS7J6S_7.0.0/com.ibm.wbit.help.bpel.doc/topics/cunder.html?cp=SS7J6S_7.0.0&lang=en.
- OpenText. 2015. "Business Process Management (BPM)." <http://www.opentext.com/what-we-do/products/business-process-management>.

GLOSSARY

All-or-nothing concept: The idea that a process needs to be completed or not done at all.

Business process reengineering (BPR): The redesign of business processes to improve how work is done.

Compliance: A BPR goal that involves the extent to which the process follows the regulatory or statutory obligations of the organization.

Dynamic process modeling languages: Process modeling language standards proposed by various (mostly industrial) organizations.

Effectiveness: A BPR goal that involves the extent to which the expected outputs of the process are obtained as expected.

Efficiency: A BPR goal that looks at the average time it takes for the process to be completed.

Internal control: A BPR goal that involves the extent to which the information and data used in the performance of the process cannot be changed by error or illegally.

Legacy systems: Older, large applications that may be mission critical.

Object-oriented languages: Process modeling languages supporting the object-oriented approach to software development.

Process: A series of steps or tasks required to achieve a specific goal.

Process integration languages: Process modeling languages for the purpose of integrating the processes of two or more business partners in electronic business.

Process modeling: Mapping of processes and subprocesses used in an organization or division.

Process modeling tool: Tools and software available to help analysts describe business processes and create business process models or diagrams.

Subprocesses: Decomposition of business processes into several tasks.

Traditional process modeling languages: Software engineering and information systems modeling languages mostly used in business process engineering.

CHAPTER 12

ENTERPRISE INFORMATION SYSTEMS

LEARNING OBJECTIVES

By reading and completing the activities in this chapter, you will be able to

- Identify the main characteristics and types of enterprise systems
- Discuss the purposes of enterprise resource planning (ERP) systems
- Explain the purposes and functioning of supply chain management (SCM) systems
- Identify the components of customer relationship management (CRM) systems
- Apply the customer life cycle concepts to CRM

CHAPTER OUTLINE

- [Focusing Story: Supply Chain Innovations at Wal-Mart](#)
- [Learning Activity 12.1: Finding the Components of an Enterprise System](#)
- [Enterprise Systems](#)
- [Enterprise Resource Planning \(ERP\)](#)
- [Learning Activity 12.2: The Online Beer Game](#)
- [Supply Chain Management Systems](#)
- [Learning Activity 12.3: Customer Relationship Management](#)
- [Customer Relationship Management Systems](#)
- [Learning Activity 12.4: Self-Servicing](#)
- [Customer-Managed Interactions \(CMI\)](#)
- [Chapter Summary](#)
- [Review Questions](#)
- [Reflection Questions](#)
- [Additional Learning Activities](#)
- [References](#)
- [Further Readings](#)
- [Glossary](#)

This chapter is about enterprise systems, which are systems that are used by a large number of individuals throughout an organization. We will discuss various ways enterprise systems are developed and explore several such systems. One of these enterprise applications is supply chain management (SCM), which is the topic of interest in the focusing study.

Supply Chain Innovations at Wal-Mart

You need a new pair of inexpensive jeans or maybe just a new set of travel speakers for your iPhone. Where would you go to buy these? Many students would turn to a local Wal-Mart store, since the company is well known throughout the world as a low-cost retailer of goods. What makes it possible for the company to offer prices that often seem to be well below what competitors can afford to offer? Of course, there are many answers to this, but one of the most important factors is how Wal-Mart manages the way it gets the products sold in its stores. This is the supply chain. Wal-Mart calls this the *productivity loop*: lower-cost products lead to lower prices for consumers, which lead to more sales, which increase profits, and then it repeats the loop as quickly as possible. However, there are many other benefits for Wal-Mart and its partners in the supply chain, as explained below.

Wal-Mart is well known for its innovative strategies regarding its supply chain and its tight management of its distribution channels. By 2010, Wal-Mart had established four very large global merchandising centers that are responsible for ordering goods and clothing products (also called *sourcing*) for the company's stores in 15 countries. It also uses direct purchasing of fresh fruits and vegetables from producers on a global basis, bypassing traditional suppliers.

Wal-Mart's supply chain strategies cover many aspects, but in a speech given at the Council of Supply Chain Management Professionals (CSCMP) annual conference in 2009, Gary Maxwell, then senior vice president of international supply at Wal-Mart, explained that effective inventory management may be the most critical element to master for an efficient supply chain.

To improve the effectiveness of its supply chain, Wal-Mart mandated in 2003 that its largest suppliers use **RFID (radio-frequency identification) tags**. This required suppliers to insert electronic tags into pallets of goods to be shipped to Wal-Mart. Using readers, both Wal-Mart and the supplier can then track the pallets as they move through the various distribution centers all the way to the store. Wal-Mart has been a leader in the development of the RFID technology. However, while it has successfully reduced out-of-stock items (8% worldwide) and improved its overall inventory data (it can resupply three times faster), the adoption of the technology was slower than expected. For many companies, the cost was quite high (from US\$100,000 to US\$300,000 for small companies to US\$20 million for larger ones). In 2003, first-generation chips sold for US\$1.25 each. In 2009, second-generation chips cost 7¢ to 10¢. By late 2008, 600 of Wal-Mart's 60,000 suppliers, plus 750 Sam's Club (owned by Wal-Mart) suppliers, deployed RFID to some degree. On Wal-Mart's end, RFID is deployed at about 1,000 of the roughly 4,000 Wal-Mart and Sam's Club stores in the United States.

Today, suppliers and Wal-Mart reap many other benefits from RFID, such as knowing in real time how long it takes for items in the promotional areas of stores to sell. They can even evaluate where in the store items sell better. This is a win-win situation for Wal-Mart and its suppliers. Some suppliers have even built the use of RFID tags into their whole information technology (IT) infrastructure, from acquisition to sales to replenishment.

Wal-Mart continuously strives to innovate in its supply chain. Its most recent effort is convincing its suppliers that reducing gas emissions and becoming more "green" in their delivery of products to Wal-Mart can result in profitability and sustainability. Wal-Mart is asking some suppliers to report how much energy they use in manufacturing the products Wal-Mart buys from them and requires them to meet stricter quality and environmental standards.

FOCUSING QUESTIONS

1. What do you believe are the key success factors for the supply chain implementation at Wal-Mart? What would those factors be for other companies trying to imitate Wal-Mart's supply chain efforts?
2. What is your assessment of Wal-Mart's move into RFID technology as a leader? Could there be an issue being at the leading edge of technology?
3. How can technology be used to help Wal-Mart in its next endeavor—its green supply chain?

Sources: Compiled from Berman, J. October 2009. "Wal-mart's Maxwell Cites Keys to Developing Best-in-Market Global Supply Chains." *Logistics Management* 48(10): 18; Birchall, J. 2010. "Wal-Mart Takes Aim at Supply Chain Cost." *Financial Times*, January 4: 1; Cassidy, W. B. 2010. "Wal-Mart Squeezes Costs from Supply

Chain.” *Journal of Commerce*, January 5; McCrea, B. 2010, March. “This Is Why ‘Green’ Equals Good Business.” *Supply Chain Management Review* 14(2): 56; Webster, J. S. 2008. “Wal-Mart’s RFID Revolution a Tough Sell.” *Network World*25(36): 34–36.

[LEARNING ACTIVITY 12.1](#)

Finding the Components of an Enterprise System

The supply chain management system at Wal-Mart represents only one type of enterprise system companies can use for running their businesses efficiently. One of the most popular enterprise systems in organizations is enterprise resource planning (ERP). We will discuss enterprise systems and ERP later, but for now, we want you to identify the components of an ERP system offered by the one of the larger companies, such as SAP, Oracle PeopleSoft, or Microsoft Dynamics.

Please prepare a short report for class that identifies the company that sells the ERP system, a brief background on the company, the components of the ERP system, and a brief description of each component. The report should be fewer than two pages long.

[Enterprise Systems](#)

Personal versus Enterprise Systems

There are many information system applications used by individuals and companies to perform tasks. For example, if you think of applications you use that are for individuals only, you might find that Quicken is used to manage your finances or that Microsoft Word is used to write your term papers. Those are considered **personal information systems**. Conversely, **enterprise systems** are information systems that serve the needs of the organization or parts of the organization. For example, the organization may use SAP’s enterprise resource planning (ERP) applications to manage its finances, including paying bills, receiving invoices, and paying employees. In [Learning Activity 12.1](#), you identified many other components of an ERP system. As you recall, many modules are available to perform functions needed across several departments in the organization.

Three perspectives on developing enterprise systems have emerged: the hierarchical perspective, the functional perspective, and the process perspective (Piccoli 2008).

In the hierarchical **perspective**, software developers build information systems to mirror the organization so that applications are built to meet the needs of individuals at a given level in the organization. The idea is that executives need strategic types of information they can use for decision making, whereas middle managers and front-line managers need tactical and operational information, respectively. [Table 12.1](#) shows the type of information needed at each level and the characteristics of that information, which is also reproduced in [Figure 12.1](#).

TABLE 12.1 Types of Information Required by Hierarchical Level

Activity	Time Horizon	Hierarchical Level	
Strategic	Long term	General management	• Externally focused
		Functional management	• Highly unstructured
Tactical	Mid term	Middle management	• Semistructured • Recurrent
Operational	Short term	Operation management	• Highly structured
		Employees	• Transaction focused

Source: Adapted from Piccoli (2008).



FIGURE 12.1 Hierarchical Information Systems

As a result, systems are built for operations, tactical, or strategic management, with sometimes limited interaction and consistency across these systems. Redundancy is also a problem, with different systems sometimes performing fairly similar functions.

In the **functional perspective**, information system applications are developed to meet the needs of individuals in a functional area, such as human resources or marketing. With this perspective, information system developers build a “financial” system, a “marketing” system, a “production” system, or a “human resources” system. The systems tend to serve the functional area well, as they are customized to the needs of the department. Again, when thinking about the various functional areas in an organization (often called *departments*), you can see that information system applications built this way could result in redundancy and inaccuracy of data. (Think of having to update customer information in five different departments.) This perspective also limits communication across functional areas.

Finally, in the **process perspective**, information systems applications are developed to support the task being done (or process) irrespective of the organizational level or functional area of the individual using the system. A *process* is a series of steps required to perform a task.

Integration and Enterprise Systems

The discussion of the three perspectives for the development of enterprise systems highlights some of the issues that arise when systems are not developed with the organization as a whole in mind. In particular, we discussed the issues of redundancy (identical data stored in multiple locations) and lack of communication across departments. To solve these problems, the process perspective focuses on integration. Integration is the unifying, or joining together, of resources and assets. This is clearly one of the primary advantages of enterprise systems, which are designed to integrate either across business processes or across information systems.

Business integration is the unification of business processes previously performed as separate activities in order to create cohesive and streamlined business processes. In other words, business integration refers to ensuring

that processes are performed the best way they can be, without having barriers along the functional areas (departments) or hierarchical levels. This is accomplished by making sure the processes are performed at the best location and by allowing access to everyone who needs the information. This is also called **data integration**. Examples of enterprise systems that provide business integration include customer relationship management (CRM) and enterprise knowledge management. **Systems integration** is the unification of information systems and databases that were previously operating as separate systems. Systems integration focuses on the technological components of information systems. Examples of enterprise systems that are used for systems integration include enterprise resource planning (ERP), content management systems (CMSs), supply chain management (SCM), unified communications, and enterprise application integration. As you can see, most enterprise systems are designed to facilitate the flow of information among all business functions inside the boundaries of the organization and to manage connections to outside stakeholders. A brief description of some of these enterprise systems is provided in [Table 12.2](#). The three most popular (ERP, SCM, and CRM) are further described in the chapter.

TABLE 12.2 Examples of Enterprise Information Systems

Tool	Description
Customer relationship management (CRM)	An organization-wide strategy for managing an organization’s multiple interactions with customers to attract, retain, and manage customer relationships—for example, by offering personalized services. CRM also allows an organization to analyze customer data to find its most profitable products, services, and markets, both technology and a philosophy of customer service.
Enterprise knowledge management (also called business intelligence [BI])	A set of tools used to analyze business data to find trends, issues, and opportunities. Companies use large amounts of data, such as sales, revenues, or expenses, to name a few, and BI tools show various reports to help decision makers. BI tools include a wide variety of analysis approaches, such as online analytics, data analytics, or data and text mining.
Enterprise resource planning (ERP)	ERP software allows organizations to manage resources throughout the organization, independent of function controls the resource. Typical modules in ERP software include financial management, human resources management, and manufacturing.
Content management systems (CMSs)	CMS applications allow companies to manage the vast amounts of information of various types and formats. This includes the capture, storing, preservation, and delivery of content. CMS refers to technological approaches to managing content.
Unified communications (UC)	UC is a framework for the integration of the various modes of communication used by an organization, such as email, videoconferencing, instant messaging, texting, and voice over IP. For example, a customer service request automatically sent as an email to the account representative (based on preferences). Similarly, an instant message can be transferred immediately to a voice mail if the representative is currently unavailable.
Enterprise application integration (EAI)	EAI is a set of tools and services (a framework instead of a single technology) to allow various applications (such as ERP or CRM) to share the data. It makes use of middleware (see Chapter 7) to perform this coordination.
Supply chain management (SCM) systems	SCM software helps organizations manage the movement of materials or products from provision to consumption. SCM involves collaboration between partners both upstream and downstream from the organization. (Upstream and downstream flows are shown in Figure 12.3 .)

Sources: Adapted from Pearlson and Saunders (2010); Piccoli (2008); [Wikipedia.com](#).

Characteristics of Enterprise Systems

The enterprise systems presented in [Table 12.2](#) have some common characteristics. First, many of these systems are modular. This means that an organization can implement the “pieces” it needs one at a time. By implementing modules as needed, the organization can limit its efforts and costs and limit disruptions for employees. However, because the modules are designed to be integrated with one another, they function more efficiently together. This

concept, called **application integration**, works because an event that occurs in one module automatically triggers events in one or more of the other modules. In addition, because data are stored in one central database, by offering data integration, companies avoid the data redundancy and inaccuracy issues found in hierarchical or functional information systems.

Enterprise Resource Planning (ERP)

As previously discussed, an **enterprise resource planning (ERP)** system is a set of information systems tools that are used to manage an organization's resources and enable information to flow within and between processes (and departments). Before ERP, organizations developed different applications to manage the information processing and management needs of the different functional areas of the organization. With ERP, various modules offer integrated management of these resources. Typical modules in ERP systems include financials (accounts receivable, general ledger, accounts payable, etc.), distribution services, human resources, and product life cycle management (marketing). Some ERP systems also include other enterprise systems applications, such as customer relationship management (CRM), supply chain management (SCM), and warehouse management systems (WMS).

Like other enterprise systems, ERP applications are built on a centralized database, as shown in [Figure 12.2](#), and offer system and business integration. The ERP system itself can reside on a centralized server, or it can be distributed across modular hardware and software units that are interconnected. Many vendors offer commercial ERP packages (such as SAP, Oracle PeopleSoft, and Microsoft Dynamics) that tend to include the collective experience of its consultants. As a result, such packages are said to include best practices from the industry. However, the biggest challenge with ERP systems is to customize them to the needs of the organization and to the computing platforms used within the organization.

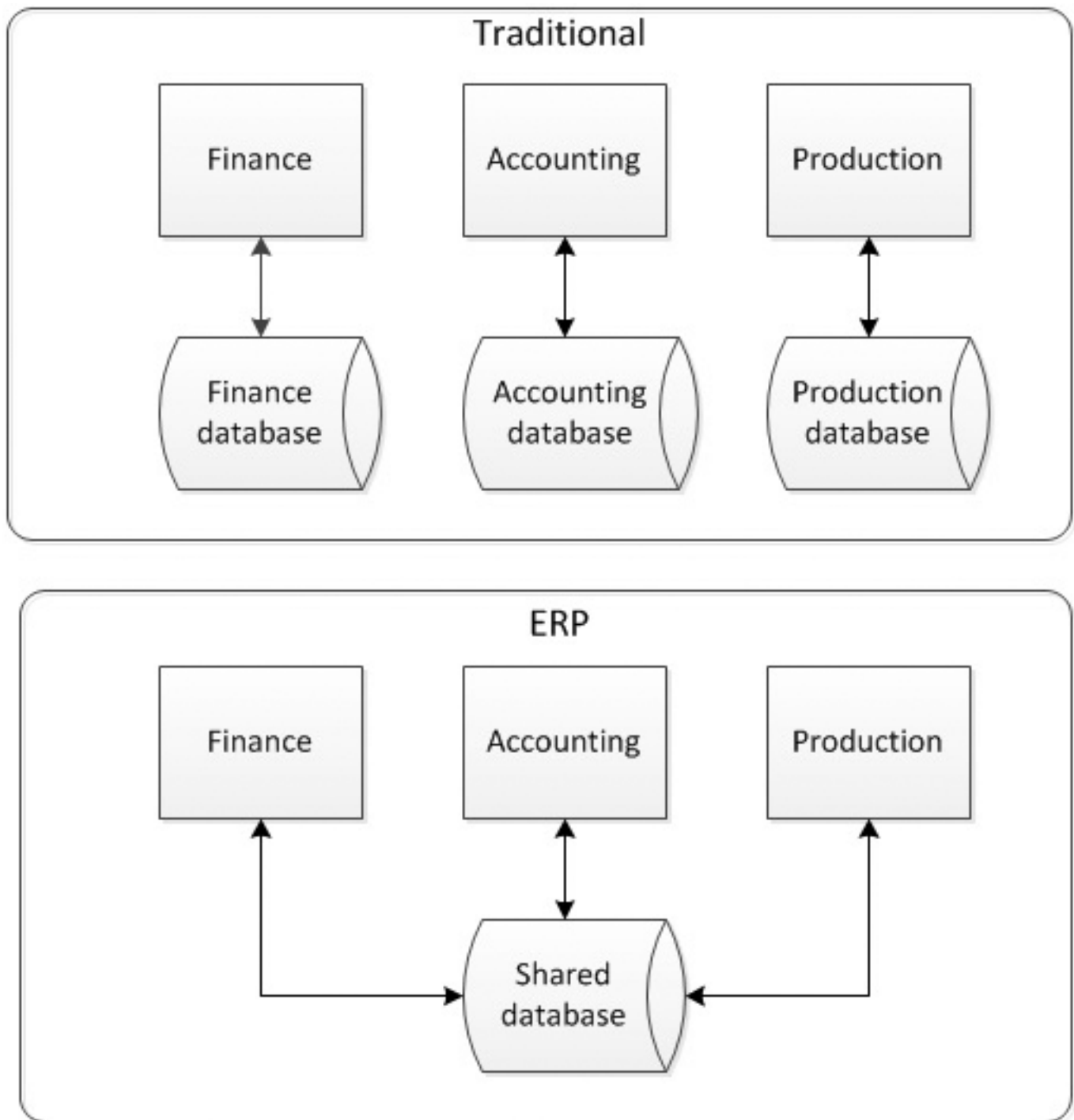


FIGURE 12.2 ERP Shared Database

Benefits and Disadvantages of ERP Systems

There are many benefits for organizations that successfully implement an ERP system. Efficiency is the most important of these, as it is quantifiable. Efficiency is achieved because ERP systems can reduce data redundancy (reduce direct costs of operation), improve communication (reduce indirect costs of operation through the streamlining of business processes), and in general allow complex systems to work together in an integrated fashion (also streamlining business operations and making sure tasks are performed in a standardized way). If properly implemented, ERP systems can also offer responsiveness to various stakeholders, including customers and suppliers, by providing more accurate information and more rapid responses to demands. ERP systems are also adaptable, since they can be configured to fit the organization's needs. However, when an ERP system

becomes too customized, it can lose some of the advantages of integration and standardization offered by the standard packages. Finally, ERP systems benefit from the expertise of ERP software vendors and consultants who, through experience implementing many of these systems over the years, have embedded into their software packages the state-of-the-art processes used in an industry.

BUSINESS EXAMPLE BOX 12.1

The Power of ERP Data: How Slumberland Furniture Cleaned Up Its Supplier List

Slumberland Furniture is a private bedding and furniture chain of 120 stores based in Little Canada, Minnesota. The company sells furniture it buys from a number of suppliers. As with many companies, Slumberland management had some perceptions as to which suppliers were better providers than others. This all changed, however, in 2008, when the company started an ERP business intelligence project to understand which furniture suppliers were most profitable. The company wanted to focus on facts instead of perceptions.

Slumberland's ERP system includes point-of-sale and order-management applications and provides sales information, including which products sell fastest in which stores and at what prices. Collecting information from the ERP application, together with the retail system and the warehouse management system, Slumberland identified data such as how many times a dresser or La-Z-Boy recliner had been moved around a warehouse or from one distribution center to another and who moved it. In performing its analyses, the company also considered subjective information such as ratings by its managers of how well suppliers responded to questions or helped solve problems that occurred.

After analyzing its supply chain data found in the ERP system, Slumberland found some surprising revelations. For example, it realized that the more large, heavy pieces of furniture (like the La-Z-Boy) were moved, the greater the risk of damaging it (which meant the company had to either spend money repairing it or send it back to the manufacturer). In the words of the company's director of information services, "Analyzing this data showed the true cost of doing business with each supplier," including shipping delays or how often some items are moved between or within warehouses. Slumberland was surprised to find that some vendors previously thought to be its most profitable partnerships were in reality not working out well. For example, some offered discounts but repeatedly delivered orders late. Others had packaging that was complicated and costly in labor to remove. As a result of analyzing its ERP data, Slumberland "cleaned up" its list of suppliers and started working more closely with better-performing vendors. In the end, the company believes it was able to reduce its inventory (and therefore costs) by 10%.

Source: Nash, K. S. 2009, November 1. "Furnishing Higher Profits; A BI Project Using ERP Data Allowed Furniture Retailer Slumberland to Find Its Most Profitable Suppliers." *CIO* 23(3).

ERP systems also suffer from a number of significant disadvantages. First, they represent an enormous amount of work and very high costs. Because most organizations do not use directly "off-the-shelf" applications but instead customize them substantially, ERP implementations can take anywhere from six months (for a few modules) to six years (for a full implementation). There are even stories of implementations lasting up to 12 years. One study reveals that in recent implementations of ERP, 72% of organizations said the implementation took longer than expected (Panorama Consulting Group 2014). Costs of ERP implementations vary depending on the size of the implementation, from a few hundred thousand (US) dollars to many millions. One reason implementing an ERP system is not as simple as loading the software is that it involves changing the way business is done. Business processes that have been in place for a long time may need to be redesigned. Users accustomed to the old way of doing business may offer significant resistance to an ERP implementation. Departments that have to relinquish control of some data or applications may also be resistant to the implementation. The bottom line is that an ERP implementation is often risky and complex, but the benefits can be substantial and worth the effort.

A recent study confirms that the typical disadvantages of ERP implementations still exist. The study shows that ERP implementations take longer and cost more than expected and underdeliver business value. The study also reveals that organizations do not do a good job managing the organizational changes that result from an ERP implementation (Panorama Consulting Group 2014). Why is it that many ERP implementations are so difficult? Because, as we said, they often involve changes in processes and people's jobs; they therefore represent a third-

order change ([Chapter 11](#)). In addition, they are often very large in scope and may require more customization than initially expected. Finally, ERP implementations require a strong champion, a person who believes enough in the implementation to see it through many obstacles and years of effort.

STATS BOX 12.1: TOP FOUR SELECTED ERP VENDORS

In a 2014 survey of companies who have implemented an ERP system, Panorama Consulting identified the top four vendors that are most often selected (the percentage of time the company's software is selected from a short list of vendors) once they have made the short list of vendors: Oracle (34%), Microsoft (20%), SAP (16%), and Epicor (10%).

Source: Panorama Consulting Group (2014).

LEARNING ACTIVITY 12.2

The Online Beer Game

As seen in the focusing story, supply chain systems are very important enterprise systems for organizations that must receive raw materials or products needed for their manufacturing or resale operations. Before we discuss the concepts in greater depth, it is helpful to experience the issues surrounding proper management of supply chains. To do so, please connect to the Beer Game developed by MIT (Massachusetts Institute of Technology) professors, which can be found at <http://beergame.pipechain.com>. Use the Web-based version of the Beer Game for this exercise. Select a new game and choose one of the four positions for how to play the game.

After you have completed the game for the time allotted by your instructor, be prepared to discuss the following questions:

1. How does information impact your supply chain decisions?
2. How could information systems help with the information needs of managing a supply chain?

BUSINESS EXAMPLE BOX 12.2

ERP Is Not Always a Horror Story: Cisco Implementation on Time and Budget

Enterprise resource planning (ERP) implementations make good horror stories for IT and business managers to talk about. As discussed in this chapter, they are often way over budget and delayed by months and sometimes years. However, there are also some good stories. For Cisco Systems, Inc., an ERP implementation went well and achieved its planned budget and time objectives.

Cisco, founded in 1984, produces telecommunications equipment. It quickly became a Fortune 500 company as a result of the growth of the Internet. To support its core business operations in the mid-1990s, Cisco used a UNIX-based software package that handled its core finance, manufacturing, and order entry functions. At the time, each functional area (business unit) used the system but made its own decisions regarding the future of its IT systems. As a result, the systems were often "upgraded" by each department for its own needs. When the CIO of Cisco at the time, Pete Solvik, decided to analyze the software applications, he found that the software package in use lacked the reliability, maintainability, and redundancy (backup) needed. A failure in the legacy system in 1994 that led to a two-day shutdown of operations resulted in the need for a new system.

