CHAPTER EIGHT OUTLINE

STUDENT LEARNING OUTCOMES

1. Define ethics and describe the two factors that affect how you make a decision concerning an ethical issue.
2. Define and describe intellectual property, copyright, Fair Use Doctrine, and pirated software.
3. Define privacy and describe ways in which it can be threatened.
4. Describe the ways in which information on your computer or network is vulnerable and list measures you can take to protect it.

PERSPECTIVES

WEB SUPPORT

www.mhhe.com/haag

- Exploring Google Earth
- Protecting your computer against viruses
- Searching for shareware and freeware
- Ethical computing guidelines
- Privacy laws and legislation

SUPPORTING MODULES

XLM/E Network Basics
Extended Learning Module E provides an introduction to the vast, exciting, and dynamic field of information technology networks. The module includes discussions of what is needed to set up a small network at home, the components used to build large business networks, Internet connection possibilities, types of communications media, and network security.

XLM/H Computer Crime and Digital Forensics
Extended Learning Module H provides an overview of computer and computer-aided crime and its investigation. First, you'll read about the various types of computer crime, malware, and hackers. Next, you'll explore digital forensics starting with the investigation process. You'll learn about the digital forensics software and hardware that experts use along with the anti-forensics measures that the bad guys employ.

CHAPTER EIGHT

Protecting People and Information

Threats and Safeguards

OPENING CASE STUDY: THEY KNOW ABOUT 96 PERCENT OF AMERICAN HOUSEHOLDS

There's a company in Little Rock, Arkansas, called Acxiom, that handles consumer information, mainly for marketing purposes. That is to say, Acxiom stores and analyzes information, both its own and its clients'. Acxiom gets the information it sells from many sources, including the three major credit bureaus (TransUnion, Equifax Inc., and Experian Inc.). Nine of the country's 10 largest credit-card issuers are clients along with many other high profile financial companies in the banking and insurance industries. Forty percent of Acxiom's revenue comes from banking alone.

The company's inventory includes 20 billion records on consumers that include names, addresses, Social Security numbers, and public-record information. In fact, Acxiom has a database with information on about 110 million Americans, or 96 percent of U.S. households. The company categorizes consumers into one of 70 lifestyle clusters that include such groups as "Rolling Stones," "Single City Struggles," and "Timeless Elders."

To help clients react quickly to changing market conditions, Acxiom offers hundreds of lists. One of these is a daily updated "pre-movers file" which lists people who are about to change residences. Another list is of people who use credit cards, and the list is sorted in order of frequency of use.

For example, Capital One Financial Corporation, a financial services company based in Virginia, spent $290 million (about 14 percent of its revenue) on marketing for the last quarter of 2003. The company sends out about 1 billion pieces of mail every year that largely consist of advertising intended to entice consumers to sign up for credit cards. Acxiom's information and analysis help Capital One send credit card solicitations only to those who are likely to want another credit card.

Another service that Acxiom provides is the merging of huge databases. The merger of Bank One and J. P. Morgan is a case in point. Both companies had huge, independent databases, and merging such mountains of information is Acxiom's specialty. First the information must be cleaned (called "data hygiene" in the industry), that is, duplicate records must be identified and combined. Acxiom also adds records from its own database to those of its clients, complementing and completing the clients' customer information.

Acxiom is only one of the many companies that collect and sell data on consumers.[1,2,3,4]

Questions

1. Do you feel comfortable about so many people collecting information about you and distributing it freely?
2. Is it an invasion of your privacy or just good business?
3. Should there be any laws regulating the collection and use of data by data brokers like Acxiom?

Introduction

As you know, the three components of an IT system are people, information, and information technology. Most of what you've seen in previous chapters has dealt with IT and how it stores and processes information. In this chapter we're going to concentrate on information—its use, ownership, and protection. The best environment for handling information is one that has stability without stagnation and change without chaos.

To handle information in a responsible way you must understand

- The importance of ethics in the ownership and use of information.
- The importance to people of personal privacy and the ways in which it can be compromised.
- Threats to information and how to protect against them (security).