As with many CIOs, Cisco's CIO was trying to avoid ERP because he was concerned that an ERP solution would involve implementation headaches and cost overruns. In particular, the independent department structure would not work well with an integrated ERP. However, the ERP did seem the best solution for the company's needs, so a consulting company was hired to help Cisco select a vendor and implement the ERP system. KPMG Consulting helped prepare the ERP request for proposal and then helped Cisco select Oracle as their ERP vendor. The agreement also involved Cisco helping Oracle market new releases to potential customers in exchange for a successful implementation within budget and on time.

The implementation team then prepared a budget and schedule, committing to top management that everything would be done within nine months for \$15 million. Using a rapid iterative prototyping to implement the ERP, 30

developers spent three months modifying the Oracle ERP system to support Cisco’s business processes. After several phases of analysis, development, implementation, corrections, and training, the final implementation was done on time and below the \$15 million budget. Meeting its goals, Cisco management offered the implementation team a bonus pool of more than \$200,000.

Source: Datta, A. 2009, April–June. “Cisco Systems: Implementing ‘Customized’ ERP in Nine Months and within Budget.” *Journal of Cases on Information Technology* 11(2): 56ff.

Supply Chain Management Systems

The focusing story at the beginning of the chapter introduced the concept of supply chain management (SCM) at Wal-Mart. We discussed how managing the flow of goods in its supplier and distribution channels helps the company tightly control its inventory and reduce its costs. Supply chain management, however, can also apply to services, financial products, knowledge, and relationships, as well as goods.

The typical **supply chain** involves the flow of goods from the manufacturer to the wholesaler to the retailer and to the consumer. A typical supply chain is shown in [Figure 12.3](#). Firms that provide or supply an organization’s products or services are considered upstream, while firms that distribute an organization’s products or services are considered downstream.

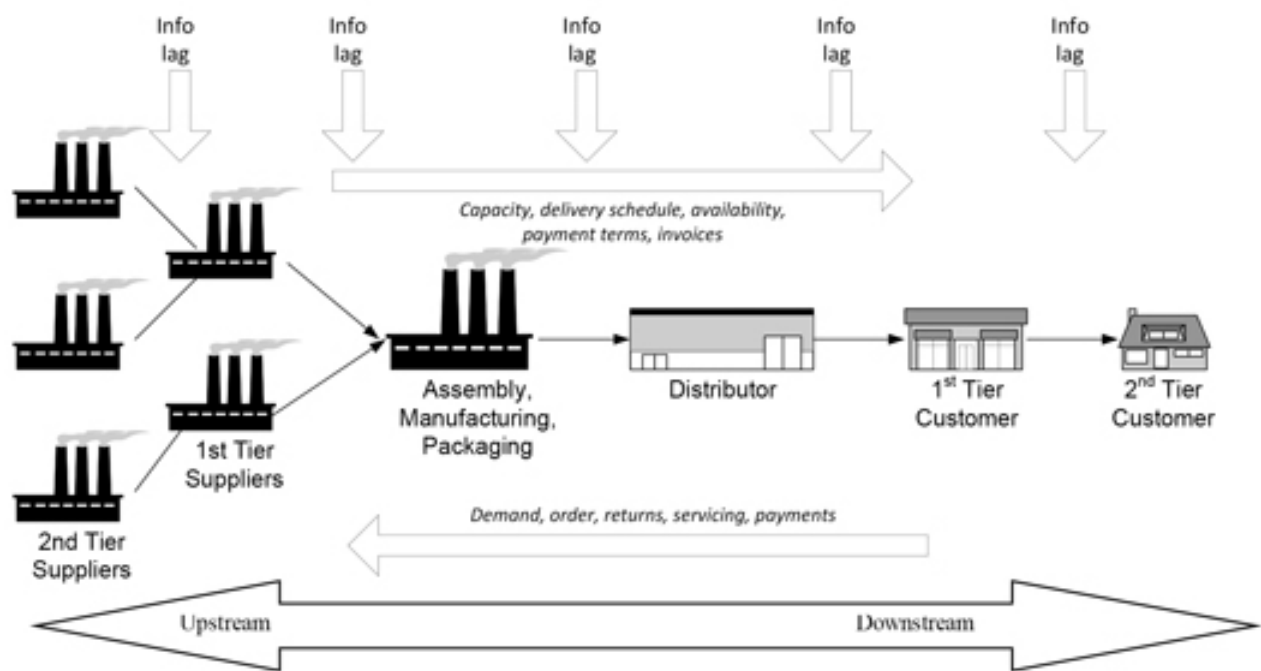


FIGURE 12.3 Traditional Supply Chain

As you can tell from your experience with the Beer Game ([Learning Activity 12.2](#)), everyone in the supply chain benefits from collaborating with other members of the supply chain. You have also discovered (depending on how you did) that a poorly managed flow of goods can result in a disaster for a company. Some of the worst supply chain disasters are presented in [Table 12.3](#).

TABLE 12.3 Supply Chain (and Other) Disaster Examples

Year	Company	What Happened?
Halloween 1999	Hershey	Due to new order management and shipping systems (implementing both ERP and SCM simultaneously) critical Halloween orders. \$150 million in revenues were lost as stock dropped 30%.

Christmas 1999	ToysRUs.com	The online retail division could not make its Christmas delivery commitments to thousands. Infamous December 23; eventually, Amazon took over fulfillment.
2001	Cisco	A lack of demand and inventory visibility as the market slowed led to a \$2.2 billion inventory write-off.
2001	Nike	A new planning system caused inventory and order woes. This was blamed for \$100 million in lost sales and price by 20%. It also triggered a flurry of class-action lawsuits.
2005	Loblaws	Plans for a significant logistics network makeover ran into poor execution problems. The company blamed results on high costs and lost sales from the effort. The CEO apologized to shareholders. Even though it stabilized by early 2006, the stock price never recovered from the hit.
2007–9	Boeing	Plans to radically overhaul the supply chain for the new <i>Dreamliner</i> 787 aircraft sound good, but mass production delays led to a two-year delay in the aircraft's launch and some \$2 billion in charges to fix supplier problems.
Christmas 2013	UPS	UPS did not have the capacity to supply deliveries for a spike in orders during Christmas 2013. In part, orders spiked by 63%. As a result, companies such as Toys R Us and Amazon.com had to inform customers that packages would not be delivered in time for Christmas.

Sources: Gilmore (2009); SCDigest (2014).

Enterprise systems are key to the management of the supply chain. A well-managed supply chain can result in a reduction in inventory costs, since products can be ordered as needed as opposed to being stored for long amounts of time. It can also reduce the amount of returned items through better inventory information. SCM can also improve a company's overall relationships with partners in the supply chain through more accurate and timely communication about the flow of products, information, and payments. These can be referred to, respectively, as the product flow (movement of goods), information flow (orders and delivery status), and financial flow (credit terms, payment schedules, and consignment and title ownership arrangements). A good SCM system also allows companies to offer just-in-time (JIT) inventory. This is when firms are able to maintain the lowest level of inventory while still being able to fulfill demand. Because SCM systems provide notices of inventory stock depletion in real time, personnel (or systems) are able to order new stock immediately.

The key to SCM's success rests in the sharing of information both upstream and downstream. Today, most companies use Web-based interfaces to access inventory, delivery, and other information from their SCM systems. The SCM systems also tend to be increasingly integrated with other enterprise systems, such as ERP and CRM systems.

STATS BOX 12.2: SUPPLY CHAIN'S IMPACT ON COMPANY PERFORMANCE

Statistical evidence suggests that enhancements in their supply chain can help companies improve their performance. Here are some statistics that support this:

- The use of drones is making same-day delivery possible, especially in densely populated areas. Drones can travel at 50 miles per hour and carry up to five pounds; 86% of the items that Amazon.com sells are fewer than five pounds, which means there is a great potential for drone delivery.
- In 2014, 60% of organizations were automating their supply chains by pursuing increased mechanization. This is expected to increase to 83% by 2018.
- The Internet of Things has utilized RFID technologies in such a way that from 2012 to 2014, the value of the RFID market has increased from \$6.96 billion to \$8.89 billion. It is expected to reach \$27.31 billion by 2024. The use of this technology enables smart devices in homes, cars, and elsewhere to seamlessly communicate with other devices over the Internet. This helps improve efficiencies in the supply chain.

Source: Cerasis, <http://cerasis.com/2015/01/16/supply-chain-facts/>.

LEARNING ACTIVITY 12.3

Customer Relationship Management

An enterprise system that has gained importance in recent years is customer relationship management (CRM). Before we discuss the concept in greater depth, learn about CRM by visiting the following demonstration websites:

- Salesforce: https://www.youtube.com/watch?v=mbo8_VHaBWw
- Microsoft Dynamics CRM: <http://www.microsoft.com/en-us/dynamics/crm.aspx>

Be prepared to discuss the following points in class:

1. What are the purposes of a CRM system?
2. What types of tasks can be accomplished with a CRM system?
3. Who benefits from a CRM system?
4. What are the benefits for each stakeholder?
5. What types of companies should have a CRM system? Why?

Customer Relationship Management Systems

Customer relationship management (CRM) refers to an organization-wide strategy for managing an organization's multiple interactions with customers. For example, when dealing with a company to buy a product, you might talk to a person via a toll-free phone number, send an email, chat in an instant messaging box with a customer representative, or simply perform your transaction online without “talking” with anyone. These are all channels of interaction.

CRM involves a set of activities (including a philosophy of customer service) and technologies (the CRM system) meant to help companies understand the needs of current and potential customers. The CRM system allows organizations to attract and retain customers and to manage customer relationships—for example, by offering personalized services and self-servicing tools. It also allows a company to analyze customer data to find its most profitable products, services, and customers.

Broadly speaking, there are three main goals for CRM (META Group 2001). First, CRM systems help organizations manage multiple channels of interaction with customers in ways that the customers prefer. The second goal of CRM systems is to provide an integrated picture of the customer across the various customer-facing parts of the organization. The third major goal of CRM systems is to enable the analysis of customer-related information. This information is gathered through interactions with customers, although external data (such as census data) may also be involved.

TABLE 12.4 Goals of CRM

Manage multiple channels of interaction with the customer

Provide a unified view of the customer across the enterprise

Analyze information collected to improve campaigns, services, and products

Source: META Group (2001).

Customer Service Life Cycle

The **customer service life cycle (CSLC)** is a framework to help us understand the various tasks a CRM system can be useful for. The CSLC is a series of phases that customers pass through when interacting with an organization. There are a number of variations on the phases, but they are all similar. Our simplified CRM includes four phases; engage, transact, fulfill, and service. [Table 12.5](#) summarizes the phases and shows some

specific CRM-related applications that can be useful for each CSLC phase. The combined phases are referred to as a *cycle*, as shown in [Figure 12.4](#), because completion of one round of the cycle often leads to another round. Note that in the following discussion, we refer to products, but similar statements could be made about services.

TABLE 12.5 Phases in the Customer Service Life Cycle

Phase	Description
Engage	Creating customer awareness of the product or service. The goal of the engage stage is to generate leads and then convert leads into customers.
Transact	All activities associated with the purchase process. The goal of this phase is to efficiently and effectively complete the purchase process so that customers do not abandon the purchase process.
Fulfill	Delivery of the product or service to the customer.
Service	Supporting the customer during the ownership of a product or service.

Source: Adapted from Van Slyke and Bélanger (2003).

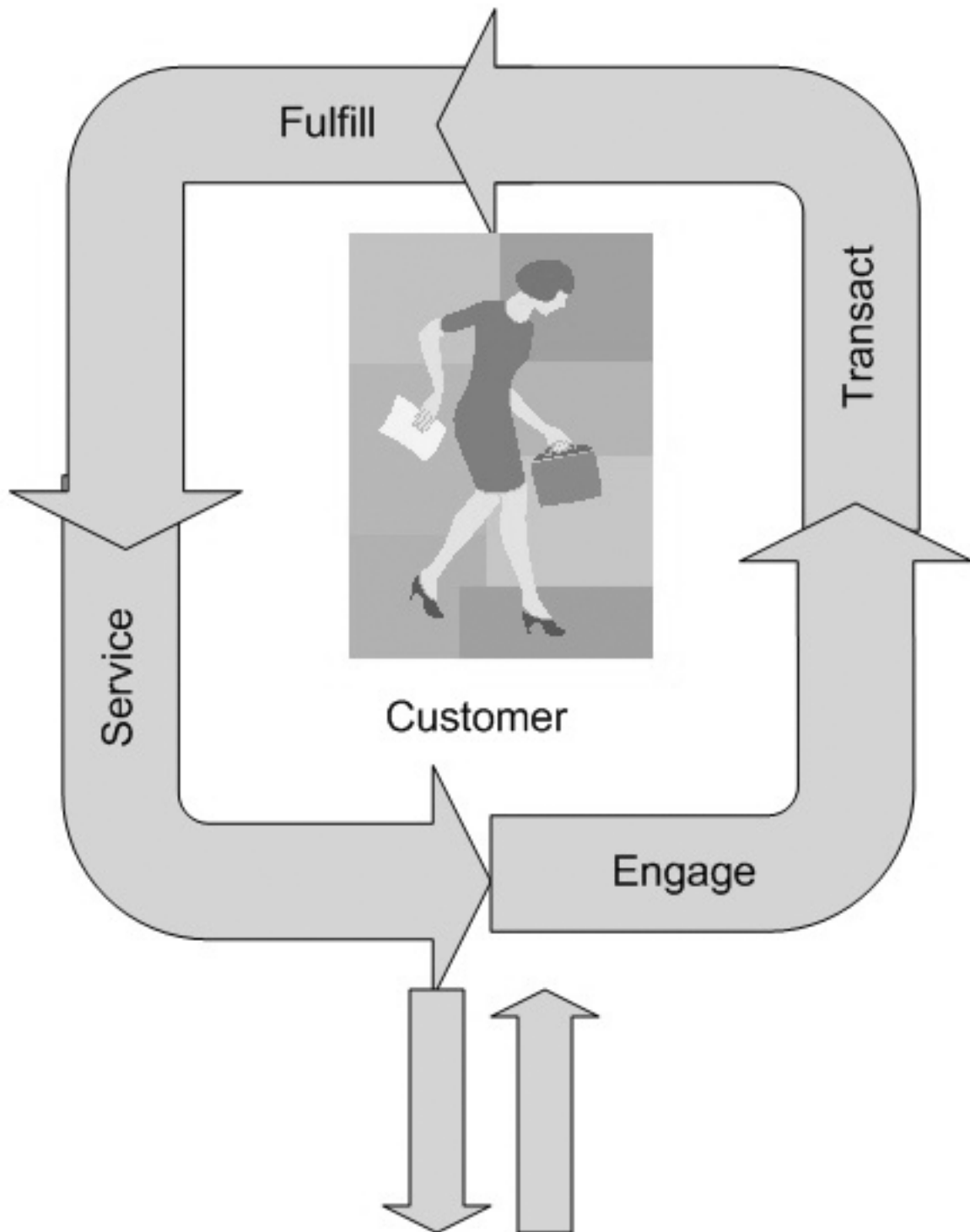


FIGURE 12.4 Customer Service Life Cycle
Source: Adapted from Van Slyke and Bélanger (2003).

Components of CRM Systems

CRM systems have three main components: operational, collaborative, and analytical (Van Slyke and Bélanger 2003). [Figure 12.5](#) shows how the components work together.

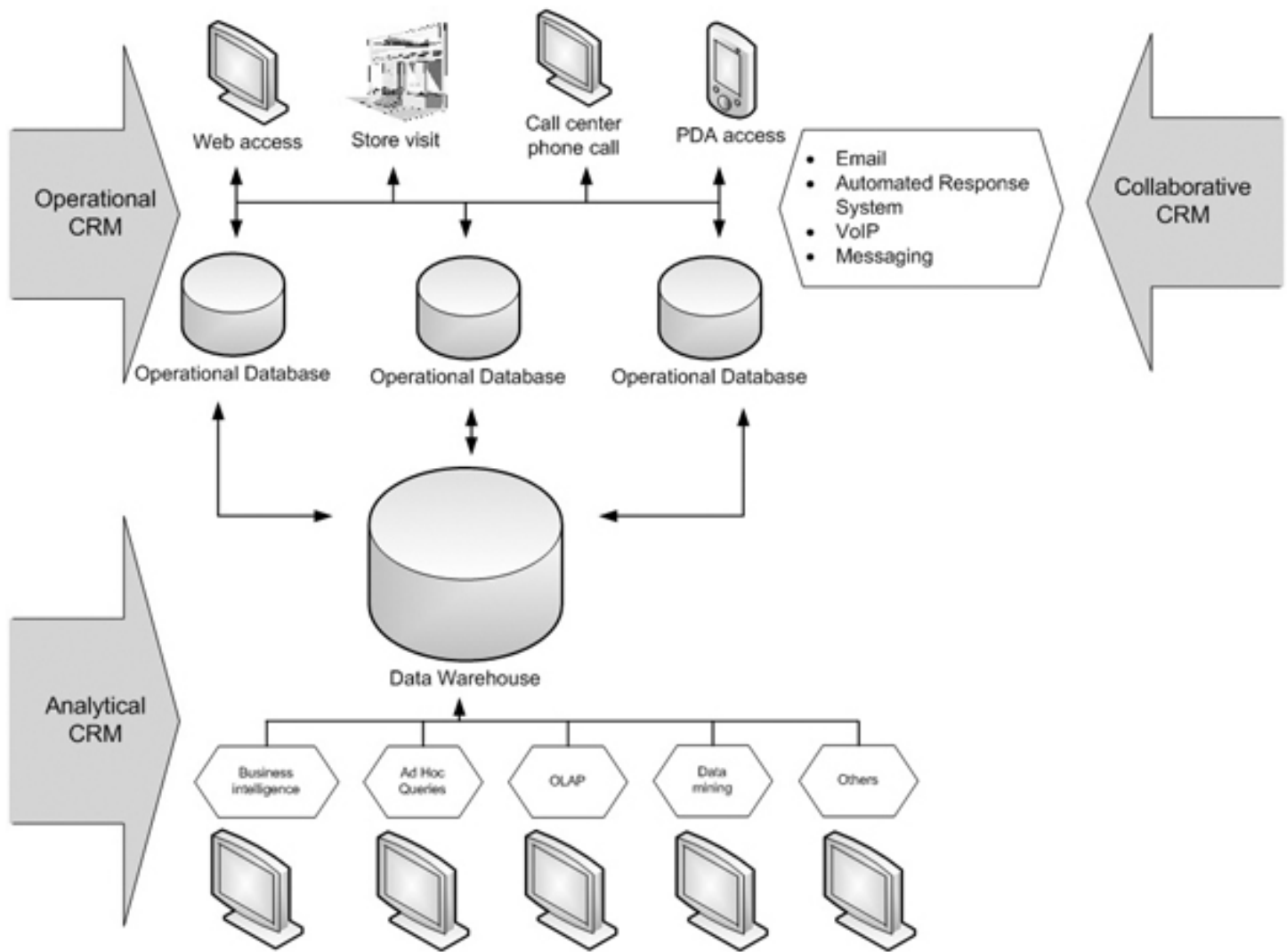


FIGURE 12.5 Sample CRM Architecture

The **operational components** of a CRM system help an organization improve day-to-day interactions with customers. They are involved with the operations of the company, such as sales or repairs.

The **collaborative components** of a CRM system help the organization interact and collaborate with its customers. They include older applications, such as email and automated response systems, but also newer ones, such as interactive chat facilities for customer service, **interactive voice response (IVR)** systems, and voice over IP (VoIP), which allows a customer to talk to a “live” customer service representative while online.

The **analytical components** of CRM consist of technologies and processes organizations can use to analyze customer data. A critical analytical component in most CRM systems is the data warehouse, which we discussed earlier. **Data mining** technologies and methods are often used to discover patterns and groups in the data stored in a data warehouse. Data mining involves using software that performs analyses of large data sets to find patterns that repeat themselves. For example, a grocery store might find that on college football weekends, certain items always seem to sell “together.” The grocery store can then locate them together within the store. This is a very simple example, and data mining can find much more complex and detailed patterns. One analysis that many organizations find useful is customer segmentation (sometimes called *customer clustering*), which allows organizations to group customers that share certain characteristics. For example, Student Advantage, a company that provides college student-oriented marketing services, uses segmentation to place its student members into very small segments. This allows Student Advantage to provide extremely targeted marketing opportunities to a wide variety of clients. Data mining can also help in customer profiling. **Customer profiling** lets companies build a picture of a customer through data collected from their interactions with this customer. These profiles allow companies to better anticipate customer needs and better predict customer behavior.

LEARNING ACTIVITY 12.4

Self-Servicing

We discussed CRM applications as a way companies can gather information about their customers and as a way to manage their communications with them. An additional function of CRM applications is to permit **customer self-service**, allowing customers to take care of their service problems themselves. Before we discuss the pros and cons of doing this, you should try self-servicing.

1. *Scenario:* You ordered new noise-free headphones for taking on your multiple trips. You bought them on Amazon.com for \$65. You opened the shipping package two months ago but never opened the actual package completely. (It has the original packaging.) You were busy with the start of classes, so you did not think about it again, but now your parents gave you the exact same item as a gift, so you want to return the package to Amazon.com.
2. Go to the Amazon website (<http://www.amazon.com>).
3. Figure out how much you are going to receive as a refund (not counting taxes, if any).
4. Estimate how long it is going to take for you to get your money once the headphones are shipped back to Amazon. Identify why this time is needed.
5. Figure out what you have to do to return the headphones.

Discussion Questions

1. How difficult was it to find the information needed?
2. How difficult do you think it would be to actually complete the return?
3. How likely are you to use this self-servicing application (Return Center) instead of calling someone at Amazon? Why?
4. What are the benefits to customers of self-servicing CRM applications?
5. What are the benefits to companies of self-servicing CRM applications?

STATS BOX 12.3: CRM VENDORS

The CRM market has been growing, with revenues of \$18 billion in 2012 and \$20.4 billion in 2013. Research suggests that for 2013, the top vendors were [Salesforce.com](http://www.salesforce.com) with 16% of the CRM market, SAP with a 13% share, and Oracle with 10% of the market.

Source: <http://www.forbes.com/sites/louiscolombus/2014/05/06/gartners-crm-market-share-update-shows-41-of-crm-systems-are-saas-based-with-salesforce-dominating-market-growth/>.

CRM Implementation Options

Like most other enterprise systems, there are two main ways that CRM can be implemented: on premise or on demand. **On-premise CRM** implementation means that the CRM system is acquired, leased, or developed by the organization and installed on its local servers. This often has the advantage of providing a customized solution. However, the costs of development and maintenance could be substantial. **On-demand CRM**, also known as **software-as-a-service (SaaS) CRM**, refers to the remote use of a CRM provider's applications through the Internet. This offers advantages like up-to-date applications and no maintenance or implementation costs. Of course, the company has to use the standard functions, also known as *plain vanilla* software.

BUSINESS EXAMPLE BOX 12.3

Not Just Technology: Training People for CRM at British Telecom

British Telecom (BT) is the largest telecommunication provider in the United Kingdom, holding approximately 45% of the UK broadband market. One of the most important business functions at BT is Business Sales, which is a division in charge of responding to customer inquiries and making sure customers use BT services. Every week, BT Business Sales handles 60,000 customer contacts. This typically generates US\$4.05 million (£2.75 million) in revenues per year.

To handle customer calls, BT has a CRM system that is available to its 540 call-handling advisors and 92 managers across the 9 sites used by BT Business Sales throughout the United Kingdom. However, over the years, BT management realized that there was a lack of consistency in how advisors serviced customers. For example, various advisors did not ask their customers some relevant questions (even though the CRM system requested this information), while others did not properly acknowledge or record replies from their customers. Not surprisingly, even when customers called to obtain information or service, advisors were trying to sell them something instead of helping the customers.

To improve customer relationships and the use of the CRM system, BT decided to develop a customer-oriented culture and a coaching philosophy through training of all call-center managers, first-line managers, and call-handling advisors. Part of the training was focused on improving the team culture in the call centers. The training effort did include new technology (to capture screens advisors used for training purposes), but it was also heavily focused on offering practical, skill-based behavioral training. The company recognized that new technology was not enough to create the change of culture that was required. The program included measurement of performance, in terms of both perceptions and actual performance.

BT achieved the expected results from the training program and the use of CRM. First, they created a culture among managers of coaching employees. Second, they now measure performance by receiving inputs from customers and others, not just measuring performance based on sales. (This is called *360-degree feedback*.) Third, they created an emphasis on ongoing relationships, which has led to stronger relationships between advisors and customers and between advisors and managers.

Source: Pollitt, D. 2010, November 4. "BT Business Sales Dials Up a Customer-focused Coaching Culture." *Human Resource Management International Digest* 18: 9.

Benefits and Limitations of CRM

There are many expected benefits from the use of CRM systems for organizations. First, CRM systems are expected to provide greater customer satisfaction because customers can receive personalized services and products, faster response time to their questions, and more streamlined interactions with the company. For companies, this results in improved customer relations, which should lead to repeat business (called *customer retention*). In addition, CRM systems can help an organization maximize its profits by reducing the costs for acquiring and servicing customers, and increasing overall revenues. Revenues can increase because of customer loyalty but also because of what is called *cross-selling*, or the selling of products to customers based on other products they acquired. For example, Amazon.com often sends its customers book recommendations based on books they have previously bought.

There are also some potential disadvantages to the use of CRM systems. First, the implementation of a CRM system requires more than simply installing the software application. In order to be successful in implementing a CRM system, an organization must look beyond purely technical issues and ensure that all customer-facing employees are customer minded. The company must also make sure that it identifies all channels of interactions with customers. The ability to achieve buy-in from various areas of the organization is key to a successful implementation. Of course, there are complicated technological issues that also must be addressed. First, the organization must ensure that its CRM architecture is scalable so that growth in customer demands is met without problems. Just like ERP systems, CRM systems can be customized to meet the specific needs of the organization. Overall, the ability to deal with both nontechnical and technical issues is a requirement for successfully implementing almost any enterprise system.

Customer-Managed Interactions (CMI)

One issue with CRM systems is that they are very firm centric in the sense that they focus on the existing transactional and behavioral data collected by the organization based on the prior and current interactions of the customer with the organization. While trends can be used to predict what customers might buy in the future, there are some acquisitions and customer activities that are unforeseeable unless the customer tells the company about it. For example, a customer might be interested in some products for a friend's upcoming wedding, but the company would not know of this need. To address this lack of information, some companies have turned their focus to customer-managed interactions (CMI).

Customer-managed interactions (CMI) involve letting customers store and manage data about themselves. Why would customers willingly tell companies of their buying intentions? For convenience, for money, or to obtain personalized service. Think of all your friends who create wish lists at some of the major online retailers like Amazon.com or [Target.com](https://www.target.com). There is even a site dedicated to helping anyone create wish lists ([WishList.com](https://www.wishlist.com)). Customers tell the company what they intend to buy; therefore, this information tends to be accurate. Once the company knows about intended purchases, it can perform targeted marketing, for example, by giving a specific discount, which may push the customer over into the buying phase of the customer service life cycle.

CHAPTER SUMMARY

In this chapter, we discussed enterprise systems. We first presented the main components, characteristics, and types of enterprise systems. We then explored in greater depth three enterprise systems: enterprise resource planning (ERP) systems, supply chain management (SCM) systems, and customer relationship management (CRM) systems. Here are the main points discussed in the chapter:

- Enterprise systems are information systems that serve the needs of the organization or parts of the organization.
- Enterprise systems are modular; they are integrated with one another (offering application integration) and use a central database (offering data integration).
- The purpose of enterprise resource planning (ERP) systems is to manage an organization's resources and enable information flow within and between processes (and departments) via a set of integrated information systems tools.
- Supply chain management (SCM) systems help organizations manage the flow of goods in their supplier and distribution channels to better control inventory, reduce costs, and improve communication with their business partners.
- CRM systems have three main components: the operational component that helps an organization improve day-to-day interactions with customers; the collaborative component that helps the organization interact and collaborate with its customers; and the analytical component, which consists of technologies and processes organizations can use to analyze customer data.
- The customer life cycle is a series of phases that customers pass through when interacting with an organization, and it can be used to identify important CRM applications.

REVIEW QUESTIONS

1. What is the difference between a personal and an enterprise information system?
2. How are applications developed using the functional perspective? The hierarchical perspective?
3. Define business integration and systems integration.
4. What is an enterprise resource planning (ERP) system, and how does it support systems integration?
5. What is the purpose of a supply chain management (SCM) system?

6. What is customer relationship management (CRM)?
7. What are the main components of a CRM system? Briefly describe each.
8. What are the main goals of a CRM system?
9. What is the difference between on-premise CRM systems and on-demand CRM systems?
10. What are customer-managed interactions? How do they differ from CRM?

REFLECTION QUESTIONS

1. What is the most important thing you learned in this chapter? Why is it important?
2. What topics are unclear? What about them is unclear?
3. How does the process perspective provide integration, and what types of integration are provided?
4. How does cloud computing relate to ERP and CRM applications?
5. How does the material in this chapter relate to the content of [Chapter 4](#) on strategic information systems?
6. Explain how data integration is essential to the success of ERP, SCM, and CRM systems.
7. Which issues are similar for both the process and the hierarchical perspectives of developing enterprise systems? Why?
8. How can process modeling ([Chapter 11](#)) enable firms to successfully implement enterprise systems?
9. We discussed different types of integration in this chapter (system, business, and data). How do they relate to one another?
10. Can a very small business implement a CRM system? What would be the advantages and disadvantages of doing so?

ADDITIONAL LEARNING ACTIVITIES

Learning Activity 12.A1

This activity requires you to complete a case analysis regarding an ERP acquisition. The case may be accessed through your university website, the Ivey Business School business case website (<https://www.iveycases.com>), or the Harvard Business School cases website (<https://cb.hbsp.harvard.edu/cbmp/pages/home>), or it may be provided to you by your instructor.

Canniff, M. 2007. "Case: Enterprise Resource Planning Software—Ongoing Maintenance Cost Benefit Analysis." *Ivey School of Business*, September 9. Product Number: 906E12-PDF-ENG.

Learning Activity 12.A2

Watch the following five-minute video:

- https://www.youtube.com/watch?v=xJfP_o_fANA

The video discusses CRM but is focused more extensively on the use of the data available from CRM systems and the marketing that can be done with these data. Prepare a short report describing the main points of the video. Be sure to address the following questions:

1. Who benefits from bigger and better data?

2. How does one obtain better quality CRM data?
3. How should strategy, process, and technology integrate to provide a better CRM system?
4. What is data migration, and how does it improve data quality?

Learning Activity 12.A3

Select a small organization you are familiar with. This could be your employer, a company where your parents or friends work, or just a company you know well. First, evaluate the company's need for a CRM system based on your knowledge from the readings, discussions, and activities you have done in this chapter. Prepare a short report including your recommended features, applications, and strategies for this small business.

Learning Activity 12.A4

After completing [Learning Activity 12.A3](#), watch the *Salesforce Marketing Cloud Overview* from [Salesforce.com](#) and include any changes to your report based on the information in the demo: <https://www.youtube.com/watch?v=x1wwxcoA82o>

Learning Activity 12.A5

Compare and contrast in a table the advantages and disadvantages of each enterprise system perspective (hierarchical, functional, and process).

Learning Activity 12.A6

Imagine that you are a new student at a university that requires each student to have a computer but does not provide guidelines beyond the fact that they have to be laptops, use wireless networks, and have the capability to use basic office applications and statistical analyses. The laptops have to be useful for three years. Develop a list of activities from the customer service life cycle that apply to this situation. Identify the CRM applications that can be used for each activity.

REFERENCES

- Gilmore, D. 2009. "The Top Supply Chain Disasters of All Time." *Supply Chain Digest*, May 7. <http://www.scdigest.com/assets/FirstThoughts/09-05-07.php?cid=2451&ctype=content>.
- META Group. 2001. "META Group Report: Five CRM Trends for 2001-'02." May 18. <http://www.cioupdate.com/reports/article.php/769091/META-Group-Report-Five-CRM-Trends-for-2001-02.htm>.
- Panorama Consulting Group. 2014. *2014 ERP REPORT*. <http://panorama-consulting.com/resource-center/2014-erp-report/>.
- Pearlson, K., and C. Saunders. 2010. *Managing and Using Information Systems*, 4th ed. Hoboken, NJ: Wiley.
- Piccoli, G. 2008. *Information Systems for Managers*. Hoboken, NJ: Wiley.
- SCDigest Editorial Staff. 2014. "Supply Chain News: The Factors Behind the UPS Failure to Deliver Christmas Goods." *SCDigest*, January 6. <http://www.scdigest.com/ontarget/14-01-06-2.php?cid=7717>

Van Slyke, C., and F. Bélanger. 2003. *Electronic Business Technologies*. New York: John Wiley & Sons.

FURTHER READINGS

Gulati, R., and J. N. Oldroyd. 2005. "The Quest for Customer Focus." *Harvard Business Review*, April. Product number: #9645.

Piccoli, G., and R. Watson. 2008, September. "Profit from Customer Data by Identifying Strategic Opportunities and Adopting the 'Born Digital' Approach." *MIS Quarterly Executive* 7(3): 113–22.

Reinhartz, W., and V. Kumar. 2002. "The Mismanagement of Customer Loyalty." *Harvard Business Review*, July. Product number: #R0207F.

SAP Information

- <http://www.sap.com/pc/bp/erp.html>
- <http://go.sap.com/solution.html>

Supply Chain Management Videos

- <http://go.sap.com/product/scm.html>
- <http://www.youtube.com/watch?v=dDmGtPQAI24> (MS Dynamics)

CRM Videos

- http://www.youtube.com/watch?v=-_6c018ZI2g

Social CRM Article

- http://www.pcworld.com/article/200897/How_Savvy_Firms_Monitor_Customers_Online_Chatter.html

GLOSSARY

Analytical components of CRM: Technologies and processes organizations can use to analyze customer data.

Application integration: Applications where modules are designed to be integrated with one another.

Business integration: The unification of business processes previously performed as separate activities in order to create cohesive and streamlined business processes.

Business intelligence (BI): A set of applications, technologies, and processes for gathering, storing, analyzing, and accessing data to help users make better business decisions.

Business process reengineering (BPR): The redesign of business processes to improve how work is done.

Call center automation: Applications that support call centers, which are often the main contact point between an organization and its customers.

Campaign management: Applications that help organizations plan, carry out, and analyze the results of marketing campaigns.

Collaborative components of CRM: Technologies and processes that help organizations interact and collaborate with their customers.

Content management systems (CMSs): Applications that allow companies to manage the vast amounts of information of various types (content) they have stored. This includes the capture, storing, preservation, and delivery of content.

Customer issues management: Applications that help organizations with tasks such as scheduling, dispatching, and communicating with field service personnel.

Customer-managed interactions (CMI): Applications that let customers store and manage data about themselves.

Customer profiling: Applications that help organizations group customers according to demographic characteristics or behaviors.

Customer relationship management (CRM): An organization-wide strategy for managing an organization's multiple interactions with customers.

Customer self-service: Software that allows customers to find solutions to problems without interacting with a customer service representative.

Customer service life cycle (CSLC): A series of phases that customers pass through when interacting with an organization.

Data integration: Applications where data are stored in one central database.

Data mining: The process of analyzing data to identify trends, patterns, and other useful information to make predictions.

Enterprise application integration (EAI): A set of tools and services (a framework instead of a single technology) to allow various enterprise systems (such as ERP or CRM) to share data.

Enterprise resource planning (ERP): Software that allows organizations to manage resources throughout the organization, independently of which business function controls the resource.

Enterprise systems: Information systems that serve the needs of the organization or parts of the organization.

Functional perspective: Software development approach where information systems applications are developed to meet the needs of individuals in a functional area, such as human resources or marketing.

Hierarchical perspective: Software development approach where software developers build information systems to mirror the organization so that applications are built to meet the needs of individuals at a given level in the organization.

Interactive voice response (IVR): Applications that allow customers to use a telephone to navigate through various types of systems, such as product request systems or customer service systems.

Lead processing: Applications used to qualify, assign, and track sales leads to maximize the probability that the leads eventually turn into sales.

On-demand CRM: Remote use of a CRM provider's applications through the Internet.

On-premise CRM: CRM specifically developed for the organization and installed on its local servers.

Operational components of CRM: Technologies and processes that help improve day-to-day interactions with customers, such as sales, repairs, and so on.

Order tracking: Applications that allow customers to determine the status of their order.

Personal information systems: Information systems applications for individual use.

Process perspective: Software development approach where information systems applications are developed to support the task being done (or process) irrespective of the organizational level or functional area the individual using the system.

Product configuration: Applications used to properly configure or choose complex products.

Radio-frequency identification (RFID) tags: Electronic tags that can be tracked remotely using wireless networks.

Sales force automation: Applications that provide functions directed at making sales representatives more efficient and effective.

Software-as-a-service (SaaS) CRM: Remote use of a CRM provider's applications through the Internet.

Supply chain: Entities involved in the flow of goods from the manufacturer to the wholesaler to the retailer and to the consumer.

Supply chain management (SCM) systems: Software that helps organizations manage the movement of materials or products from provision to production to consumption.

Systems integration: The unification of information systems and databases that previously operated as separate systems.

Unified communications (UC): A framework for the integration of the various modes of communication used by an organization, including email, voice mail, videoconferencing, instant messaging, texting, and voice over IP.

CHAPTER 13

INFORMATION FOR ELECTRONIC BUSINESS

LEARNING OBJECTIVES

By reading and completing the activities in this chapter, you will be able to

- Describe the concept of e-business and various e-business models
- Identify the business-to-consumer (B2C) e-business models, enablers, and impacts
- Explain search engine optimization
- Discuss the main business-to-business (B2B) e-business models
- Identify the major trends related to e-business

CHAPTER OUTLINE

- [Focusing Story: The iPod and the Music Industry](#)
- [Learning Activity 13.1: Why Is E-Business Important?](#)
- [Introduction to E-Business](#)
- [E-Business Models](#)
- [B2C E-Business Enablers](#)
- [B2C E-Business Impacts](#)
- [Learning Activity 13.2: Why Would I Trust Them or Buy from Them?](#)
- [Design for B2C E-Business](#)
- [Business-to-Business \(B2B\)](#)
- [Learning Activity 13.3: B2C versus B2B](#)
- [Learning Activity 13.4: Where Is My Web Page?](#)
- [Search Engine Optimization](#)
- [Trends in E-Business](#)
- [Learning Activity 13.5: Usa.gov](#)
- [Chapter Summary](#)
- [Review Questions](#)
- [Reflection Questions](#)
- [Additional Learning Activities](#)
- [References](#)
- [Further Readings](#)
- [Glossary](#)

The growth of the Internet has changed our everyday lives, just as it has changed how businesses and governments interact and conduct transactions with consumers. These digital interactions have led to the phenomenon of e-

business, also known as digital markets. In this chapter, we explore various ways that organizations and individuals interact online and the implications that that digital interactions have for us all, as you will see in the focusing story on digital music.

FOCUSING STORY

The iPod and the Music Industry

Who would have thought that a small device like an iPod could dramatically change a well-established major industry? Yet that is what happened when Apple Inc. launched the iPod and electronic music downloads. Because of this new way of selling songs and albums, the music industry has been one of the most affected by e-business.

In the “old” music industry, artists recorded songs and albums through record companies, which were the major players in the industry. Companies could sell CDs (and before the 1980s, LPs) and make significant profits on each album customers bought, with some fees (rights) going to the artists and some commissions going to distributors and retailers. Eventually, the record companies decided not to release singles, only albums. That was not to the liking of music listeners. Then came the iPod, announced on October 23, 2001. It allowed users to download only the songs they wanted to a very portable device. The industry was never the same. The music industry faced two significant problems with the growing use of the Internet for access to digital music. The first is that digital music is easy to steal, and users started to download music illegally and share it with one another. In this scenario, everyone in the industry lost money. Even though illegal downloads had started years before, with Napster allowing illegal downloads for free between 1999 and 2001, the iPod made it easy to copy songs. At the same time, however, many users are happy to spend small amounts of money for legal downloads of the songs they really want. That is why Apple is said to have sold more than six billion songs on iTunes by the end of 2009.

A second phenomenon that occurred with the ability to download songs through the Internet was that some artists decided to sell their own music online. They were able to charge less to consumers because they only had to pay the e-business website for selling their music; they also made more profits this way. Apple keeps 30% of the profits from each song sold, with the rest going to the artist. So on a song that sells for \$1.29, Apple receives about \$0.39, and the label and artist receive about \$0.90. When artists produce their own music, they get the full \$0.90 that normally goes to the artist and label. Record companies changed their licensing approaches to embrace new online services in response to this major threat to the industry. However, they did not envision online streaming: the new online threat to the music industry. Online music streaming services allow listeners to play music on their computers or Internet-enabled devices instead of buying CDs or downloading music to their MP3 players (one of which is the iPod). These services, like Pandora (<http://www.pandora.com>), Last.fm (<http://www.last.fm>), or Spotify (<http://www.spotify.com>), are free or relatively inexpensive. As users listen online instead of purchasing music, sales of music keep going down every year. The total music industry sales in 2000 were approximately US\$14 billion but were down to US\$10 billion by 2008. In 2014, revenue from streaming sources of music outpaced the revenue from CDs for the first time.

FOCUSING QUESTIONS

1. Will the streaming audio approach change the music industry once more? How?
2. How can the streaming audio business model be successful?
3. What other ways could companies use to leverage digital music?

Sources: Woollaston, V. 2013. “15,000 Songs a MINUTE Downloaded on iTunes as Apple’s Music Service Celebrates Its Tenth Birthday.” *Daily Mail*, April 29. <http://www.dailymail.co.uk/sciencetech/article-2316473/A-decade-iTunes-How-Apple-revolutionised-way-buy-music.html>; MacMillan, D. 2009. “The Music Industry’s New Internet Problem.” *Bloomberg BusinessWeek*, March 6. <http://www.bloomberg.com/bw/stories/2009-03-06/the-music-industrys-new-internet-problembusinessweek-business-news-stock-market-and-financial-advice>;

Mansfield, B. 2015. “Streaming Revenue Passes CDs for First Time.” *USA Today*, March 19. <http://www.usatoday.com/story/life/music/2015/03/19/streaming-revenue-passes-cds-riaa-report/25023773/>.

LEARNING ACTIVITY 13.1

Why Is E-Business Important?

Most of you have already experienced electronic business, the topic of this chapter, when acquiring products electronically. E-business, however, is much broader than just buying something online. In this learning activity, we want you to think broadly about what e-business is and find two interesting, up-to-date statistics online about the size of electronic business. These can be for a subset (such as B2C or B2B), an industry, or a market segment. Make sure your statistics are current—say, within the last two years. Be careful about some of the older information available online. For example, you may find predictions from five years ago about expected e-business sales. It is much better to find out what current e-business sales are. Prepare a short report of your two statistics (make sure to include your citations!) and a brief discussion of why you think e-business is important today.

Introduction to E-Business

In [Learning Activity 13.1](#), you found several statistics about e-business. What you found should have already convinced you of the importance of e-business in today’s economy. However, the importance of e-business goes beyond any number you could find online. The reality is that e-business changed how most organizations interact with their customers and suppliers and even how they interact with the government. More important, complete industries have been transformed with the emergence of e-business applications. This is the case in the focusing story, which showed how e-business completely changed the music industry. What other industries have been changed by e-business? You may think of travel, publishing, and even education, just to name a few. Later in this chapter, we discuss specific impacts e-business has had on these industries.

What is e-business exactly? There are many definitions, but another way to look at it is as a digital market. [Table 13.1](#) provides some terminology used when discussing e-business and digital markets. Note that electronic funds transfer (EFT) and electronic data interchange (EDI) provide tools for transferring documents or financial data between organizations, and we discussed them in [Chapter 7](#). The other terms include variations on whether only the Web, other Internet tools, or any other electronic means are used for business transactions, such as collaboration software, kiosk technologies, and so on. For our purposes, we will use the term *e-business*, which is often recognized as the broader term that includes various electronic means of conducting business, as shown in [Figure 13.1](#).

TABLE 13.1 E-Business Terminology

Electronic funds transfer	Electronic means to conduct financial transactions such as payments and remittances
Electronic data interchange	Electronic means to transfer documents between organizations
Web commerce	Electronic means to conduct business transactions using the Web as an interface
Internet commerce	Electronic means to conduct business using the Internet (for example, email, the Web, or file transfer)
Electronic commerce	Electronic means to conduct business transactions, including the Internet, electronic data interchange
Electronic government	Electronic means to interact or conduct transactions with government agencies
Electronic business	Electronic means to interact or conduct business with individuals, companies, or government agencies

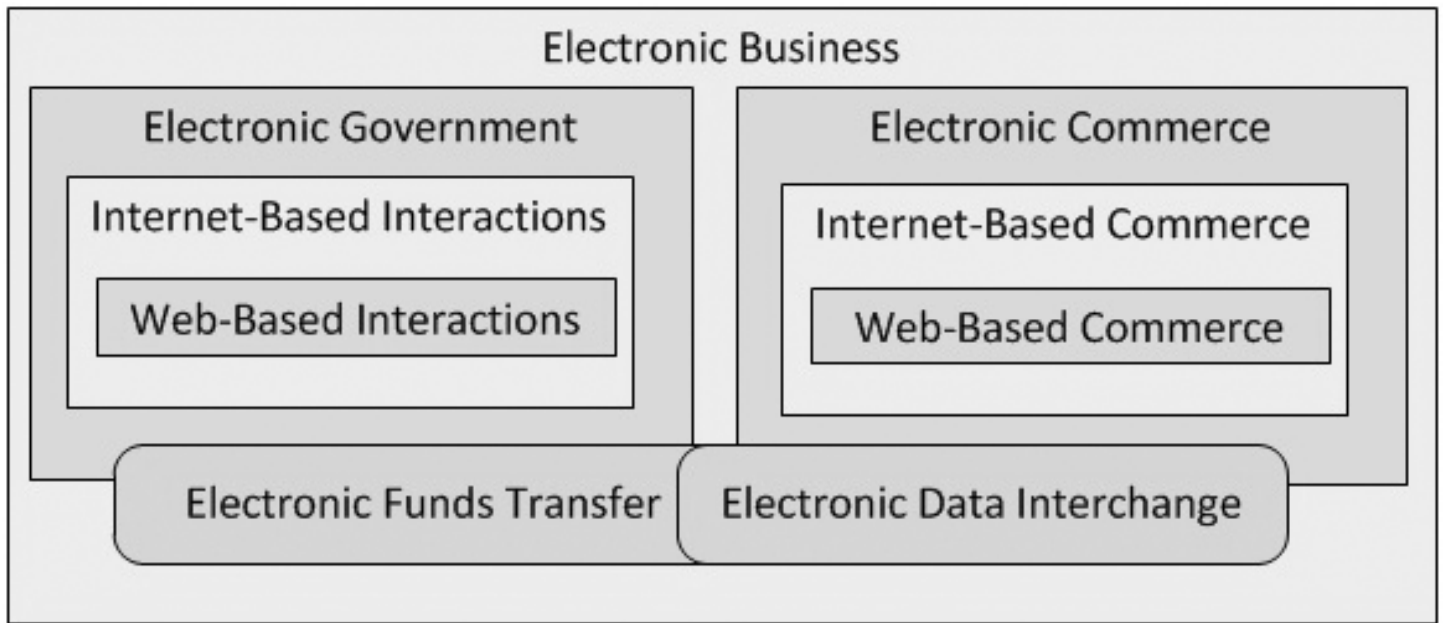


FIGURE 13.1 E-Business Terminology

Types of E-Businesses

In [Table 13.1](#) and [Figure 13.1](#), we differentiate between commerce and government. There are other ways to categorize the various types of e-business. Some of the most common categorizations are as follows:

- **Business-to-consumer (B2C):** This is when interactions are taking place between a consumer and a business. For example, when you buy books on Amazon.com, you are conducting a B2C e-commerce transaction.
- **Business-to-business (B2B):** This is when interactions are taking place between two businesses. For example, when Wal-Mart sends electronic requests for inventory to its suppliers, it is conducting a B2B e-commerce transaction.
- **Consumer-to-consumer (C2C):** This is when interactions are taking place between two consumers. For example, when you buy goods from another individual on [eBay.com](#), you are conducting a C2C e-commerce transaction.
- **Government-to-constituent (G2C):** This is when interactions are taking place between a government agency and a constituent. Constituents could be citizens, businesses, or even other agencies. For example, when you pay your taxes online, you are having a G2C interaction with the government. This is most often referred to today as *electronic government*, or *e-government*.

There are many more types of e-business, although they tend to be variations of the definitions in [Table 13.2](#); for example, consumer-to-business (C2B), business-to-employee (B2E), or government-to-government (G2G). The main ones outlined above, however, seem to be the most popular categories.