The most important part of any IT system consists of the people who use it and are affected by it. How people treat each other has always been important, but in this information-based and digital age, with huge computing power at our fingertips, we can affect more people's lives in more ways than ever before. How we act toward each other, and this includes how we view and handle information, is largely determined by our ethics.

You don't have to look far to see examples of computer use that is questionable from an ethical viewpoint. For example,

- People copy, use, and distribute software they have no right to.
- Employees search organizational databases for information on celebrities and friends.
- Organizations collect, buy, and use information and don't check the validity or accuracy of that information.
- Misguided people create and spread viruses that cause trouble for those using and maintaining IT systems.
- Information system developers put systems on the market before they're completely tested. A few years ago, the developers of an incubator thermostat control program didn't test it fully, and two infants died as a result.[5]
- Unethical people break into computer systems and steal passwords, information, and proprietary information.
- Employees destroy or steal proprietary schematics, sketches, customer lists, and reports from their employers.
- People snoop on each other and read each other's e-mail and other private documents.

LEARNING OUTCOME 1

Ethics

Ethical people have integrity. They're people who are just as careful of the rights of others as they are of their own rights. They have a strong sense of what's fair and right and what isn't. But even the most ethical people sometimes face difficult choices.

Ethics are the principles and standards that guide our behavior toward other people. Acting ethically means behaving in a principled fashion and treating other people with respect and dignity. It's simple to say, but not so simple to do since some situations are complex or ambiguous. The important role of ethics in our lives has long been recognized. As far back as 44 B.C., Cicero said that ethics are indispensable to anyone who

wants to have a good career. Having said that, Cicero, along with some of the greatest minds over the centuries, struggled with what the rules of ethics should be.

Our ethics are rooted in our history, culture, and religion, and may stay the same and yet also shift over time. In this electronic age there's a new dimension in the ethics debate—the amount of personal information that we can collect and store, and the speed with which we can access and process that information.

TWO FACTORS THAT DETERMINE HOW YOU DECIDE ETHICAL ISSUES

How you collect, store, access, and use information depends to a large extent on your sense of ethics—what you perceive as right and wrong. Two factors affect how you make your decision when you're faced with an ethical dilemma. The first is your basic ethical structure, which you developed as you grew up. The second is the set of practical circumstances inevitably involved in the decision that you're trying to make, that is, all the shades of gray in what are rarely black or white decisions.

Your ethical structure and the ethical challenges you'll face exist at several levels (see Figure 8.1).[6] At the outside level are things that most people wouldn't consider bad, such as taking a couple of paper clips or sending an occasional personal e-mail on company time. Do these things really matter? At the middle level are more significant ethical challenges. One example might be accessing personnel records for personal reasons. Could there ever be a personal reason so compelling that you would not feel ethical discomfort doing this? Reading someone else's e-mail might be another middle-level example. At the innermost ethical level are ethical violations that you'd surely consider very serious, such as embezzling funds or selling company records to a competitor. And yet, over time, your ethical structure can change so that even such acts as these could seem more or less acceptable. For example, if everyone around you is accessing confidential records for their own purposes, in time you might come to think such an act is no big deal. And this might spell big trouble for you.

It would be nice if every decision were crystal clear, such as in the innermost circle in Figure 8.1, but ethical decisions are seldom so easy. Ideally, your personal ethics should