TABLE 13.2 Types of E-Businesses

E-Business Type	Acronym	Definitions
Business-to-consumer	B2C	When interactions are taking place between a consumer and a business
Business-to-business	B2B	When interactions are taking place between two businesses
Consumer-to-consumer	C2C	When interactions are taking place between two consumers
Government-to-constituent (e-government)	G2C	When interactions are taking place between a government agency and a cons

There is another way to categorize commercial electronic business, and it refers to the online versus offline structure of the organization. There are three main categories used:

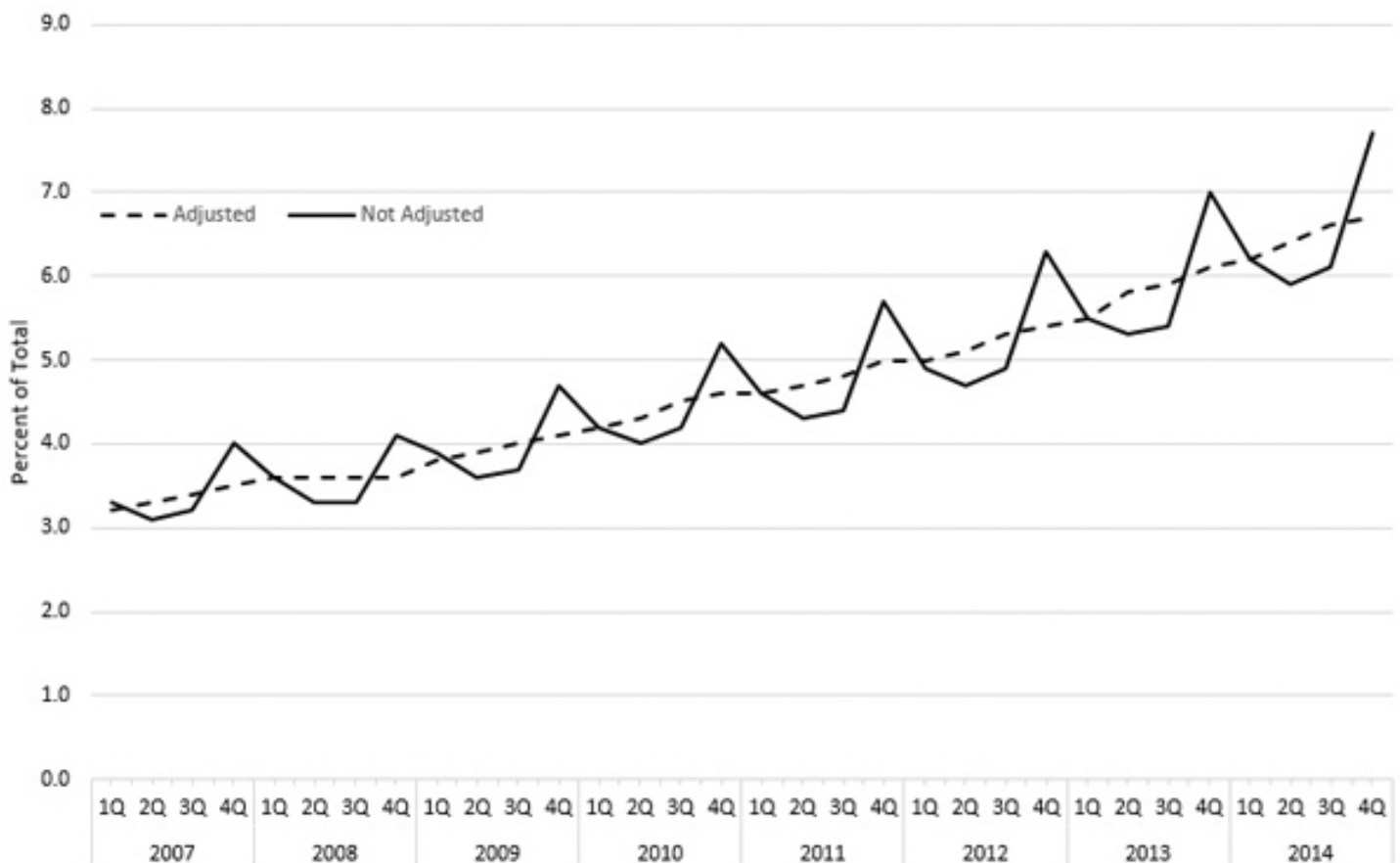
STATS BOX 13.1: RETAIL E-COMMERCE IN THE UNITED STATES

As you might have found in [Learning Activity 13.1](#), there are many statistics on e-business that are often not consistent with one another. One good source of statistics for the United States is the U.S. Census Bureau, which provides quarterly statistics on retail e-commerce. The following table shows the statistics available at the end of 2014. You can obtain the most recent statistics at the following site: <http://www.census.gov/retail/#ecommerce/>. Note that although the numbers are impressive, e-commerce still represents less than 8% of all retail sales in the country, as can be seen in the following figure.

Estimated Quarterly Total and E-Commerce U.S. Retail Sales, 2013–14

Quarter	Retail Sales Total (Millions)	Retail Sales E-commerce (Millions)	E-Commerce as a Percent of Total
4th quarter 2014	1,187,169	79,567	6.7%
3rd quarter 2014	1,185,773	77,789	6.6%
2nd quarter 2014	1,174,741	75,080	6.4%
1st quarter 2014	1,149,198	71,503	6.2%
4th quarter 2013	1,145,128	69,426	6.0%

Estimated Quarterly U.S. Retail E-Commerce Sales as a Percent of Total Quarterly Retail Sales: 1st Quarter 2007–4th Quarter 2014



Source: U.S. Census Bureau, <http://www.census.gov/retail/#ecommerce>.

- **Bricks and mortar:** This category represents traditional organizations with physical locations. For example, large automobile manufacturers tend to have physical offices and operations.
- **Bricks and clicks:** This category represents traditional organizations with physical locations but that also operate an online business. There are many such companies today that have physical stores and online stores; for example, Wal-Mart has Walmart.com, BestBuy has BestBuy.com, and so on.
- **Pure play (or click only):** This category represents organizations with only an online business. For example, Amazon.com and eBay.com started as online companies only, where you could not go to a physical store to conduct a transaction. Many pure play companies, like Google, exist in the online world only, although they still have offices for people to work at.

E-Business Models

The various types of e-business previously discussed refer to who participates in the e-business interaction and whether this organization uses offline, online, or both business environments. Another important way to classify e-businesses is with respect to their business model.

What Is a Business Model?

A **business model** represents the way the organization functions and creates value. In other words, it is how an organization makes money. The business model often identifies the market that a business is in, the products or services that it offers, and the strategies and major activities it uses to seek competitive advantages in that market. Importantly, the business model should identify the organization's key business processes and organizational capabilities that allow the business to generate revenues and profits.

B2C E-Business Models

There are many different business models in the world of e-business, some more popular than others, and many that did not really exist before the increased use of the Internet for business. [Table 13.3](#) shows a variety of B2C e-business models.

TABLE 13.3 B2C E-Business Models

E-Business Model	Description	Important Facts
Online retailing	Offers products or services for sale to consumers online. Some businesses acquire the products for resale, while others act as electronic intermediaries for selling products.	The ability to distribute products efficiently and effectively (fulfillment and logistics functions) is critical to success in this business model.
Infomediary	Offers specialized information to consumers via the Internet that aggregates or analyzes products or services from several providers. The term comes from information intermediaries .	These companies do not sell products or services directly, and they do not have any inventory. The ability to maintain up-to-date information is crucial in this business model.
Content providers	Offers consumers content or relevant information and receives money from vendors for ads or downloads or from consumers for subscriptions.	Content can be generated and published by the organization, or it can be user-generated content that the business publishes.

			• <i>Histori</i> <i>refere</i> • <i>Travel</i>
Exchanges	Offers a location (marketplace) for buyers and sellers to transact online. Revenues come from fees for sellers or buyers or commission on sales.	Generating a large number of buyers and sellers (a critical mass) is crucial for success in this business model.	• eBay.co • uBid.co
Online community or social media	Offers individuals with similar interests and/or goals an online meeting place to interact with one another. Many start as not-for-profit but end up charging for select services or information or allow ads to be posted on the community.	Online communities are virtual in the sense that the meeting place is online only.	• Facebook • Delphi
E-business infrastructure provider	Offers infrastructure hardware, software, or services to other organizations for e-business. Revenues come from fees paid for the services.	Online businesses can use these infrastructures through cloud computing (Chapter 7) or directly through the provider. This has substantially reduced the cost of starting online businesses.	• <i>Online</i> • <i>Credit</i> <i>servic</i> • <i>Web an</i> <i>servic</i> • <i>Domain</i> <i>and d</i> <i>hostin</i>

The e-business models presented in [Table 13.3](#) continue to evolve as individuals find new ways to use the Internet, and increasingly mobile technologies, to create new approaches to generate revenue. In fact, the use of location-based services on mobile devices (knowing where you are based on your cell phone's location) allows marketing firms to offer targeted advertising and services that you may need at a specific moment based on where you are. Some of the business models would not exist without the Internet, like infrastructure companies such as [PayPal.com](#) or [Squareup.com](#) or social media websites like [Facebook.com](#) or [Delphiforums.com](#). There are even some fairly unique business models in existence today, like the name-your-own-price model of [Priceline.com](#) (<http://www.priceline.com>).

It is necessary for business models to evolve with today's rapid changes in technology and the changes in the way individuals interact with one another. For example, as many students know, changes in your online profile on a social networking site result in changes in the types of ads you see when accessing the site. This change in the social media business model has occurred in the last few years. However, while keeping up with technological and social changes is important, the most important factor for success is to start with a proper business model. Back in the early days of e-business, many entrepreneurs jumped on the bandwagon of e-business without proper business models. Not surprisingly, many of them failed. This is one reason behind what is today called the *dot-com bust*, when many individuals and companies lost money in their attempts to take advantage of e-business. Today, there are too many e-business successes to even attempt to summarize them. Some are very innovative, while others simply follow solid business models.

BUSINESS EXAMPLE BOX 13.1

Adapting Its Business Model: Amazon.com

When the dot-com bust happened in the early 2000s, many e-businesses simply went out of business, unable to generate sufficient revenues to cover their costs. Others, however, were able to survive and thrive. One such company is Amazon.com. However, Amazon.com, which for most of its life span has existed only as a website, is now adapting to maintain its competitive advantage in the retail sector.

In 2015, Amazon.com opened its first retail store location on the campus of Purdue University. Students can place any orders that they want at the store but receive one-day shipping if they have it delivered to Amazon.com's on-campus location. Amazon.com plans to create more retail stores on other campuses in the future.

Amazon is also in the process of testing and obtaining permission to utilize drones, or pilotless aircraft, to deliver packages. Doing so would allow Amazon.com to deliver products without requiring a human delivery driver to bring products to the customer's location.

Sources: "Amazon Opens Its First Store." 2015. *CNN Money*, February 4. <http://money.cnn.com/2015/02/04/technology/amazon-purdue/>; Lapowsky, I. 2015. "Amazon Can Now Test Its Delivery Drones in the U.S." *Wired*, April 10. <http://www.wired.com/2015/04/amazon-drone-faa-green-light/>.

B2C E-Business Enablers

The statistics previously presented and those that you found in [Learning Activity 13.1](#) clearly show that B2C e-business continues to increase in value worldwide. What has made this growth possible? A combination of technological and social factors can help explain why B2C e-business has grown so much over the years.

Technological Enablers

There are several technological requirements that must be met for consumers to successfully acquire goods or services online. First, there must be an easy-to-navigate website. The graphical user interfaces of today's browsers and the search tools available on websites are examples of technological improvements that have enabled e-business to grow. In addition, e-business requires that consumers have sufficient network bandwidth to access e-businesses' websites. Think of how much time it takes sometimes to download images for goods you want to purchase. If it takes too long, you might end up going to a different site. The bandwidth required depends on the images and other features of the site, and the overall bandwidth is a function of the vendor's network bandwidth (and server processing capability) and the consumer's Internet access bandwidth. In recent years, the use of broadband networks for Internet access (see [Chapter 7](#)) has significantly improved the overall bandwidth availability and therefore the online shopping experience of consumers.

A less visible but just as critical technological requirement is interoperability. We discussed **interoperability** in [Chapter 7](#), where we defined it as the ability of heterogeneous systems to communicate with one another. Interoperability is key to e-business success because, by definition, e-business allows individuals using a wide variety of platforms (PCs, Macs, laptops, tablets, smartphones, etc.) to access businesses that also use a wide variety of platforms (with different operating systems, databases, Web servers, etc.).

Critical Mass

Beyond technological factors, one key social factor that has had a huge impact on the growth of e-business is the attainment of a critical mass of users. The impact of critical mass is best understood under the concept of network effects, which we define further below. In e-business, attaining **critical mass** means that there are sufficient buyers to sustain the business of vendors and sufficient vendors to attract buyers to the Internet.

Network effects or network economics can be used to discuss how value is created in a network. Recall from [Chapter 4](#) that a firm can get competitive advantages when it owns a resource that is rare or unique. This is considered *value in scarcity*. In networks, however, there is also something completely opposite, which is *value in plentitude*. In a network (think of a group of people), the value of the network increases every time a new member is added to the network. Let us take the example of email. If only two of you use email, it makes one possible link. Eventually, you might find it limiting to only be able to send email to this one other person. Now if you add a third person to your group, you each have two potential people to send email to (or the existence of three links in the network). The addition of the third person adds value to your network. Now consider the networks in [Figure 13.2](#). How many links are possible now?

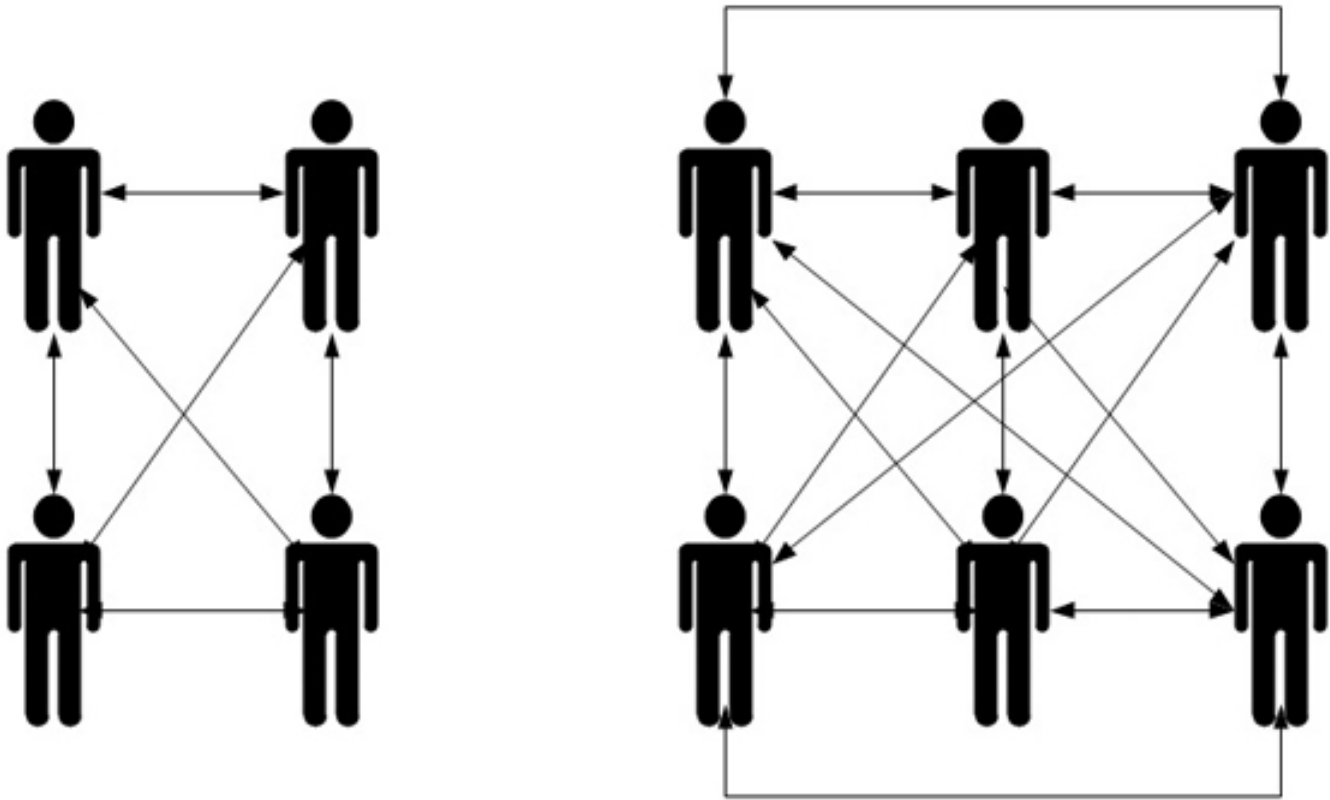


FIGURE 13.2 Networks of People

Extend this concept to e-business, and you realize that the more vendors there are on the Internet, the more interesting it is for you to shop online. For vendors, the same is true: the more consumers there are shopping online, the more interesting it is to use the Internet to sell their goods or services. Today, as we saw in previous chapters, there are close to one billion hosts (servers) on the Internet and more than 30% of the world population has Internet access. We could say that the Internet and the Web have reached critical mass.

B2C E-Business Impacts

We discussed early in the chapter how e-business has changed industries. For some, these changes have been extremely positive (lower costs), while for others, the changes may be perceived as very negative (loss of profits or even disappearance of some businesses). There are two specific terms used to refer to two impacts of e-business: channel compression and channel expansion.

Channel Compression (Disintermediation)

Channel compression is an impact on the downstream portion of the supply chain. Recall from [Chapter 12](#) that the supply chain consists of several distributors and retailers upstream and downstream of the focal firm. In the distribution channel, the distributors and retailers are called *intermediaries*. **Channel compression** refers to situations when the distribution chain is shortened by eliminating some or all of these intermediaries between the focal firm (product producer) and the end consumer. For this reason, channel compression is also called *disintermediation*. As previously discussed, this change in the distribution structure has led to some major restructuring in several industries, including the music, publishing, and travel industries. When organizations have to decide whether or not to eliminate members of their distribution channel, they are often faced with channel conflict, or when to eliminate distributors and when to work with them. For example, if the Dell company decides to offer products through Dell retailers but also to sell directly online, how can it price products so that its resellers can make a profit but its consumers still feel they are getting the best prices when they buy directly online?

Channel Expansion

While channel compression has resulted in fewer organizations involved in the supply chain for some industries, channel expansion offers the reverse impact. **Channel expansion** is the addition of intermediaries in an industry whose purpose is to aggregate and provide information or brokering functionalities. In other words, intermediaries facilitate bringing buyers and sellers together or bringing relevant information to buyers and sellers. Think of the role of kayak.com. It does not offer its own flights but pulls information from different vendors (airlines) as well as other search engines (like Expedia.com or Priceline.com). These intermediaries can make money by receiving fees from vendors or by allowing ads on their sites. The larger the volume of users, the better they can sell ad placement (selling ads on their websites based on number of viewers). An overall important effect of these intermediaries is to reduce search costs and the information asymmetries that existed before the Internet and e-business. A good example is provided by real estate e-brokers. [Figure 13.3](#) shows the most visited real estate websites in December 2014. How many of these companies existed before e-business?

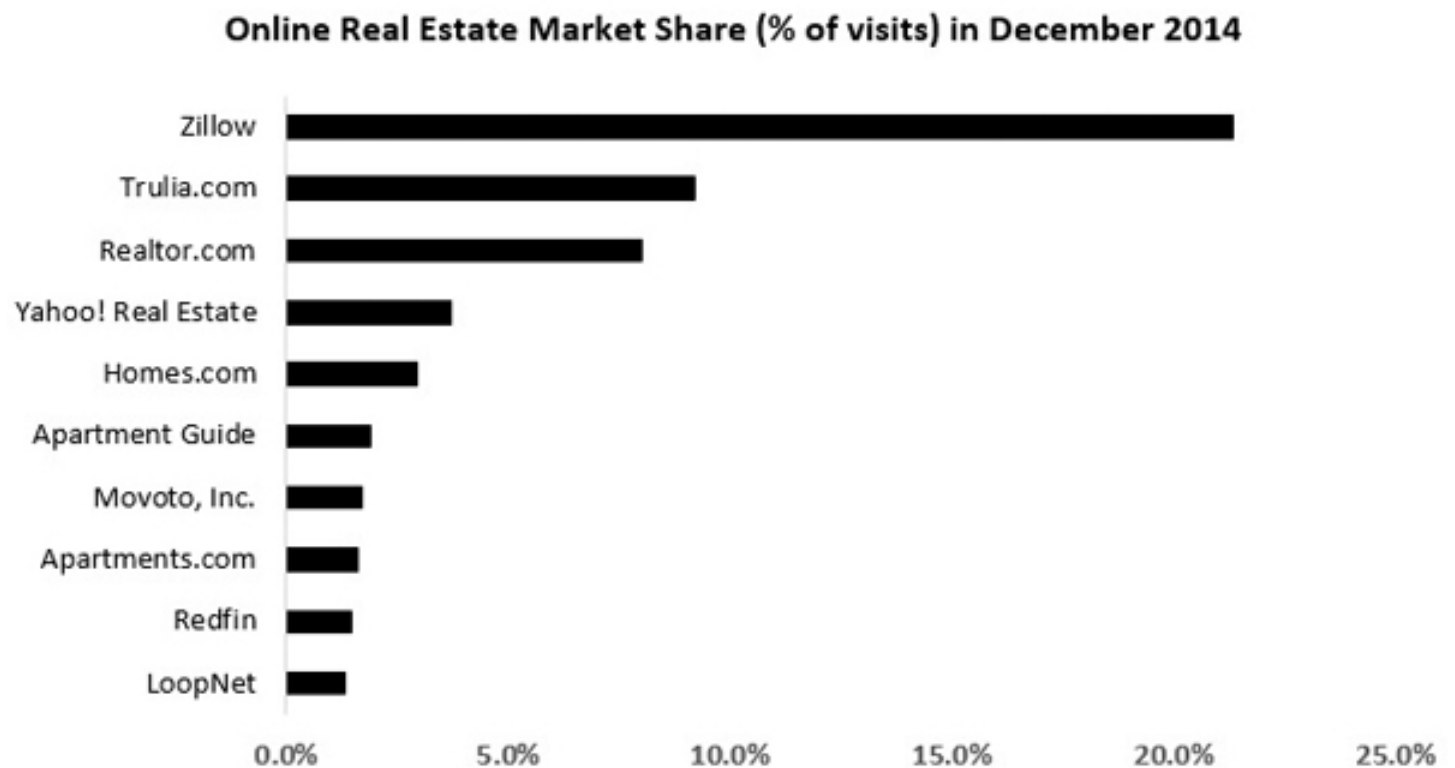


FIGURE 13.3 Top Real Estate Websites, December 2014

Source: Based on data from Experian Hitwise, available at <http://www.experian.com/marketing-services/consumer-insights.html> and <http://www.marketingcharts.com/updates/top-10-multi-platform-real-estate-websites-december-2014-50468/>.

LEARNING ACTIVITY 13.2

Why Would I Trust Them or Buy from Them?

In this activity, visit two retail websites and identify the factors that would make you more willing to trust the Web merchant and to buy and/or share information with the website. Select *two* of the following Web merchants:

- Dell: <http://www.dell.com>
- Amazon: <http://www.amazon.com>
- BestBuy: <http://www.bestbuy.com>
- Sierra: <http://www.sierratradingpost.com>
- Road Runner: <http://www.roadrunnersports.com>
- Murad: <http://www.murad.com>

Create a table, as shown below, to list the specific features that would make you trust, buy, or share information:

	Trust	Intentions to Buy	Willingness to Share Inform
Site A	Feature 1	Feature 1	Feature 1
	Feature 2	Feature 2	Feature 2
	(etc.)	(etc.)	(etc.)
Site B	Feature 1	Feature 1	Feature 1
	Feature 2	Feature 2	Feature 2
	(etc.)	(etc.)	(etc.)

Design for B2C E-Business

There are many important design features that can make e-business websites more or less successful. In [Learning Activity 13.2](#), you identified several of them. For example, most of you will have identified the security of the website as a requirement for trusting the Web merchant and its privacy practices as a requirement for being willing to share information with the website. In [Chapters 8](#) and [9](#), we discussed various features that increase (or reassure customers about) the security and privacy of information systems. In fact, many researchers have identified trust as one key determinant of individuals' intentions to buy from online merchants. Ease of use of the system in terms of navigating, checking out, and accessing information are usually important design features as well. The overall look of the website is also a factor in online buying decisions. Sites that are overloaded with information can be distracting for some users, while sites that have features and graphics that are too simplistic may look unprofessional. There are also nontechnological features for website success, such as return policies, shipping policies, and communication tools. Research also suggests that websites that offer customer reviews see increased site traffic and overall conversion rate (<http://www.eMarketer.com>). The conversion rate is the rate at which consumers who are browsing the website end up buying from the website. Other features that are found to annoy customers on websites include pop-up ads, the need for extra software to view a site, dead links, confusing navigation, the need to log in to view content, slow-loading pages, and out-of-date content, to name a few ([eMarketer.com](http://www.eMarketer.com) 2015).

Business-to-Business (B2B)

Most of this chapter so far has discussed B2C e-business, mainly because you are more familiar with this type of e-business but also because many of the basic principles also apply to B2B e-business. However, there is a significant difference between B2C and B2B e-business beyond the type of players involved, and that is the size of the market involved. B2B e-business represents a significantly larger market than B2C.

LEARNING ACTIVITY 13.3

B2C versus B2B

Every year, the U.S. Census Bureau collects data on e-commerce. Their studies reveal that the amount of money spent on e-commerce grows each year. For this learning activity, visit the following website and collect the amount of e-commerce sales over the last three years. While you are doing this, differentiate how many sales occur through B2C and B2B channels. Compare these numbers and write a short response as to what they tell you about these two markets:

<http://www.census.gov/econ/estats/index.html>

There are several other differences between B2B and B2C. Of course, B2B involves two or more organizations as opposed to individual consumers. In B2B, these organizations typically know their trading partners fairly well, and as a result, B2B is often relationship based, except for marketplaces that we will describe later.

B2B E-Business Models

B2B involves the sharing of electronic documents, funds, and/or information between organizations. There are many ways to implement this. First, B2B e-business includes supply chain management, which we discussed in [Chapter 12](#). In fact, when organizations share knowledge electronically across the supply chain to facilitate inventory control, reduce time delays in billing, and improve customer handling, they are conducting B2B e-business. Two other models of B2B e-business need further explanation: electronic data interchange and e-marketplaces.

Electronic data interchange (EDI) is the electronic exchange of information between two or more organizations using a standard format. The types of information exchanged are defined within the standards that are used and usually include business documents like bills, purchase orders, payment slips, invoices, and so on. EDI has been in existence for a very long time, allowing trading partners to lower transaction costs and improve profits through faster billing cycles, reduced errors, and improved customer responsiveness. [Figure 13.4](#) shows a simplified sample set of EDI transactions.

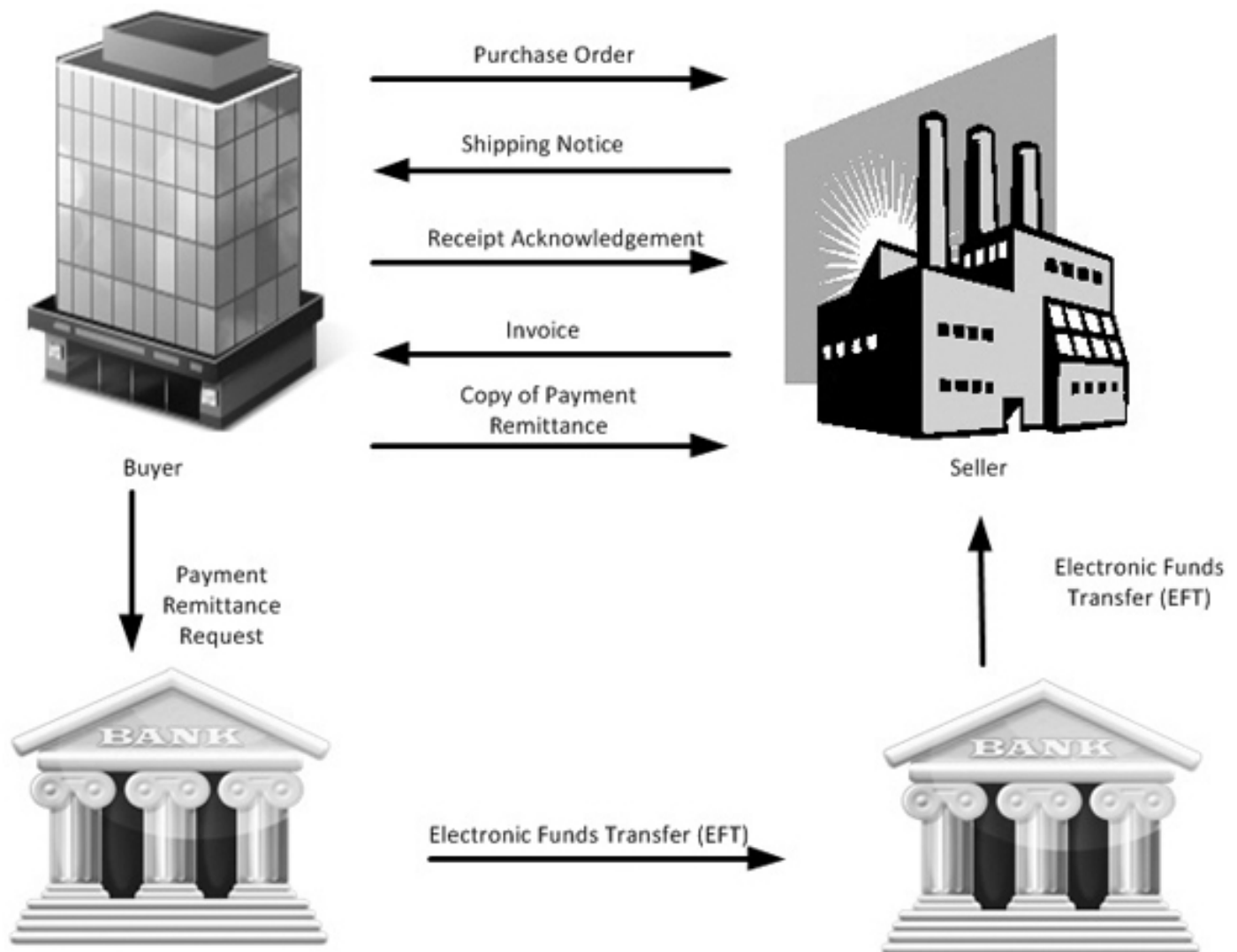


FIGURE 13.4 Electronic Data Interchange Example

An important characteristic of EDI is that organizations must use standardized formats for the documents they are exchanging. In fact, every organization has its own internal systems to handle purchase orders, invoices, and other business documents; therefore, each organization stores and handles data in different formats. An EDI transaction starts with the conversion of the documents and data from the format used by the internal system of

the organization to an EDI format. This is called the **outbound transformation**. The EDI documents are then sent to the partner organization, where the company’s systems must perform an **inbound transformation**, which involves the system converting the EDI documents into the format used by the internal systems of that organization. The most-used standardized formats for EDI are **ANSI X.12** and **EDIFACT**.

TABLE 13.4 B2B E-Business Models

Electronic data interchange (EDI)	Electronic exchange of information between two or more organizations using a standard format.
Supply chain management (SCM)	Allows organizations to manage the movement of materials or products from provision to production to collaboration between partners both upstream and downstream from the focal organization.
E-marketplaces	Also known as an <i>exchange</i> . Allows vending companies and buying companies to “meet” electronically t

EDI used to be limited to one-to-one communications between two trading partners. Today, it has evolved into a multipartner environment, allowing transmission of documents across a variety of information systems, even if they are incompatible in terms of hardware and software, since EDI documents themselves have to be in a very strict format. The use of a strict format is both an advantage and a disadvantage of EDI systems; on the one hand, it allows for fast processing and support for the various platforms, but on the other hand, it limits the flexibility of transmission that organizations want. Today, organizations want to conduct more complex activities than simply trading documents with one another to support their business processes, and they want to use the Internet as opposed to proprietary networks for the transmissions. This is where **extensible markup language (XML)** becomes a popular way of conducting B2B transactions. XML is a markup language that allows organizations to give meaning to their data but inserts tags that describe the data within documents. A markup language (such as HTML or XML) is used to give “meaning” to information by placing a beginning and end tag around the information. For example, in HTML, we can use bold tags: `<b>this is bolded</b>`. This will appear as **this is bolded** on the Web page.

XML is very flexible, since organizations can define their own tags. Once documents are tagged with XML, a variety of systems can read and understand the documents, as long at the systems know the definitions of the tags. In conducting B2B, therefore, organizations have to agree on the meaning of the tags. For example, if one company decides to code its standardized documents in XML using the term *client* (`<CLIENT> Mr. Jones </CLIENT>`) but its trading partner uses the term *customer* (`<CUSTOMER> Mr. Jones </CUSTOMER>`), their respective systems could not read each other’s data. Some industries are tackling this problem by developing industry-wide XML definitions or standards, such as **Electronic Business Extensible Markup Language (ebXML) for e-business**.

Finally, B2B can also be conducted in marketplaces, also known as exchanges. An **exchange** allows vendors or sellers to meet electronically. When a limited number of buyers or sellers are allowed to use a marketplace, we refer to this as a *consortia marketplace* or even a *private market*. When a large number of buyers and sellers exist, it is considered a **neutral auction**. Sometimes many buyers bid on a seller’s products (a **seller-oriented or forward auction**), or sometimes many sellers offer their products to a single buyer (a **buyer-oriented or reverse auction**). Over the years, many B2B marketplaces have come and gone, although some have succeeded. For example, Buyerzone.com allows small businesses to buy and sell products to one another. However, marketplaces are difficult to sustain because they need to have a sufficient number of buyers and sellers to ensure the growth of the marketplace.

LEARNING ACTIVITY 13.4

Where Is My Web Page?

In this activity, you will select two different Internet search engines to find some specific items. Record your results in a word processing file.

1. First, search for “intellectual property rights.” Identify the top three sponsored (if any) and the top three organic links found.
 2. Use the same two search engines to find the following products: a Trek mountain bike and an iPad Air 2.
- Indicate in your document the search engine used, the links you found, and your preferred search engine. Explain why you prefer a specific search engine.

Search Engine Optimization

Anyone involved in B2C e-business today would probably tell you that one of the most important factors for success online is being visible, which means showing up in searches. In fact, research has shown that if an organization’s link is not in the top 30, it does not exist. Other research says that it is the first page of results that counts. In a study of which links individuals click on in the search results page, 42% of individuals clicked on the first organic link (explained below); 12% on the second; 8% on the third; and then 6%, 5%, and 4% on the following ones, with 3% for the remainder of the links on the first page of search results (<http://www.redcardinal.ie/search-engine-optimisation/>). Clearly, being at the top of the search results page is important for e-businesses. But how does an organization make sure it shows up toward the top of the search results? This is the role of **search engine optimization (SEO)**, which is the series of practices an organization can use to improve its visibility or optimize how its Web pages or website shows up on the search engine results pages. SEO uses a combination of how the Web page is designed, which keywords and language are used on the Web page, and which search engines are most used by specific audiences.

SEO is not a one-time effort, since search engines change their requirements often, people change their searching patterns, and competitors also try to optimize their own websites. In terms of design, one of the most important first steps for an organization is to clearly identify which keywords best represent what the organization’s *intended audience* would use to find them. The key is to identify what the targeted audience thinks when they search online. It is also important to note that a keyword could actually be a keyword phrase, such as “mortgage lender” or “best place to eat.” With this information, the Web designers can do several things to help the ranking of the Web page. They can include the main keywords more often on the page and in more prominent places (headings, for example). They can include keywords in meta tags, which is information included with the page but not seen on the Web. There are many other factors that impact the ranking, such as including in-links, or inbound links, where other sites link to the organization; the age of the website domain (the older the better); and the overall size of the website. The exact details of how a website is more highly ranked vary over time and across search engines. This is why many consultants have started to offer SEO services to small, medium, and even large e-businesses.

Another way to have an organization’s website show up higher in the rankings is to pay for placement. These are considered **sponsored links**, as opposed to **organic links** (ranked by design and SEO only). Some research suggests that most individuals prefer organic links, with 80% to 90% of the clicks being on organic links (<http://www.redcardinal.ie/search-engine-optimisation/>). Sponsored links show up separate from the search results and are based on the keywords entered in the search engines, as seen in [Figure 13.5](#). The figure shows an example of Google AdWords, which is Google’s sponsored link service.

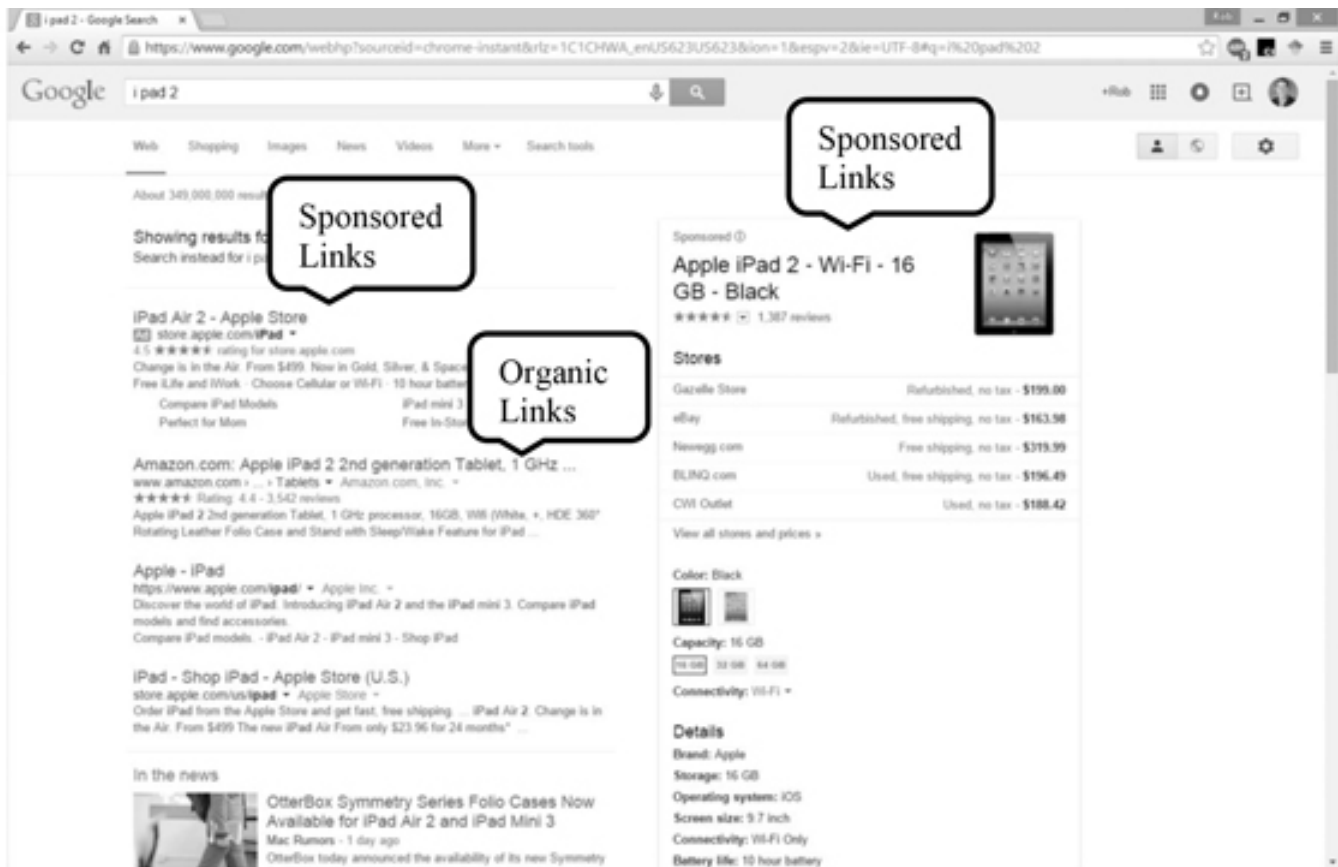


FIGURE 13.5 Search Results for Organic and Sponsored Links

Keyword bidding is another form of paying for a better ranking. It is also known as pay-per-click (PPC). The concept is that an organization pays the search engine owners only when someone clicks its link on the search results page. In most cases, companies bid for keywords, and the company that bids the highest will show up higher in the results when someone uses the keywords in a search. There is another type of PPC called *flat-rate PPC*, where the price of keywords is fixed. Nevertheless, you can easily see why PPC is an important source of revenues for companies like Google AdWords, Yahoo!, Search Marketing, or Bing Ads. Every time a user clicks on a link, the organization pays the search engine. In fact, many companies increased their paid search engine use for the holiday season in 2014 and saw revenue increase 50% on Thanksgiving Day due to online sales directly attributable to paid searches (Enright 2011). What does it cost to “buy” a keyword from a search engine? The cost varies substantially depending on the month of the year and what is going on at that time. An updated list can be found at <http://www.wordstream.com/articles/most-expensive-keywords>. In May 2014, the most expensive keywords were “insurance” at \$54.91 per click and “loans” at \$44.28 per click. Table 13.5 shows some of the other popular keywords at that time. As you can see, keywords can be very expensive. Therefore, organizations are often told to find the best and most representative keywords for their businesses and to aim to be number two instead of number one in the search results.

TABLE 13.5 Most Expensive Keywords, May 2014

1. Insurance	\$54.91
2. Mortgage	\$47.12
3. Attorney	\$47.07
4. Loans	\$44.28
5. Lawyer	\$42.51

6. Claim	\$42.05
7. Donate	\$42.02
8. Degree	\$40.61
9. Credit	\$36.06
10. Hosting	\$31.91

Source: Based on data by WordStream, available at <http://www.wordstream.com/articles/most-expensive-keywords>.

Paid search engines are a huge business, and the main players in the United States are Google, Yahoo!, and Bing. However, when considering the global market, another player enters the scene: Baidu. As of mid-2015, Google owned about 66% of the market; Baidu, 13%; Yahoo!, 9%; and Bing, 9%. In China, the search engine Baidu owns the majority of the market share, helping it reach second place in the global rankings (<https://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=0>).

Trends in E-Business

E-business has become mainstream, with individuals and organizations becoming increasingly comfortable transacting and interacting electronically. We discuss three major trends in e-business in the remainder of the chapter. Students, however, can go to the book's website for more interesting trends.

Mobile Business

Today, many individuals use sophisticated Internet-enabled mobile technologies, such as cellular phones, smartphones, and tablets in their daily work and personal lives. This has enabled another form of e-business known as **mobile business (m-business)**, which is when individuals conduct commercial transactions and interactions using handheld mobile devices and wireless communication networks. With mobile devices, users have access to critical information anywhere and anytime, which allows them to seize business opportunities (such as enjoying the sale of the day on Woot! [<http://www.woot.com>]). As discussed earlier, with the advent of **location-based services (LBS)**, it is even possible to provide targeted advertisements to users, such as discounts based on their current location. Therefore, as the user walks in front of a certain restaurant at mealtime, a coupon appears on the user's mobile device.

STATS BOX 13.2: MOBILE BEHAVIORS

Mobile phones are being used by almost everyone today. In the following table, you can see the mobile technology usage of people in the United States.

Mobile Behaviors and Ownership in the United States, November 2014

	Percentage
Adults who own a smartphone	71%
Adults who own a cell phone	91%
Adults who own an e-reader	23%
Adults who own a tablet	35%
Smartphone is only access to the Internet	15%

Checked phone for messages or alerts when the phone was not ringing or vibrating

Slept with phone next to bed so as not to miss calls or messages

Can't imagine living without cell phone

Used for text messaging

Used for Internet access

Used for Email

Downloaded apps

Received directions and recommendations based on location

Listened to music

Engaged in video calls/chats

Texted a charitable donation

Uninstalled apps due to privacy concerns

Source: <http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/>.

Global E-Business

Another important trend for e-business is the global nature of the phenomenon. Usage of electronic means for business is growing everywhere in the world. In fact, the Internet is also becoming multilingual, facilitating e-business. By the end of 2013, there were 800.6 million users of English websites on the Internet (<http://www.internetworldstats.com/stats7.htm>). At the same time, 649.4 million used Chinese, 222.4 million used Spanish, and 135.6 million used Arabic websites. As you might have learned in [Learning Activity 13.1](#), the growth of e-commerce sales corresponds with this growth in Internet usage. [Stats Box 13.3](#) lists some global e-business facts published by [eMarketer.com](http://www.eMarketer.com).

STATS BOX 13.3: GLOBAL E-BUSINESS

E-business is a global phenomenon. [eMarketer.com](http://www.eMarketer.com), a leading digital research firm, offers the following statistics:

- In 2012, e-commerce sales topped \$1 trillion for the first time.
- In 2012, North America was the leading location of e-commerce sales at \$364.66 billion.
- In 2012, the average online spending per user in China was \$591, compared to \$2,293 in the United States.

Source: "Ecommerce Sales Topped \$1 Trillion for First Time in 2012," <http://www.eMarketer.com/Article/Ecommerce-Sales-Topped-1-Trillion-First-Time-2012/1009649>.

LEARNING ACTIVITY 13.5

Usa.gov

Government websites are sometimes different than e-commerce websites. In this learning activity, you are to interact with the [usa.gov](http://www.usa.gov) website (<http://www.usa.gov>) or your local government's website. Identify five similarities and differences between this e-government site and the e-commerce sites used in [Learning Activity 13.2](#).

E-Government

A final trend we discuss is e-government, which was introduced at the beginning of the chapter. **E-government** involves using information technologies to enable and improve the efficiency with which government services are provided to citizens, employees, businesses, and agencies. It can occur at various levels of government, such as municipalities, counties, districts, states, provinces, or countries. It has become popular not only for obtaining information from government agencies but also for conducting transactions such as paying taxes, renewing licenses, or downloading government forms. According to Smith (2010), 82% of Internet users search for government information or complete government transactions online. The most leading-edge applications in e-government include platforms for citizen feedback via blogs, Twitter, or social networking sites. The future of e-government is also likely to include some form of **Internet voting**, where citizens will be able to cast their votes electronically via the Internet. In fact, some countries and states have already started to allow citizens to vote via the Internet.

CHAPTER SUMMARY

In this chapter, we discussed e-business. We first presented various ways to categorize e-business and then explored specific business models in greater depth. More specifically, we explained how business-to-consumer (B2C) e-business is conducted and what its enablers and impacts are. We also discussed business-to-business (B2B) e-business models in depth. The chapter concluded with search engine optimization and a discussion of important trends related to e-business.

Here are the main points discussed in the chapter:

- E-business involves electronic means to interact or conduct business with individuals, companies, or government agencies. E-business can be classified according to type: business-to-consumer (B2C; interactions are taking place between a consumer and a business), business-to-business (B2B; interactions are taking place between two businesses), consumer-to-consumer (C2C; interactions are taking place between two consumers), and government-to-constituent (G2C; interactions are taking place between a government agency and a constituent). E-businesses can also be classified according to their online component: bricks and mortar are traditional organizations with physical locations, bricks and clicks are traditional organizations with physical locations but that also operate an online business, and pure plays are organizations with only an online business.
- Business-to-consumer (B2C) e-business models include online retailing (offering products or services for sale to consumers online), infomediaries (offering specialized information to consumers via the Internet that aggregates or analyzes products or services from several providers), content providers (offering consumers content or relevant information), exchanges (offering a location [marketplace] for buyers and sellers to transact online), online communities or social media (offering individuals with similar interests and /or goals an online meeting place to interact with each other), and e-business infrastructure providers (offering infrastructure hardware, software, or services to other organizations for e-business). Enablers of B2C e-business include technological enablers (ease of use, bandwidth, and interoperability) as well as a social enabler (critical mass). Finally, impacts of e-business include channel compression and channel expansion.
- Search engine optimization (SEO) is the series of practices an organization can use to improve its visibility, or optimize how its Web pages or website show up on the search engine results pages. SEO uses a combination of Web page design, keywords and languages used on the Web page, and listings on search engines most used by specific audiences. One way to optimize placement is through sponsored links, where companies pay for placement or use keyword bidding, which gives companies with the highest bids higher placement in search engine results.
- Business-to-business (B2B) e-business involves the sharing of electronic documents, funds, and/or information between organizations. B2B e-business models include supply chain management, electronic data interchange (EDI), and e-marketplaces. EDI is the electronic exchange of information between two or more organizations using a standard format. The most-used standardized formats for EDI are ANSI X.12 and EDIFACT, but

organizations are increasingly using XML (extensible markup language) to conduct B2B transactions because it is much more flexible in terms of the types of information it allows organizations to exchange with one another. B2B marketplaces, or exchanges, allow vendors or sellers to “meet” electronically.

- Three major trends in e-business are mobile business, global e-business, and e-government. Mobile business, or m-business, occurs when individuals conduct commercial transactions and interactions using handheld mobile devices and wireless communications networks. Global e-business is occurring because usage of electronic means for business is growing everywhere in the world and the Internet is becoming increasingly multilingual. E-government involves using information technologies to enable and improve the efficiency with which government services are provided to citizens, employees, businesses, and agencies.

REVIEW QUESTIONS

1. Define e-business and compare this to e-commerce, e-government, and Internet commerce. Is Internet commerce considered e-business?
2. Explain what a business model is and what it should include.
3. Describe the various ways to classify e-business models, including B2C and B2B models.
4. Identify the main technological factors that have enabled e-business growth and compare them to the technological enablers of m-business.
5. Explain the concept of network effects or network economics and its importance to e-business.
6. Explain how e-business has led to disintermediation and provide examples.
7. Explain how e-business has led to channel expansion, discuss its impacts, and provide examples.
8. Describe the goals of search engine optimization, the various ways in which it is performed, and other options organizations have for marketing their websites.
9. Compare and contrast B2B e-business to B2C e-business.
10. Describe how electronic data interchange (EDI) functions and how it is evolving today.

REFLECTION QUESTIONS

1. What is the most important thing you learned in this chapter? Why is it important?
2. What topics are unclear? What about them is unclear?
3. Is it important to distinguish among e-business, e-commerce, and Internet commerce? Why or why not?
4. How is the material in this chapter related to the material on transmitting information in [Chapter 7](#)?
5. What is the relationship between network effects and the material on competitive advantages in [Chapter 4](#)?
6. What is the role of security in e-business success?
7. What is the role of privacy in e-business success?
8. If both channel compression and channel expansion occur in an industry because of e-business, does that mean that e-business had limited impacts on that industry? Why or why not?
9. A businessperson the authors know said that search engine optimization is as much art as science. What does he mean?
10. Why is mobile commerce more popular in other areas of the world compared to the United States?

ADDITIONAL LEARNING ACTIVITIES

Learning Activity 13.A1

For this activity, read the article “Failed E-Businesses” on the book’s website. Identify three common mistakes made by the e-businesses that failed during the dot-com bust era. Pick two of them and identify what could you do to make those businesses work today.

Learning Activity 13.A2

This activity requires you to complete a case analysis regarding e-business. The case may be accessed through your university website, the Ivey Business School business case website (<https://www.iveycases.com>), or the Harvard Business School cases website (<https://cb.hbsp.harvard.edu/cbmp/pages/home>), or it may be provided to you by your instructor:

Upton, D., and Fuller, V. 2003. “CASE: The ITC eChoupal Initiative.” *Harvard Business Case*, October 28. Product number: #9-604-016 (revised).