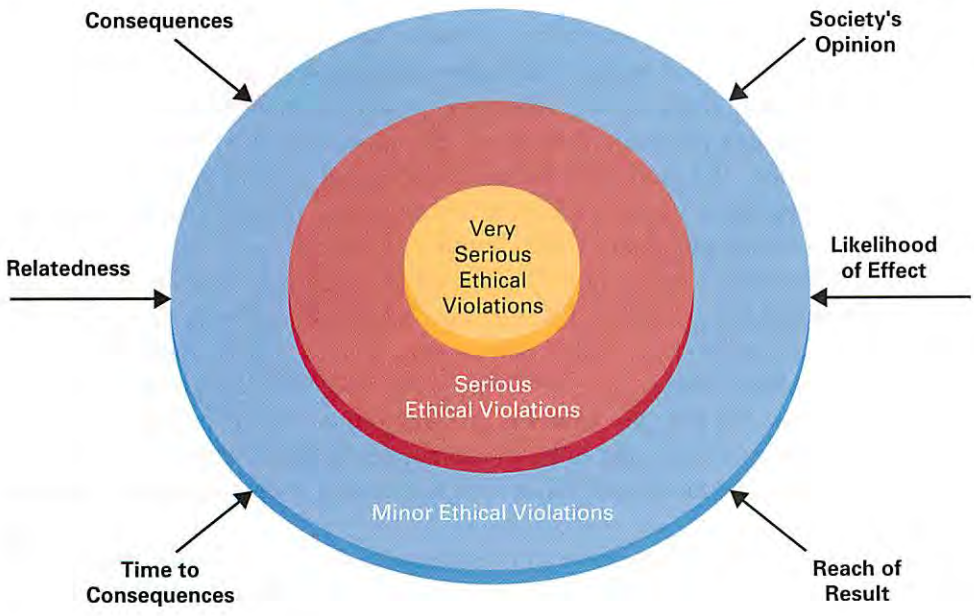


Figure 8.1
Your Ethical Structure

tell you what to do. But the practical circumstances of a decision inevitably also influence you in an ethical dilemma:[7]

1. *Consequences.* How much or how little benefit or harm will come from a particular decision?
2. *Society's opinion.* What is your perception of what society really thinks of your intended action?
3. *Likelihood of effect.* What is the probability of the harm or benefit that will occur if you take the action?
4. *Time to consequences.* How long will it take for the benefit or harm to take effect?
5. *Relatedness.* How much do you identify with the person or persons who will receive the benefit or suffer the harm?
6. *Reach of result.* How many people will be affected by your action?

No matter how strong your sense of ethics is, these practical aspects of the situation may affect you as you make your decision—perhaps unduly, perhaps quite justifiably. Thus, ethical dilemmas usually arise not out of simple situations but from a clash between competing goals, responsibilities, and loyalties. Ethical decisions are complex judgments that balance rewards for yourself and others against responsibilities to yourself and others. Inevitably, your decision process is influenced by uncertainty about the magnitude of the outcome, by your estimate of the importance of the situation, sometimes by your perception of conflicting "right reactions," and more than one socially acceptable "correct" decision.

LEARNING OUTCOME 2

INTELLECTUAL PROPERTY

An ethical issue you will almost certainly encounter is one related to the use or copying of proprietary software. Software is a type of intellectual property. ***Intellectual property*** is intangible creative work that is embodied in physical form.[8] Music, novels, paintings, and sculptures are all examples of intellectual property. So also are your company's product sketches and schematics and other proprietary documents. These documents along with music, novels, and so on are worth much more than the physical form in which they are delivered. For example, a single U2 song is worth far more than the CD on which it's purchased. The song is also an example of intellectual property that is covered by copyright law.

Copyright law protects the authorship of literary and dramatic works, musical and theatrical compositions, and works of art. ***Copyright*** is the legal protection afforded an expression of an idea, such as a song, video game, and some types of proprietary documents. Having a copyright means that no one can use your song or video game without your permission. As a form of intellectual property, software is usually protected by copyright law, although sometimes it falls under patent law, which protects an idea, such as the design of a sewing machine or an industrial pump valve.

Copyright law doesn't forbid the use of intellectual property completely. It has some notable exceptions. For example, a TV program could show a video game you created without your permission. This would be an example of the use of copyrighted material for the creation of new material, i.e., the TV program. And that's legal; it falls under the Fair Use Doctrine. The ***Fair Use Doctrine*** says that you may use copyrighted material in certain situations, for example, in the creation of new work or, within certain limits, for teaching purposes. One of those limits is on the amount of the copyrighted material you may use.