Learning Activity 13.A3

E-business has become a global phenomenon. However, not all countries are equal when it comes to having infrastructures, laws, and business practices that support e-business. The Economist Intelligence Unit (EIU; <http://www.eiu.com>) ranks each country on its digital economy readiness. In this learning activity, you will be assigned a country and will need to explore its e-business readiness. Your instructor will assign you a country to research. Bring a short report to class that includes the following:

- The country you are assigned
- The EIU ranking for digital economy readiness
- Any e-business statistics you can find about your assigned country
- Your research of potential explanations for the ranking of your country (You will have to make assumptions.)

Learning Activity 13.A4

Conduct research on the Web to give examples of each type of e-business defined in [Table 13.1](#).

Learning Activity 13.A5

Extend the existing business models presented in [Table 13.2](#) with the use of location-based services (LBS). Describe how mobile users could make use of these models.

Learning Activity 13.A6

Identify the business models of the following websites: <http://www.pandora.com>, <http://www.consumerreports.org>, <http://www.yahoo.com>, and <http://www.weightwatchers.com>.

Learning Activity 13.A7

Identify additional major trends in e-business beyond the ones presented at the end of the chapter.

REFERENCES

- eMarketer. 2015. "Referrals Fuel Highest B2B Conversion Rates." [eMarketer.com](http://www.eMarketer.com/Article/Referrals-Fuel-Highest-B2B-Conversion-Rates/1012000), February 10. <http://www.eMarketer.com/Article/Referrals-Fuel-Highest-B2B-Conversion-Rates/1012000>.
- Enright, A. 2011. "Paid Search Pays Off over the Holidays: Budgets Were Up 52% during November and December, and Related Sales Rose 69%." *Internet Retailer*, January 13. <http://www.internetretailer.com/2011/01/13/paid-search-paid-over-holidays>.
- Smith, A. 2010. "Government Online: The Internet Gives Citizens New Paths to Government Services and Information." *Pew Internet and American Life Project Report*. Retrieved January 26, 2011, from <http://pewinternet.org/Reports/2010/Government-Online.aspx/>.

FURTHER READINGS

- Chaffey, D. 2010. "[Boo.com](http://www.boocom.com) Case Study—a Classic Example of Failed E-business Strategy." *Digital Marketing Case Studies*, February 15.
- Segal, D. 2011. "The Dirty Little Secrets of Search." *New York Times*, February 12.

GLOSSARY

ANSI X.12: One of the most-used standardized formats for EDI.

Bricks and clicks: Traditional organizations with physical locations as well as an online businesses.

Bricks and mortar: Traditional organizations with physical locations.

Business model: The way the organization functions and creates value.

Business-to-business (B2B): A type of e-business where interactions are taking place between two businesses.

Business-to-consumer (B2C): A type of e-business where interactions are taking place between a consumer and a business.

Buyer-oriented or reverse auction: Many sellers offer their products to a single buyer.

Channel compression (disintermediation): A situation in which the distribution chain is shortened by eliminating some or all of the intermediaries between the focal firm (product producer) and the end consumer.

Channel expansion: The addition of intermediaries in an industry whose purpose is to aggregate and provide information or brokering functionalities.

Consumer-to-consumer (C2C): A type of e-business where interactions are taking place between two consumers.

Content providers: An e-business model where companies offer consumers content or relevant information and receive money from vendors for ads or downloads or from consumers for subscriptions.

Critical mass: A point when there are sufficient buyers to sustain the business of vendors and sufficient vendors to attract buyers to the Internet.

E-business infrastructure provider: A company that offers infrastructure hardware, software, or services to other organizations for e-business.

ebXML for e-business (E-business XML): An industry-wide set of XML definitions or standards for e-business.

EDIFACT: One of the most-used standardized formats for EDI.

Electronic business (e-business): An electronic means to interact or conduct business with individuals, companies, or government agencies.

Electronic commerce (e-commerce): An electronic means to conduct business transactions, including the Internet, EDI, or private networks.

Electronic data interchange (EDI): A B2B e-business model focusing on the electronic exchange of information between two or more organizations using a standard format.

Electronic funds transfer (EFT): An electronic means to conduct financial transactions such as payments and remittances.

Electronic government (e-government): An electronic means to interact or conduct transactions with government agencies.

E-marketplaces (exchanges): Allows vendors or sellers to “meet” electronically.

Exchange: An e-business model where companies offer a location (marketplace) for buyers and sellers to transact online.

Extensible markup language (XML): A markup language that allows organizations to give meaning to their data by inserting tags that describe the data within documents; a popular way of conducting B2B transactions.

Government-to-constituent (G2C): A type of e-business where interactions are taking place between a government agency and a constituent.

Inbound transformation: Converting the EDI documents into the format used by the internal systems of that organization.

Infomediaries: An e-business model where companies offer specialized information to consumers via the Internet that aggregates or analyzes products or services from several providers.

Internet commerce: An electronic means to conduct business using the Internet (for example, email, the Web, or file transfers).

Internet voting: When citizens are able to cast their votes electronically via the Internet.

Interoperability: The ability of heterogeneous systems to communicate with each other.

Keyword bidding (pay-per-click: PPC): When organizations pay the search engine owners when someone clicks their links on the search engine results page.

Location-based services (LBS): Services that make use of knowing where users are based on their cell phone location to offer targeted advertising or services at a specific moment.

Markup language (such as HTML or XML): Used to give “meaning” to information by placing a beginning and end tag around the information.

Mobile business (m-business): When individuals conduct commercial transactions and interactions using handheld mobile devices and wireless communications networks.

Network effects or network economics: Explains how value is attained in a network when critical mass, or plentitude of members, is achieved. The value of the network increases every time a new member is added to the network.

Neutral auction: A marketplace with a large number of buyers and sellers.

Online community or social media: An e-business model where organizations offer individuals with similar interests and /or goals an online meeting place to interact with one another.

Online retailing: An e-business model where companies offer products or services for sale to consumers online.

Organic links: Links on search engine results achieved by design and search engine optimization.

Outbound transformation: Conversion of the documents and data from the format used by the internal system of the organization to an EDI format.

Pure plays (click only): Organizations with only an online business.

Search engine optimization (SEO): A series of practices an organization can use to improve its visibility or optimize how its Web pages or website shows up on the search engine results pages.

Seller-oriented or forward auction: Many buyers bid on a seller's products.

Sponsored links: Links that show up higher in the search engine results because the organization has paid for placement.

Supply chain management (SCM): A B2B e-business model focusing on the electronic exchange of information along the supply chain.

Web commerce: An electronic means to conduct business transactions using the Web as an interface.

CHAPTER 14

INFORMATION AND KNOWLEDGE FOR BUSINESS DECISION MAKING

LEARNING OBJECTIVES

By reading and completing the activities in this chapter, you will be able to

- Explain why knowledge management is important to organizations
- Compare and contrast explicit and tacit knowledge
- Describe the main processes for knowledge management
- Compare and contrast major knowledge management technologies

CHAPTER OUTLINE

- [Focusing Story: Managing Knowledge by Texting](#)
- [Learning Activity 14.1: How You Manage Knowledge](#)
- [Knowledge Management](#)
- [Why Managing Knowledge Is Important](#)
- [Main Processes for Knowledge Management](#)
- [Learning Activity 14.2: Wikis for Managing Knowledge](#)
- [Knowledge Management Technologies](#)
- [Learning Activity 14.3: Using a Decision Support System](#)
- [Decision Support Systems and Group Decision Support Systems](#)
- [Business Intelligence](#)
- [Chapter Summary](#)
- [Review Questions](#)
- [Reflection Questions](#)
- [Additional Learning Activities](#)
- [References](#)
- [Further Readings](#)
- [Glossary](#)

Ultimately, a business's ability to compete depends heavily on how its employees apply knowledge to make decisions and solve problems. Information systems and technologies can help organizations better manage knowledge. In addition, information systems and technologies can facilitate better decision making. In this chapter, we help you understand knowledge management and how technologies can help organizations manage knowledge. Knowledge is often applied to decision making. Because of this, we also discuss decision support

systems. As organizations gather an increasing amount of data, being able to leverage these data for decision making and action is an increasingly important aspect of business. Business intelligence systems, which we also discuss in this chapter, help organizations make sense of this sea of data.

FOCUSING STORY

Managing Knowledge by Texting

Several years ago, I was teaching an onsite class to information technology (IT) professionals working at a major logistics company. While waiting for class to start one night, I overheard one of the students asking another if he had received a text message regarding a problem he was having with a computer program. This surprised me. At the time, such messaging was generally done more for personal than business reasons. So I asked the student who sent the text how frequently they exchanged such messages. The student replied, “All the time. Whenever one of us runs into a problem we haven’t seen before, we send a message to the group. Usually someone has seen a similar problem, so they can help.” Essentially, the group had informally created a “knowledge network” of shared expertise. By sending a simple text message, an individual worker can tap into the knowledge of the entire group. The result is hours of saved time and frustration.

More recently, people are using social networking sites such as LinkedIn and Facebook as a means of accessing the knowledge of others. For example, when I had to write a job description for an unusual faculty job, I turned to several LinkedIn groups for advice. Some individuals responded with helpful advice. When you are faced with a decision, it is often necessary to reach out to those who may have knowledge useful to the decision. This may be as simple as calling your car-loving brother when you are buying a new vehicle, or it may mean convening a meeting of experts to help a corporate board decide whether to pursue a merger. Regardless of the decision, the intent is the same. Additional knowledge can have great value to decision making. Whether you use text messaging to get help solve a computer problem or you fly in experts from around the world, you are still trying to leverage the knowledge of others to help you make a decision. Fortunately, information technologies can aid in the quest to use the knowledge of others to help make better decisions.

FOCUSING QUESTIONS

1. When have you used the knowledge of others to help you make a decision? Briefly describe the decision. Whom did you contact to help you? What knowledge were you trying to access?
2. How have you used information technologies to help you connect with others for the purpose of tapping their knowledge? Why did you use those technologies?

LEARNING ACTIVITY 14.1

How You Manage Knowledge

This chapter helps you understand organizational knowledge management, but individuals also manage their knowledge. The goal of knowledge management is to make sure the right knowledge is available in a useful form to the right people. Personal knowledge management is the process of determining what knowledge you need and how to find, organize, and use that knowledge. Prepare a one- to two-page paper on how you manage your personal knowledge. What tools do you use? How effective are they? Compare your response with another student’s response.

Knowledge Management

In an earlier chapter, we introduced you to the concepts of data, information, and knowledge. You may recall that data are unconnected facts, information is data that have been processed so that they are useful, and knowledge

is information that is applied to a decision or action. If you think about these differences, you may see that as we progress from data to information to knowledge, there is a greater level of human contribution and greater value.

However, as we move up the hierarchy toward knowledge, things get harder to manage, in part because of the increased level of human contribution. It is relatively easy to manage data, but managing knowledge is quite difficult. [Table 14.1](#) shows some characteristics of data, information, and knowledge. As you can see from the table, knowledge is hard to structure, transfer, and capture, which leads to knowledge being much harder to manage than data or information.

TABLE 14.1 Characteristics of Data, Information, and Knowledge

Data	Information	Knowledge
Easily structured	Made up of processed data	Hard to structure
Easily captured	Requires unit of analysis	Difficult to capture
Easily transferred	Requires human involvement	Often tacit
Often quantified		Hard to transfer
Made up of mere facts		Information applied to some decision or action

Source: Adapted from Pearlson and Saunders (2006).

Knowledge management is a process that allows organizations to generate value from their knowledge-based assets. Knowledge management involves capturing and documenting what employees and other stakeholders know and developing systems that make it easier to share and use that knowledge. Later in this chapter, we discuss the process of knowledge management. Before getting into that, however, we help you understand why knowledge management is important.

Why Managing Knowledge Is Important

Knowledge is among the most important resources of any organization. Recall that knowledge is information directed toward action and decision making. To be successful, organizations must not only effectively manage information, but they must also manage knowledge. Unfortunately, knowledge management is often messy and complex.

Organizations have always managed knowledge. More recently, however, organizations have begun using information and communication technologies to help manage knowledge. Organizations that manage knowledge well make better decisions, are generally more innovative, and tend to be more successful overall than those that do not.

Effective knowledge management can bring about big benefits, including the following:

- Better problem solving
- Improved customer service
- More effective product management
- Increased innovation
- More efficient and more effective processes
- Increased intellectual capital
- Better leveraging of intellectual assets

Types of Knowledge

Understanding more about knowledge will help you better understand important aspects of knowledge management systems. We can divide knowledge into two categories: explicit knowledge and tacit knowledge. **Explicit knowledge** can be expressed relatively easily. Examples include operations manuals, books and articles, scientific formulas, and statistical analysis. Because explicit knowledge can be easily expressed, it can be more easily shared, stored, and managed than our other category of knowledge, tacit knowledge. It may be helpful to think of explicit knowledge as “knowing that,” while tacit knowledge is more about “knowing how.”

Tacit knowledge is not easy to express or communicate. It is internalized and highly individualized. An individual’s tacit knowledge is rooted in life experiences, values, and biases. Ask an artist how to create a beautiful piece of art. The chances are that he or she will have trouble expressing exactly how striking art is created. This is an example of tacit knowledge. The artist may be able to create such art but may not be able to easily communicate the process to you. In fact, sometimes the person who possesses the tacit knowledge may not even be aware that he or she has the knowledge.

Tacit knowledge also exists in more mundane contexts. A good salesperson knows when to close a sale and when to back off. A knowledgeable computer programmer can quickly diagnose an error message. There are examples of tacit knowledge in any organization and in any profession. One of the most interesting examples comes from the world of poultry. Determining the sex of a baby chick immediately after hatching is important for commercial egg producers. Egg producers prefer female chicks, since they will be able to lay eggs. Egg producers employ chicken sexers, who have the uncanny ability to discriminate between female and male chicks with a quick glance. What is interesting about this ability is that most expert chicken sexers cannot tell you how they make their decisions, yet they are very accurate. They have the tacit knowledge but are unable to easily convert this into explicit knowledge. Capturing tacit knowledge and codifying it so that it can be shared is one of the major challenges of knowledge management.

Types of Knowledge Resources

Knowledge is a critical resource for organizations, as we noted earlier. There are different types of knowledge resources in any organization. Understanding these will help you understand knowledge management, which we discuss later. Knowledge resources can be divided into four categories (Nonaka and Takeuchi 1995):

- **Experiential knowledge** resources consist of tacit knowledge that can be shared through common experiences and interpersonal communication. Examples include skills, know-how, and emotional knowledge.
- **Conceptual knowledge** resources are made up of explicit knowledge that is embodied in language, symbols, and images. Concepts for products, services, and designs are examples.
- **Systemic knowledge** resources consist of explicit knowledge that has been systemized and packaged. Knowledge assets in this category are the easiest to share and manage. Intellectual property, such as patents and licenses, documents, and databases are examples.
- **Routine knowledge** resources are made up of the tacit knowledge embedded in the organization’s practices. Organizational routines for day-to-day activities and organizational culture are examples of routine knowledge.

Now that you understand more about knowledge and its characteristics, we can turn our attention to how to manage knowledge.

Main Processes for Knowledge Management

A complete knowledge management system should consist of knowledge creation, capture, codification, storage, retrieval, transfer, and application, as shown in [Figure 14.1](#). Knowledge management processes form a cycle. Applying knowledge often leads to the creation of new knowledge, which restarts the cycle. While information

technology is not required for any of these, as you will see, IT can facilitate each process in a knowledge management system. In this section, we discuss each of these processes.

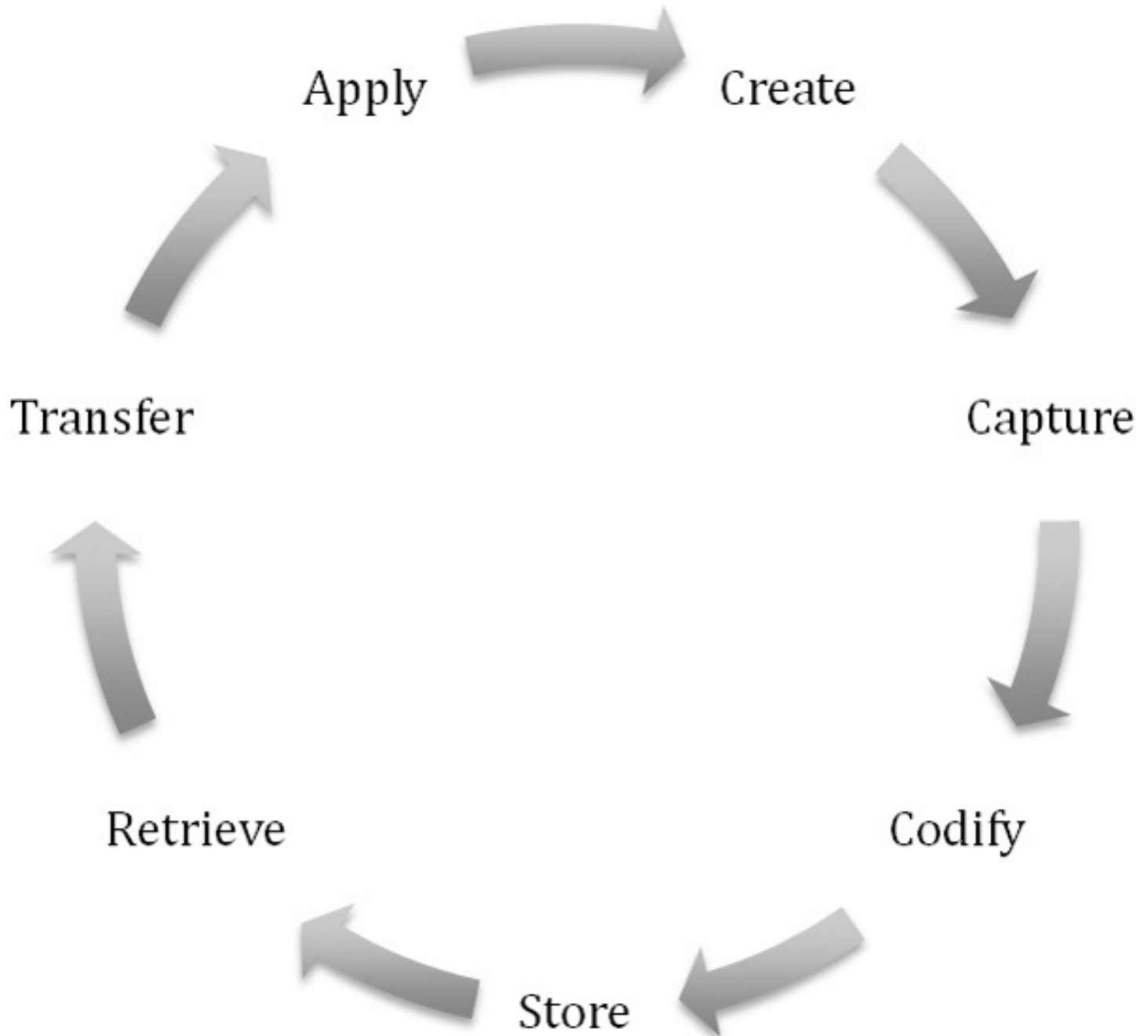


FIGURE 14.1 Knowledge Management Cycle

Information technology is critical to modern knowledge management, but technology alone cannot ensure effective knowledge management. Effective knowledge management also requires social and structural mechanisms that support knowledge management. For example, a culture of trust can greatly enhance knowledge sharing within an organization. Poor organizational processes and culture can bring about knowledge management failure.

Creating Knowledge

While knowledge exists in individuals, organizational knowledge can also be created. Nonaka and Takeuchi (1995) proposed the SECI model of organizational knowledge creation. The model is shown in [Figure 14.2](#).

According to the model, knowledge creation is a continuous process consisting of interactions between implicit and explicit knowledge. There are four processes by which knowledge is created:

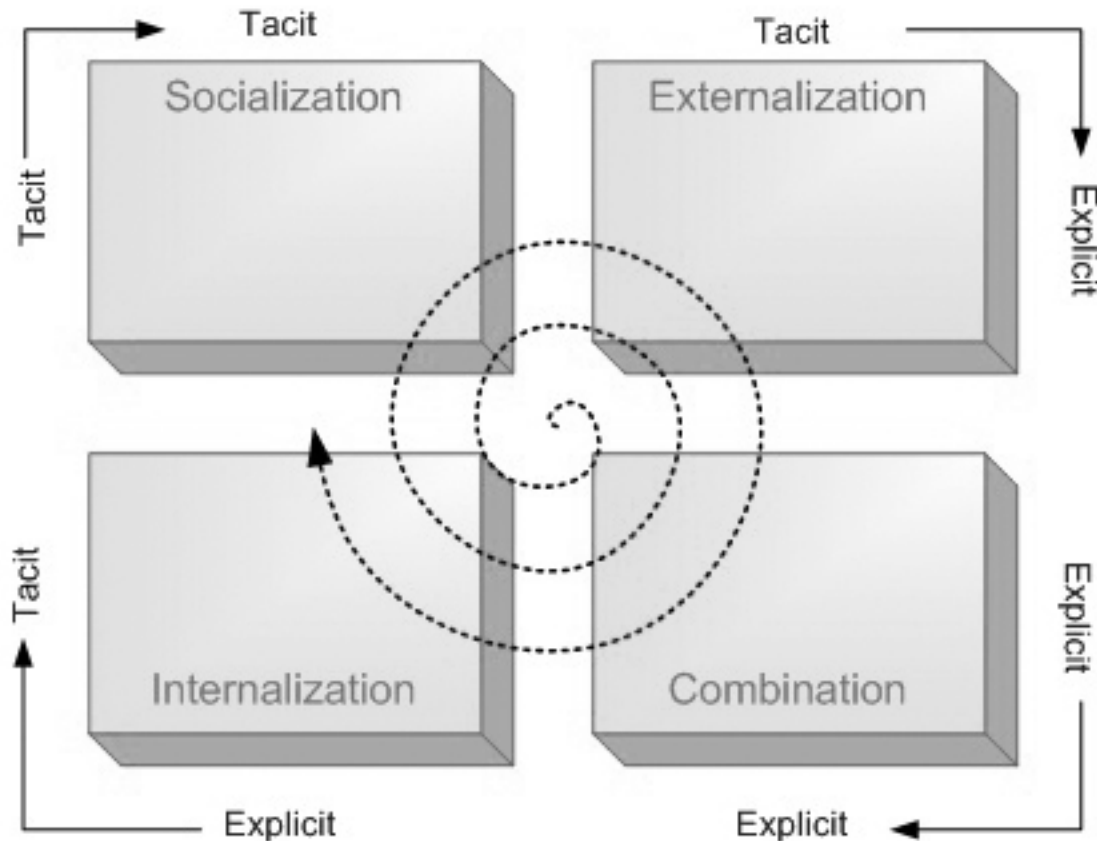


FIGURE 14.2 SECI Model of Organizational Knowledge Creation

- *Socialization* involves sharing tacit knowledge through direct communication or shared experience. This is tacit-to-tacit communication.
- *Externalization* is tacit-to-explicit communication. Tacit knowledge is converted to explicit knowledge by developing specific concepts, models, and the like. This conversion allows the knowledge to be understood and interpreted by others. This also serves as a foundation for creating new knowledge.
- *Combination* is the process of combining the externalized explicit knowledge to form broader concepts, models, and theories.
- *Internalization* occurs when explicit knowledge transforms to tacit knowledge and becomes internalized by individuals within the organization. This can start a new cycle, beginning with the socialization of the new tacit knowledge.

These four processes form a cycle of increasing knowledge. Completing one cycle can start a new trip through the four processes, but with an ever-increasing amount of knowledge. This is represented by the spiral in [Figure 14.2](#).

Knowledge can also be “purchased” by hiring knowledgeable individuals as either consultants or employees. Knowledge can also be acquired by purchasing reports or even entire companies. An organization may acquire another company to gain access to the company’s knowledge assets.

Capturing and Codifying Knowledge

Once knowledge is created or otherwise acquired, it needs to be captured and codified. There are many techniques for capturing knowledge, including interviewing experts, observing groups as they make decisions, forming focus groups, holding “lessons learned” debriefings, and performing task analysis.

Codifying knowledge means converting tacit and explicit knowledge into a form that organizational members can use. It is representing knowledge so that it can be reused. This also includes documenting knowledge that was previously undocumented. To codify knowledge, organizations should do the following (Davenport and Prusak 1998):

- Define the strategic intent. (How will the codified knowledge serve the organization?)
- Identify the knowledge necessary to achieve the intent.
- Evaluate the existing knowledge’s usefulness and ability to be codified.
- Determine the best way to codify and distribute the knowledge.

Codifying knowledge is difficult, but there are tools that can help. Some of these are described below.

Cognitive maps represent the mental model of the expert’s knowledge. Key concepts and the relationships among them are shown. Software such as Freemind, MindMeister, and Visio can help document the maps. [Figure 14.3](#) illustrates a cognitive map of Web 2.0 concepts and tools.

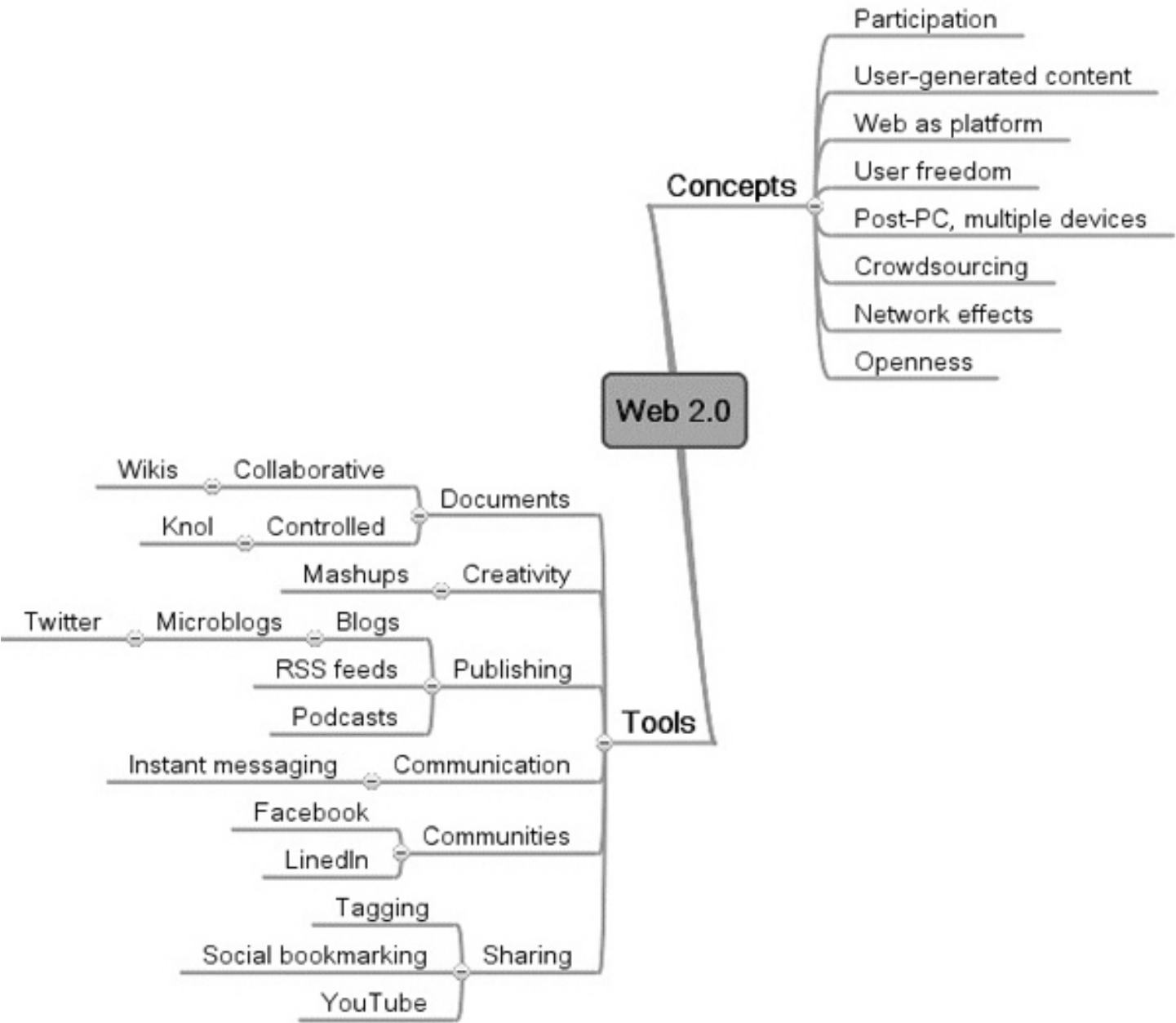


FIGURE 14.3 Cognitive Map of Web 2.0 Concepts and Tools

Decision tables show a list of conditions and their values along with a list of conclusions or actions. The conditions necessary for each conclusion are indicated. [Figure 14.4](#) shows a decision table for making MBA admission decisions. In each Y column indicates that the condition was met, while N means that the condition was not met. The X entries indicate the appropriate action.

Condition Stub	Condition Entry				
	1	2	3	4	5
Applicant has undergraduate degree	Y	Y	Y	Y	Y
Applicant has > 2 years work experience	Y	Y	Y	Y	N
GMAT > 600	Y	Y	N	N	N
Undergraduate GPA > 3.0	Y	N	Y	N	N
Admit	X				
Conditionally admit		X		X	
Advise to retake GMAT			X		
Decline admission					X

FIGURE 14.4 Decision Table Example

Decision trees show the alternate paths that impact decisions. The tree shows various paths that can lead to certain outcomes. Here the idea is to use decision trees as a way to document how a decision is made. [Figure 14.5](#) shows a decision tree for making MBA admission decisions.

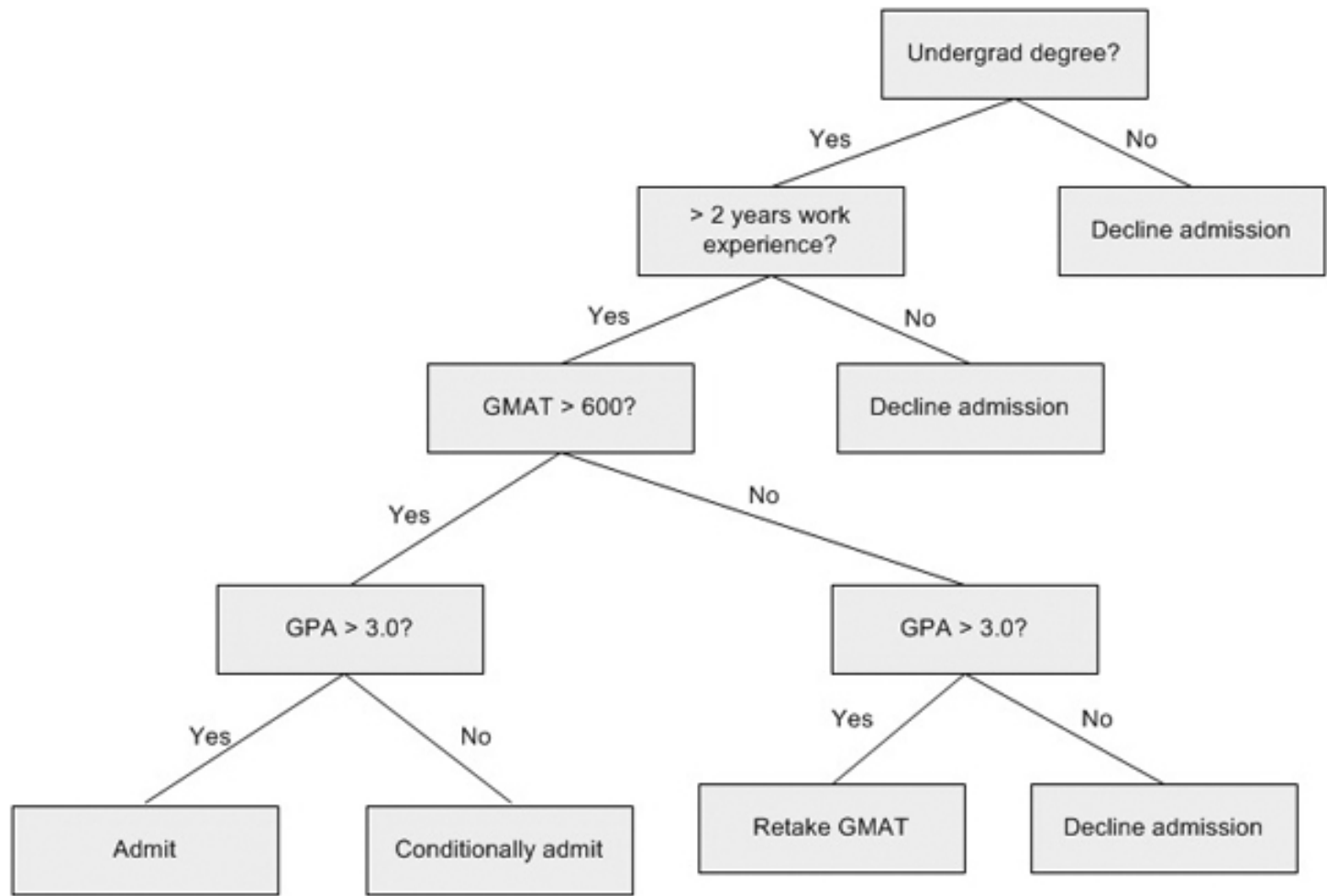


FIGURE 14.5 Decision Tree Example

The purpose of these and other codification tools is to systematically document knowledge that is “stored” in the minds of experts. By working with the experts to create these diagrams and tables, knowledge modelers can help capture and document experts’ knowledge. Documenting the knowledge allows us to store, organize, and share the knowledge so that others can use it.

BUSINESS EXAMPLE BOX 14.1

The Issue of Trust in Knowledge Management

Managers who want to have good knowledge management systems must work hard to create a culture that rewards rather than punishes knowledge sharing. Knowledge is a critical asset for any business professional. The more useful knowledge you possess, the more valuable you are to the organization. As is the case with any resource, the rarer the knowledge, the more valuable it is. In other words, if you have knowledge that few others have, you are more valuable to the business.

This simple fact can hinder knowledge management. Since sharing knowledge makes it more widespread (less rare), sharing decreases the value of possessing that knowledge. So if you share your knowledge, you become less valuable to the organization. Because of this, trust is important to knowledge management. Experts who possess knowledge must trust that their organization will not unfairly take advantage of the individual who shares the knowledge. If this trust does not exist, the expert may hoard the knowledge to maintain its value.

Storing and Retrieving Knowledge

Organizing knowledge so that it can be easily accessed is challenging. One reason for this is that knowledge can exist and be documented in many different forms. As a result, there is no single knowledge base for an organization. Knowledge is stored in a variety of forms, including some that you might find surprising. For example, a well-organized corporate directory that lists areas of expertise can be thought of as a knowledge store. Such a directory effectively points to experts, who are repositories of knowledge. Document storage systems are also examples of knowledge stores.

Knowledge storage and retrieval are closely interrelated. Even the most well-designed knowledge storage system is ineffective if knowledge consumers cannot retrieve the knowledge. Search technologies are important knowledge retrieval tools. Think about how many times you have used Google or some other search tool to locate knowledge. Accurate, fast search results are a boon to anyone seeking knowledge.

Transferring and Applying Knowledge

Knowledge needs to be applied to be useful, and application implies that knowledge is available to those who need it. Knowledge maps can facilitate knowledge transfer. Knowledge maps show the location of knowledge within the organization. A knowledge map can identify individual experts, networks of experts, or documents and databases.

To manage knowledge transfer, you must consider the sources of knowledge, the media used to transfer the knowledge, and the knowledge consumers. Sources of knowledge include experts, knowledge bases (databases for knowledge), and document repositories. Media may include computer networks and other communication media. Consumers are the individuals and groups that apply the knowledge.

You have engaged in knowledge transfer, even though you may not have realized it. Education is a form of knowledge transfer; your instructor is transferring some of her or his knowledge to you. Have you ever contacted a friend for help on an assignment or project? If so, you used your social network for transferring knowledge.

While humans have always used their social networks to access knowledge, the emergence of social networking technologies is increasing this sort of knowledge transfer. The use of instant messaging in the focusing story is

an early example of using software to tap into others' knowledge. New social networking tools make this sort of knowledge transfer even more effective.

LEARNING ACTIVITY 14.2

Wikis for Managing Knowledge

A wiki is a website that allows individuals to jointly create and edit Web pages about a chosen topic using a simple Web-based interface. (You learned about wikis in [Chapter 7](#). See the book's website for a link to a video explaining wikis.) Wikipedia, the online collaborative encyclopedia, is the most popular use of a wiki, but many other wikis exist. Prepare a one-page paper that discusses how a wiki can be used for knowledge management.

Knowledge Management Technologies

Information and communication technologies have helped with knowledge management for a long time. Even the telephone can be used to help individuals tap external knowledge. In this section, we discuss several knowledge management technologies.

Repositories

The goal of **knowledge repositories** is to make it easy to find and retrieve documents that contain knowledge. According to Pearlson and Saunders (2006), there are three main types of knowledge repositories:

- Externally focused knowledge
- Structured internal knowledge, such as research reports and marketing materials
- Informal internal knowledge, such as “lessons learned” reports and discussion databases and frequently-asked-questions collections.

Communication-Based Tools

There are many communication-oriented tools for knowledge management. Email is an example. We often email colleagues when we need knowledge that we do not possess. For example, a sales representative may email another sales rep for advice on how to position a certain offering. While email can be effective, you need to know who has the knowledge you need. You also need access to that individual. Social networks can help overcome these limitations. **Communities of practice** that exist within networks are especially helpful. LinkedIn groups are an example. Some of these groups are effectively communities of practice. For example, the group “Technology-Using Professors” is a network of college faculty who are interested in how technology can enhance learning.

Collaboration tools combine elements of repositories and communication-based knowledge management tools. Systems such as Google Docs and Microsoft SharePoint allow for document sharing and coediting. (You may recall that we discussed Google Docs in [Chapter 7](#).)

Some knowledge management experts see a trend from a content-focused view of knowledge management to one that is more connection focused. This means that rather than being centered around the ideas of collecting knowledge, the focus is shifting to tools that help you manage your connections to those who have helpful knowledge. The social networking tools we mentioned earlier are among the technologies that can help you with this form of knowledge management. For example, [Stats Box 14.1](#) provides some statistics for groups in LinkedIn. These groups are good examples of how social networking tools can be used for connection-focused knowledge management.

STATS BOX 14.1: LINKEDIN GROUPS AS COMMUNITIES OF PRACTICE

As of spring 2015, there were more than two million LinkedIn groups. (LinkedIn is a popular profession-oriented social networking site with more than 300 million members in more than 200 countries.) Many of these are professional or conference-oriented groups, many of which can be considered communities of practice. Some of these groups are quite large. The Social Media Marketing group has more than 90,000 members. The Project Manager Network group has more than 40,000 members. Members use these groups to connect with others with similar interests and professions. Most groups allow discussions, which are often used to access the knowledge of group members.

Sources: <http://www.linkedin.com>; <https://www.linkedin.com/pulse/20140430123558-49016055-the-10-largest-groups-on-linkedin>.

Executive Information Systems and Dashboards

Executive information systems (EISs) help provide high-level managers with the information they need to monitor business activities and make decisions. EISs typically make heavy use of graphical displays of data. They also tend to have easy-to-use interfaces that let executives quickly access the information they need. Both prebuilt reports and tools for custom queries are important components of an EIS. EISs also give executives the ability to “drill down” into information to access more detailed data when necessary. EISs have evolved to make greater use of the dashboard concept. **Digital dashboards** provide graphical views of key data along with graphical warnings when data indicate areas that need attention. [Table 14.2](#) lists a number of companies that create dashboard products. Visit these to view the various ways visuals are used to present data using dashboard software.

TABLE 14.2 Dashboard Products

Company	Link
BOARD	http://www.board.com/us/solutions-7/bi/dashboards
ClicData	http://www.clicdata.com/dashboards/
Dash	https://www.thedash.com/
IBM	http://www-01.ibm.com/software/analytics/rte/an/dashboards/
iDashboards	http://www.idashboards.com/Solutions.aspx
Klipfolio	http://www.klipfolio.com/guide-to-business-dashboards
SAP	http://www.sap.com/pc/analytics/business-intelligence/software/dashboards/index.html
Tableau	http://www.tableau.com/solutions/business-dashboards

Expert Systems

Expert systems help users solve problems or answer questions in a way that mimics an expert’s thought processes. An expert system typically has a narrow focus on a particular problem domain. For example, an insurance company can use an expert system to guide a salesperson through the process of selecting the most appropriate product for a customer. Many organizations use expert systems to guide nonexpert employees through complex decisions or problems such as technical troubleshooting. There are also systems for medical self-diagnosis,

although these systems should be used with caution, as they do not make a true diagnosis but rather provide probabilities of underlying causes for symptoms.

To close this section, we want to make sure that you understand that all organizations need to manage knowledge, even if they do not have formal knowledge management systems. Managing the knowledge resources of an organization is a critically important aspect of organizational success. While knowledge management is seen by some as an esoteric concept favored only by academics, in our opinion, organizational leaders are well advised to pay more attention to how they manage knowledge.

LEARNING ACTIVITY 14.3

Using a Decision Support System

Pick one of the following decisions and use the associated decision support system (DSS) to help you analyze the decision. (Your instructor may give you a different decision and DSS.)

- What car can you afford? DSS: <http://www.edmunds.com/calculators/affordability.html>
- Should you trade your “gas guzzler” for a more fuel-efficient vehicle? DSS: <http://www.edmunds.com/calculators/gas-guzzler.html>
- Should you buy or rent a house? DSS: <http://www.realtor.com/mortgage/tools/rent-or-buy-calculator/>

Partner with another student and describe your experience using the DSS. Was it useful? Why or why not?

Knowledge is typically applied to some decisions; decision making requires knowledge. While knowledge management technologies are relatively immature, decision support technologies are much more mature in comparison. Decision support systems provide technology tools for helping decision makers deal with the data and information that are necessary for applying knowledge. The next section discusses these tools.

Decision Support Systems and Group Decision Support Systems

Decision support systems (DSSs) are computer-based systems that help decision makers use data and models to solve semistructured or unstructured problems. There are many different types of DSSs, so it is convenient to divide them into categories. Our categories are based on Alter’s (1977) and Power’s (2001) DSS frameworks (<http://www.dssresources.com>).

- **A data-driven DSS** focuses on the retrieval and manipulation of data that are stored in an organization’s data stores. Data warehouses (which we discuss in the next section) are often important data-driven DSSs. While these DSSs are useful, they do little to guide the decision maker in making the decision. So if the decision maker does not use the data properly, a poor decision is likely. However, in the case of unstructured decisions, a data-driven DSS may be particularly useful because of the amount of data retrieval required.
- **A model-driven DSS** focuses on providing the decision maker with the ability to access and manipulate analytical models. These models are used to help the decision maker perform sophisticated analysis that would be difficult and time-consuming without the DSS. Model-driven DSSs are appropriate for semistructured decisions. Without some degree of structure, it is difficult to build an appropriate model. A model-driven DSS can be applied to decisions in a wide variety of domains, including logistics, portfolio management, demand forecasting, and optimization.
- **A document-driven DSS** focuses on managing and retrieving documents that may help with decision making. The term *documents* should be taken broadly to include chat session transcripts, graphics, and even video and audio files. Document-driven DSSs are particularly useful for less structured decisions. Because there is no analytical aspect of document-driven DSSs, they draw heavily on the decision maker’s analytical ability and cognitive models.
- **A communication-driven DSS** facilitates collaboration and group-based decision making. According to Power (2001), communication-driven DSSs support one or more of the following: communication, information sharing, collaboration, and/or group-based decision making. Groupware, which we discuss next, is one type of

communication-driven DSS. Email, document sharing, coediting systems (such as Google Docs), and remote meeting systems are other examples.

Groupware is a network-based system that helps workgroups communicate and collaborate. Time and place are often used to categorize groupware. *Synchronous* and *asynchronous* describe whether the users collaborate at the same time (synchronous) or at different times (asynchronous). When group members are in the same physical location, they are colocated. [Figure 14.6](#) uses the dimensions of time and place to categorize common groupware applications, which are described following the figure.

	Same time (synchronous)	Different time (asynchronous)
	Group decision support systems (decision room), presentation support	
Place	Group decision support systems (remote), videoconferencing, chat, remote presentation, shared whiteboards	Discussion databases, email, email lists, word document coediting

FIGURE 14.6 Groupware Examples

- *Group decision support systems:* Group decision support systems (GDSSs) facilitate group-based decision-making tasks. GDSSs often include applications for brainstorming, anonymous commenting, and voting. The goal of GDSSs is to make group decision making more rational by supporting established group methods that encourage equal participation. Some organizations have “decision rooms,” which consist of individual computers that access GDSS software, along with shared devices, such as projection systems. GDSSs can also be used remotely.
- *Shared whiteboards:* Whiteboards have long been used to help workgroups communicate. You have probably used one yourself. Shared whiteboard systems allow users who are not colocated to share drawings or notes in the same way. Often, shared whiteboard systems assign different colors to each user so that you can tell who is drawing each element.
- *Videoconferencing:* Videoconferencing allows individuals to communicate using both voice and video. Videoconferencing systems range from free services such as Skype that you can access through your personal computer to dedicated rooms that have special equipment and software installed. Capability and quality vary widely from the simple desktop systems to the dedicated videoconferencing rooms.
- *Chat systems:* Online chat systems allow users to write real-time messages in a public space. (Note that we are specifically referring to group-oriented chat systems.) Some systems allow for a moderator to lead the interaction. Many chat systems capture a transcript of a session, which can be useful for documentation purposes.
- *Remote presentation:* Remote presentation software allows noncolocated groups to view a presentation remotely. These systems often have a chat window that allows the presenter and remote audience to interact.
- *Email and email lists:* Email is one of the simplest groupware applications. Most of us have used email to distribute documents or ideas to a group. Email lists facilitate group communication by making broadcasting emails to the group easier. Some systems allow you to subscribe to an email list. These often let you choose whether you want to see each individual message or periodically receive digests of messages that show all messages sent to the group in a single email message.
- *Discussion databases:* Similar to discussion forums, discussion databases store threaded, online, asynchronous discussions in a way that allows users to search and retrieve relevant information. These are different from chat session transcripts in that discussion databases are oriented toward asynchronous discussions. Discussion databases are particularly useful for new group members who need to come up to speed on the group’s discussions.
- *Workflow systems:* Workflow systems route documents through a group in a relatively predetermined manner. Workflow systems ensure that documents are routed properly so that the relevant group members are provided with documents in a timely manner. These systems also make sure that the proper authorities within the group review the documents.
- *Document coediting:* Document coediting systems, which we discussed earlier, help groups with their work by allowing group members to work on documents synchronously rather than having to email documents back and forth (or otherwise share them). These systems also help with versioning by having all members work on the same

version of a document. (If you have ever spent time editing the wrong version of a document, you will appreciate the importance of versioning.) While we list document coediting in the “asynchronous” column of [Figure 14.6](#), most systems allow for simultaneous coediting.

It is important to understand that DSSs support decision making. The decision maker’s knowledge is still critical to the decision-making process. The DSS provides tools that help the decision maker operate more efficiently and effectively, but the DSS does not replace the decision maker.

Business Intelligence

Organizations are drowning in a sea of information. A major goal of this book is to help you understand how organizations are trying to cope with the ever-increasing amount of information. Managers know that this information potentially represents a gold mine of value but are often unsure how to transform the raw material into an information treasure. Business intelligence (BI) systems may hold the key to unearthing the value of the information.

Business intelligence is set of applications, technologies, and processes for gathering, storing, analyzing, and accessing data to help users make better business decisions. Often, BI combines two sets of technologies, data warehousing and data mining, to help managers leverage the organization’s data resources for better decision making. [Figure 14.7](#) illustrates how data warehousing and data mining combine with transactional systems to enable BI.

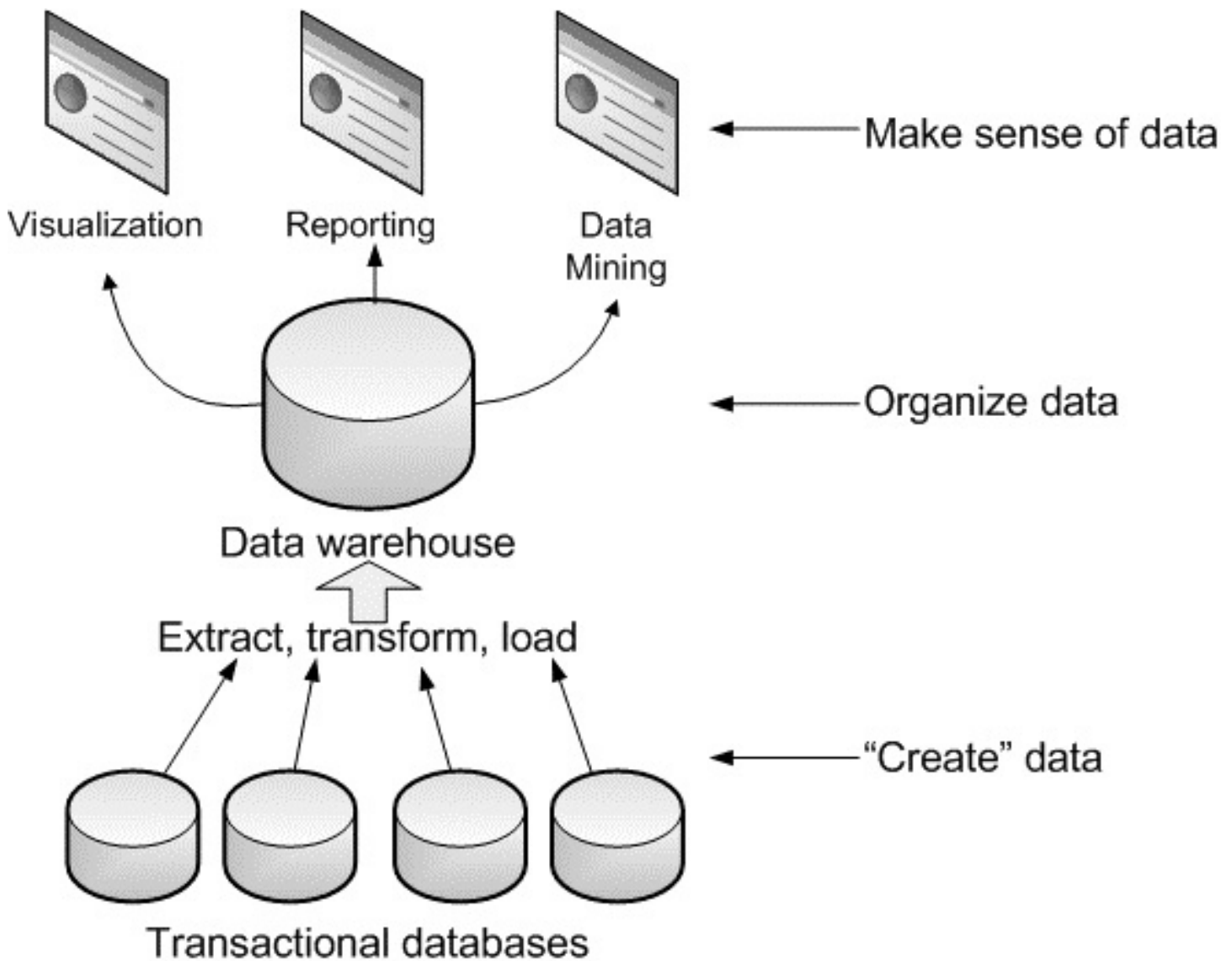


FIGURE 14.7 Business Intelligence Framework

The goal of BI is to help managers make sense of data. To get to that level, the data first must be generated. Transactional databases “create” the data. (Data may also come from other sources, such as external systems and databases, but most will come from the organization’s internal transactional systems.) The data from the transactional databases are put into the data warehouse by a process called extract, transform, and load (E/T/L), which we discuss later. The data warehouse stores and organizes the data in a way that is better suited for supporting decision making. Analysts and managers use data mining tools make sense of the data stored in the data warehouse.

Business intelligence tools help many different types of organizations reduce spending and increase sales. BI software helped eHarmony evaluate the effectiveness of their marketing program, causing them to save \$5 million by eliminating an affiliate program that only provided low-quality traffic. Toyota used BI tools to save more than \$800,000 by eliminating double payments to shippers. American Airlines used BI to save \$5 million by detecting fraudulent ticket sales. There are many similar examples (<http://www.cio.com/article/2845557/mobile-application-management/business-intelligence-meets-mobility-at-eharmony.html>; http://www.thebusinessintelligenceguide.com/industry_solutions/airline/Americian_Airlines.php, <http://smallbusiness.chron.com/advantages-business-intelligence-24548.html>).

Data Warehousing

Data warehouses support decision making. Understanding this is a key to understanding the purpose of data warehousing. Supporting transactions requires that databases perform many data additions, deletions, and updates. Decision support, in contrast, is more about data retrieval. Unfortunately, a database that is very efficient for data updates usually does not perform as well for data retrieval. There is another problem: decision making often requires getting data from multiple transaction databases. Finally, transaction databases usually store data at a very detailed level. Aggregated data are often better for decision making. So gathering all the data necessary for decision making can be time consuming and inefficient. Data warehousing addresses these issues. Data warehousing is a process, the goal of which is to gain value from an organization's information through the use of data warehouses. A **data warehouse** is a copy of transactional data (and other data) that is formatted so that it is useful for decision support.

Data warehouses have several characteristics that set them apart from transactional databases:

- Data warehouses are subject oriented. They are organized around particular subjects such as marketing, human resources, sales, or production.
- Data in data warehouses are integrated from a variety of internal and external sources.
- Data in data warehouses are typically transformed from their original format. Detailed data are often aggregated. For example, a data warehouse for a restaurant chain would aggregate individual sales into total sales from some time period (such as per hour).
- Data in data warehouses typically are nonvolatile, which means that the data do not change. Once data are in the warehouse, they stay in the warehouse and are not changed. (Data that are no longer of value may be deleted from the warehouse.)

Data from various sources are gathered together, prepared, and loaded into the data warehouse through the extract, transform, load (E/T/L) process, as mentioned earlier. The E/T/L process is easy to understand conceptually but is often very complex and time consuming to perform in practice. Each element is described below.

- *Extract:* Data are pulled from the source systems (such as the transactional databases). Deciding exactly what data to extract is important.
- *Transform:* Data must be changed into a form that is suitable for decision support. Often this involves aggregating detailed data. Data cleansing is also an important part of the transform process. Data in transactional databases are often messy. This problem gets worse when data are extracted from multiple systems. These messy data must be cleaned up before being loaded into the warehouse. Think about all the ways a company such as AT&T could be represented in different databases: AT&T, ATT, American Telephone and Telegraph, American Tel and Tel, AT and T, and so on. All these need to be recognized as the same company; otherwise, you could make decisions based on faulty data. Data cleansing is often complicated and expensive.
- *Load:* The cleaned data needs to be put into the data warehouse. This must be repeated periodically. Figuring out how often data should be loaded can be difficult. It primarily depends on how up to date the data need to be in order to support good decision making. The more time-critical the data, the more frequent the loads.

Once you have the data in the data warehouse, you need to be able to retrieve and analyze in order to gain value from the information. Data mining can help with this.

Data Mining

Data mining is the process of analyzing data to identify trends, patterns, and other useful information. Data mining typically involves applying statistical techniques to identify trends and patterns. Some people consider querying and visualization to be related to data mining. Since we covered those topics in earlier chapters, the focus here is on statistical data mining.

Wouldn't it be nice to be able to predict the future? That is a goal of data mining. Data mining techniques seek to take large amounts of data and form predictions based on the data. There are wide applications of data mining

in areas ranging from business to picking players in a pro sports draft. The basic process of data mining is shown in [Figure 14.8](#). Existing data are analyzed using the appropriate data mining technique to build a predictive model. The new model is then applied to new data to make a prediction.

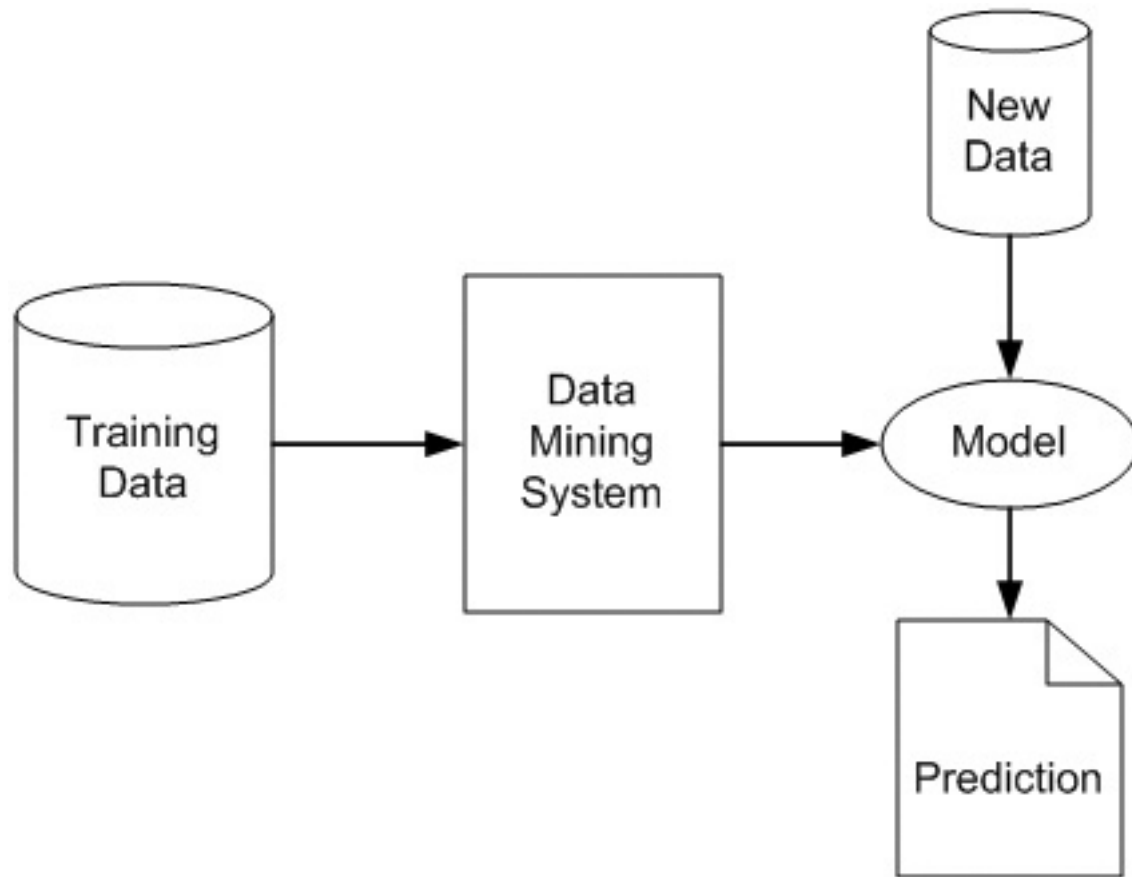


FIGURE 14.8 High-Level View of Data Mining

Source: Adapted from http://www.thearling.com/dmintro/dmintro_2.htm/.

While data mining uses many statistical techniques, it is important to understand the difference between traditional statistical analysis and data mining. In most traditional statistical analyses, you create a model (such as a regression equation) and then test that model using data. Essentially, you have a hypothesis and then use data and statistical analysis to test that hypothesis. While this is often effective, it is limited by your knowledge and creativity. You can only test what you can hypothesize. Data mining can help overcome these limitations. In data mining, the emphasis is on discovering the model and then testing the validity of the model. Statistical techniques are used to uncover the relationships in the data that lead to the model. [Table 14.3](#) shows common data mining techniques with descriptions and examples.

TABLE 14.3 Common Data Mining Techniques

Technique	Description	Example
Association detection	Discovering patterns in which multiple events are connected	Customers tend to purchase eggs
Sequence analysis	Discovering when one event leads to another event	A student graduates from college
Classification	Dividing data into mutually exclusive groups based on the variable you want to predict	Students are classified according to whether they drop out.
Clustering	Dividing data into mutually exclusive groups using all available data (not just the variable you want to predict)	Hotel guests are grouped according to their stay length.

Data mining has many applications in business. You may have talked about customer segmentation in a marketing class. Customer groups (segments) can be built through cluster analysis. Cluster analysis divides information into mutually exclusive groups. (Each member can be in at most one group.) The goal is to build the groups so that each member in a group is as close as possible to every other member of the group and the different groups are as different as possible. For example, a hotel chain might use cluster analysis to segment customers into different groups, such as short-stay business customers, vacationers, and long-stay business customers. Advertisements could then be tailored to each of these customers, which should increase the ads' effectiveness. CRM systems can use cluster analysis to customize product or service offerings.

Market basket analysis identifies affinities among customers' product or service offerings. Retailers often use checkout scanner data to identify products that customers tend to buy together. For example, a restaurant might determine that customers who order wine typically buy dessert, while beer drinkers usually buy appetizers. The restaurant could develop special offerings based on this information. Market basket analysis is an example of association detection. Association examines the degree to which variables in a data set are related by considering the frequency with which the variables occur together.

Have you ever played the 20-questions game? If so, you have some familiarity with the concept of decision trees, which are a classification technique. A decision tree makes a prediction based on a series of questions. The next question in the series depends on the answer to the current question. You might have concluded that decision trees are useful devices, since we have discussed them twice in this chapter. Earlier, we discussed decision trees as a method for knowledge capture. Here the focus is on prediction rather than knowledge capture.

There are many other data mining techniques, including statistical methods such as regression analysis, time series analysis, neural networks, and text analysis. As we mentioned earlier, statistical analysis emphasizes testing preexisting models, while data mining tries to discover the models. Many of the same statistical techniques can be applied to both.

Reporting and data visualization tools (discussed in [Chapter 6](#)) are also considered by some to be data mining tools. (There is some debate about this.) These tools help you quickly build different views of your data. In some cases, these views are in the form of visualizations, while in other cases, they are built around numbers and text. Spreadsheet pivot tables are an example. Pivot tables allow you to see multidimensional views of a data set. For example, [Figure 14.9](#) shows sales data from a small retail clothing chain. The data in this figure show the total revenue for each store, broken down by state and quarter.

	A	B	C	D	E	F	G
1							
2							
3	Sum of Sales revenue	Column Labels					
4	Row Labels	Q1	Q2	Q3	Q4	Grand Total	
5	California	1,899,680.30	1,760,147.80	1,930,516.50	1,889,224.70	7,479,569.30	
6	e-Fashion San Francisco	770,502.70	779,742.50	822,383.60	886,011.70	3,258,640.50	
7	e-Fashion San Diego	1,129,177.60	980,405.30	1,108,132.90	1,003,213.00	4,220,928.80	
8	Colorado	525,682.20	500,076.00	510,776.90	523,740.10	2,060,275.20	
9	e-Fashion Dillion	525,682.20	500,076.00	510,776.90	523,740.10	2,060,275.20	
10	DC	766,821.70	706,446.60	692,258.20	796,423.40	2,961,949.90	
11	e-Fashion Washington Midtown	766,821.70	706,446.60	692,258.20	796,423.40	2,961,949.90	
12	Florida	515,687.70	489,997.80	387,809.70	485,663.30	1,879,158.50	
13	e-Fashion Miami Beach	515,687.70	489,997.80	387,809.70	485,663.30	1,879,158.50	
14	Illinois	846,408.40	850,595.00	610,765.20	714,889.80	3,022,658.40	
15	e-Fashion Chicago Loop	846,408.40	850,595.00	610,765.20	714,889.80	3,022,658.40	
16	Massachusetts	312,896.40	291,431.00	249,529.00	429,850.20	1,283,706.60	
17	e-Fashion Boston Newbury	312,896.40	291,431.00	249,529.00	429,850.20	1,283,706.60	
18	New York	1,987,114.70	2,028,090.70	1,672,580.70	1,894,434.50	7,582,220.60	
19	e-Fashion New York 5th	804,084.40	795,193.60	637,277.10	723,811.40	2,960,366.50	
20	e-Fashion New York Midtown	1,183,030.30	1,232,897.10	1,035,303.60	1,170,623.10	4,621,854.10	
21	Texas	2,875,569.20	2,499,276.80	2,146,302.80	2,596,515.50	10,117,664.30	
22	e-Fashion Dallas	555,458.70	450,588.30	467,925.90	496,061.30	1,970,034.20	
23	e-Fashion Houston	614,284.60	560,650.20	465,677.10	662,570.90	2,303,182.80	
24	e-Fashion DFW	775,482.70	667,850.30	581,470.40	674,869.80	2,699,673.20	
25	e-Fashion Houston Downtown	930,343.20	820,188.00	631,229.40	763,013.50	3,144,774.10	
26	Grand Total	9,729,860.60	9,126,061.70	8,200,539.00	9,330,741.50	36,387,202.80	
27							
28							
29							

FIGURE 14.9 Pivot Table Example

You can quickly modify the dimensions by which you view the data. Suppose you want to add product categories to the analysis. In a matter of seconds, you can modify the pivot table to include the new dimension, as shown in [Figure 14.10](#). (Note that only a portion of the table is shown in the figure.) The flexibility of pivot tables makes them ideal reporting and analysis tools for many common business decisions. You can learn how to build pivot tables in [Appendix G](#).

	A	B	C	D	E	F
3	Sum of Sales revenue	Column Labels				
4	Row Labels	Q1	Q2	Q3	Q4	Grand Total
5	California	1,899,680.30	1,760,147.80	1,930,516.50	1,889,224.70	7,479,569.30
6	e-Fashion San Francisco	770,502.70	779,742.50	822,383.60	886,011.70	3,258,640.50
7	2 Pocket shirts	27,876.20	33,324.60	30,122.00	31,773.80	123,096.60
8	Belts,bags,wallets	49,517.90	40,896.40	17,621.40	29,908.20	137,943.90
9	Bermudas	994.90		340.30	4,883.40	6,218.60
10	Boatwear	11,091.60	2,065.60	2,040.30	8,949.70	24,147.20
11	Cardigan	36,084.10	22,446.50	14,003.60	1,176.40	73,710.60
12	Casual dresses	4,293.20	4,458.50	12,908.10	5,014.70	26,674.50
13	Day wear	4,344.90	28,676.30	29,980.00		63,001.20
14	Dry wear	1,396.10		6,236.20	10,935.60	18,567.90
15	Evening wear	26,296.00	4,699.80	32,976.70	101,981.50	165,954.00
16	Fancy fabric	4,758.00	3,607.60	3,646.70	4,964.70	16,977.00
17	Full length	1,935.50		4,459.90	15,833.50	22,228.90
18	Hair accessories	4,852.80		3,388.10	7,065.60	15,306.50
19	Hats,gloves,scarves	66,386.40	24,783.20	19,091.00	3,175.00	113,435.60
20	Jackets			6,570.00	381.30	6,951.30
21	Jeans	4,238.70	1,711.80	5,678.80	10,353.60	21,982.90
22	Jewelry	185,083.10	209,951.90	43,683.00	1,815.20	440,533.20
23	Long lounge pants	970.80	424.60	5,234.90	7,961.90	14,592.20
24	Long sleeve	17,300.00	10,490.60	40,848.40	61,425.20	130,064.20
25	Lounge wear	6,423.70	16,771.60	16,017.80	5,639.40	44,852.50
26	Mini city	818.00	3,445.20	5,697.80	1,098.40	11,059.40
27	Night wear			1,837.80	2,846.00	4,683.80
28	Outdoor	3,151.00	3,503.40	7,544.60	6,310.50	20,509.50
29	Pants	572.90		1,831.60	946.20	3,350.70
30	Party pants	8,416.00	14,143.80	59,198.40	4,208.90	85,967.10
31	Samples	1,022.80	10,618.70	12,960.80	7,878.90	32,481.20

FIGURE 14.10 Pivot Table with Additional Dimension

One important point to keep in mind is that you should always assess whether your model and its predictions are reasonable. Many data mining techniques are based on mathematics; they are all about the numbers. The mathematics does not consider whether the underlying associations have any real meaning. That is where human interpretation and judgment come in.

CHAPTER SUMMARY

In this chapter, we discussed knowledge and the processes and tools that help organizations manage knowledge. We also helped you understand technologies that support decision making and that help organizations gain more value from their information resources. Here are the main points discussed in the chapter:

- Knowledge management is a process that allows organizations to generate value from their knowledge-based assets.
- Managing knowledge is important because knowledge is among the most important resources of any organization.
- Explicit knowledge can be easily expressed. Tacit knowledge is difficult to express and communicate.
- The main processes for knowledge management are create, capture, codify, store, retrieve, transfer, and apply.
- Information and communication technologies that facilitate knowledge management include knowledge repositories, communication and collaboration tools, executive information systems, dashboards, and expert systems.
- Decision support systems are computer-based systems that help decision makers use data and models to solve semistructured or unstructured problems.

- Business intelligence is a set of applications, technologies, and processes for gathering, storing, analyzing, and accessing data to help decision makers.
- Data warehouses and data mining systems are important business intelligence components.
- Data warehouses store and organize data for decision support.
- Data mining is the process of analyzing data to identify trends, patterns, and other useful information.

REVIEW QUESTIONS

1. Briefly explain how knowledge and information differ in the terms of ease of management and the level of human contribution.
2. Why is managing knowledge important to organizations?
3. State five benefits of effective knowledge management.
4. Contrast explicit and tacit knowledge.
5. Give an example of tacit knowledge.
6. Name and briefly describe the four types of knowledge resources described in the chapter.
7. Name the processes in the knowledge management cycle.
8. Briefly describe the four knowledge creation processes in the SECI model.
9. What is knowledge codification? Why is it important to knowledge management?
10. Compare and contrast decision tables and decision trees.
11. Explain why search technologies are important to knowledge management.
12. Give an example of each of the following: a knowledge repository and a communication-based knowledge management tool.
13. What is a digital dashboard?
14. Name and briefly describe the DSS categories described in the chapter.
15. Compare and contrast synchronous and asynchronous groupware.
16. Name and briefly describe the groupware examples discussed in the chapter.
17. What are the two main components of a business intelligence system? Briefly describe each component.
18. Describe the E/T/L process.
19. What is the purpose of data mining?
20. Name three data mining techniques.

REFLECTION QUESTIONS

1. What is the most important thing you learned in this chapter? Why is it important?
2. What topics are unclear? What about them is unclear?
3. What relationships do you see between what you learned in this chapter and what you have learned in earlier chapters?
4. The chapter focused on organizational knowledge management, but knowledge management is also important to individuals. (This is called personal knowledge management.) Why is knowledge management important to your personal and professional development?
5. Have you ever tried to explain to someone how you are able to do something (hit a golf ball, draw, study, etc.)? Was it easy or hard to explain? What about the knowledge you were trying to transfer determined whether it was easy or hard to explain?

6. In [Chapter 7](#), you learned about cloud computing. How can cloud computing facilitate knowledge management?
7. How does data warehousing facilitate data mining?
8. What is the relationship between business intelligence and knowledge management?
9. How is the need for quick decisions related to the need to make ethical decisions?

ADDITIONAL LEARNING ACTIVITIES

Learning Activity 14.A1

Describe a situation in which you used technology to access knowledge. Address the following in your description: What knowledge were you seeking? How did you go about finding the knowledge? What technologies did you use? How effective were they?

Learning Activity 14.A2

Form groups of two or three.

1. One of you (the explainer) will answer the following question: Why is knowledge management important to organizational success?
2. When the first person finishes, the other person (the questioner) will seek clarification and provide her or his own ideas.

Record and be prepared to share your answers.

Learning Activity 14.A3

Some music services, including Pandora and iTunes, can build smart playlists that use the songs in your library (or playlists) to build playlists that you will like. Research how these services work and prepare a one-page paper on how these services relate to the data mining tools you read about in this chapter.

Learning Activity 14.A4

Create a decision table or decision tree to document how you go about making the following decisions:

1. Deciding whether to take a class
2. Deciding which section of a class to take
3. Deciding on a major
4. Deciding whether to join a club

Learning Activity 14.A5

Partner with two other students. Create a wiki on how to choose which section of a multisection class to take. You can use Wikispaces (<http://www.wikispaces.com>), PK Works (<http://pbworks.com>), or any other wiki service to create your wiki. Be prepared to share your wiki with the class.

Learning Activity 14.A6

Research how companies are using data mining. Pick one example and prepare a one- to two-page report on how the company used data mining.

REFERENCES

- Alter, S. 1977. "Why Is Man-Computer Interaction Important for Decision Support Systems?" *Interfaces* 7(2): 109–15.
- Davenport, T., and L. Prusak. 1998. *Working Knowledge: How Organizations Manage What They Know*. Boston, MA: Harvard Business School Press.
- Nonaka, I., and H. Takeuchi. 1995. *The Knowledge Creating Company*. New York: Oxford University Press.
- Pearlson, K., and C. Saunders. 2006. *Managing and Using Information Systems*, 3rd ed. Hoboken, NJ: John Wiley & Sons.
- Power, D. 2001. "Supporting Decision-Makers: An Expanded Framework." In *E-Proceedings of the Informing Science Conference*, Krakow, Poland, edited by A. Harriger, June 19–22: 431–36.

FURTHER READINGS

- Courtney, J. 2001. "Decision-Making and Knowledge Management in Inquiring Organizations: Toward a New Decision-Making Paradigm for DSS." *Decision Support Systems* 31: 17–38.

GLOSSARY

- Business intelligence:** A set of applications, technologies, and processes for gathering, storing, analyzing, and accessing data to help users make better business decisions.
- Codifying knowledge:** Converting tacit and explicit knowledge into a form that organizational members can use.
- Cognitive map:** A graphical representation of a mental model of an expert's knowledge.
- Communication-driven decision support system:** A DSS that facilitates collaboration and group-based decision making.
- Community of practice:** A group of people who share a common interest, usually in a craft or profession, and who interact to share knowledge.
- Conceptual knowledge:** Explicit knowledge that is embodied in language, symbols, and images.
- Data-driven decision support system:** A DSS that focuses on the retrieval and manipulation of data that is stored in an organization's data stores.
- Data mining:** The process of analyzing data to identify trends, patterns, and other useful information to make predictions.
- Data warehouse:** A copy of transactional data (and other data) that is formatted so that it is useful for decision support.
- Decision support systems:** Computer-based systems that help decision makers use data and models to solve semistructured or unstructured problems.
- Decision table:** A list of conditions and their values along with a list of conclusions or actions.

Decision tree: A diagram that shows alternate paths that impact decisions.

Digital dashboards: Computer-based systems that provide graphical views of key data along with graphical warnings when data indicate areas that need attention.

Document-driven decision support system: A DSS that facilitates the management and retrieval of documents that may help with decision making.

Executive information systems (EISs): Information systems that help provide high-level managers with the information they need to monitor business activities and make decisions.

Experiential knowledge: Tacit knowledge that can be shared through common experiences and interpersonal communication.

Expert systems: Systems that help users solve problems or answer questions in a way that mimics an expert's thought processes.

Explicit knowledge: Knowledge that can be expressed relatively easily.

Groupware: A network-based system that helps workgroups communicate and collaborate.

Knowledge management: The process by which organizations create, capture, store, apply, and protect knowledge to achieve organizational objectives.

Knowledge repositories: Tools that make it easy to find and retrieve documents that contain knowledge.

Model-driven decision support system: A DSS that provides the decision maker with the ability to access and manipulate analytical models.

Routine knowledge: Tacit knowledge that is embedded in the organization's practices.

Systemic knowledge: Explicit knowledge that has been systemized and packaged.

Tacit knowledge: Internalized and highly individualized knowledge that is difficult to express or communicate.