Generally, the determining factor in legal decisions on copyright disputes is whether the copyright holder has been or is likely to be denied income because of the

infringement. Courts will consider factors such as how much of the work was used and how, and when and on what basis the decision was made to use it.

Remember that copyright infringement is *illegal.* That means it's against the law, outside of a fair use situation, to simply copy a copyrighted picture, text, or anything else without permission, whether the copyrighted material is on the Internet or not. In particular, it's illegal to copy copyrighted software. But there's one exception to that rule: In the United States, you may always make one copy of copyrighted software to keep for backup purposes. When you buy copyrighted software, what you're paying for is the right to use it—and that's all.

How many more copies you may make depends on the copyright agreement that comes with the software package. Some software companies state emphatically that you may not even put the software on a second computer, even if they're both yours and no one else uses either one. Other companies are less restrictive, and agree to let you put a copy of software on multiple machines—as long as only one person is using that software package at any given time. In this instance, the company considers software to be like a book in that you can have it in different places and you can loan it out, but only one person at a time may use it. Music companies often allow three copies of a CD or individual music track to be played on different platforms, like your computer, your stereo system, and your MP3 player.

If you copy copyrighted software and give it to another person or persons, you're pirating the software. ***Pirated software*** is the unauthorized use, duplication, distribution, or sale of copyrighted software.[9] Software piracy costs businesses an estimated $12 billion a year in lost revenue. Microsoft gets more than 25,000 reports of software piracy every year, and the company reportedly follows up on all of them. Countries that experience the greatest losses are (in rank order) the United States, Japan, the United Kingdom, Germany, China, France, Canada, Italy, Brazil, and the Netherlands. One in four business applications in the United States is thought to be pirated.[10] In some parts of the world, more than 90 percent of business software is pirated. The Software and Information Industry Association (SIIA) and the Business Software Alliance (BSA) say that pirated software means lost jobs, wages, and tax revenues, and is a potential barrier to success for software start-ups around the globe.

Privacy

LEARNING OUTCOME 3

Privacy is the right to be left alone when you want to be, to have control over your own personal possessions, and not to be observed without your consent. It's the right to be free of unwanted intrusion into your private life. Privacy has several dimensions. Psychologically, it's a need for personal space. All of us, to a greater or lesser extent, need to feel in control of our most personal possessions, and personal information belongs on that list. Legally, privacy is necessary for self-protection.[11] If you put the key to your house in a special hiding place in your yard, you want to keep that information private. This information could be abused and cause you grief. In this section, we'll examine some specific areas of privacy: individuals snooping on each other; employers' collection of information about employees; businesses' collection of information about consumers; government collection of personal information; and the issue of privacy in international trade.

PRIVACY AND OTHER INDIVIDUALS

Other individuals, like family members, associates, fellow employees, and hackers, could be electronically invading your privacy. Their motives might be simple

curiosity, an attempt to get your password, or to access something they have no right to. Obviously, there are situations in which you're well within your rights, and would be well advised to see what's going on. Examples may be if you suspect that your child is in electronic contact with someone or something undesirable, or if you think that someone is using your computer without permission. Many Web sites are offering programs, collectively referred to as snoopware, to help people monitor what's happening on a computer.

For general snooping you can get key logger software and install it on the computer you want to monitor. ***Key logger,*** or ***key trapper, software,*** is a program that, when installed on a computer, records every keystroke and mouse click. It records all e-mail (whether you're using Eudora or Microsoft Outlook), instant messages, chat room exchanges, Web sites you visit, applications you run, and passwords you type in on that computer.

Also available for monitoring computer use are screen capture programs that periodically record what's on the screen. (They get the information straight from the video card.) These programs don't trap every single screen, just whatever is on the screen when the capturing program activates. But they still give whoever is doing the monitoring a pretty good idea of what the computer user is up to. Other tools for monitoring include packet sniffers (that examine the information passing by) on switches, hubs, or routers (the devices on networks that connect computers to each other), and log analysis tools that keep track of logons, deletions, and so forth.

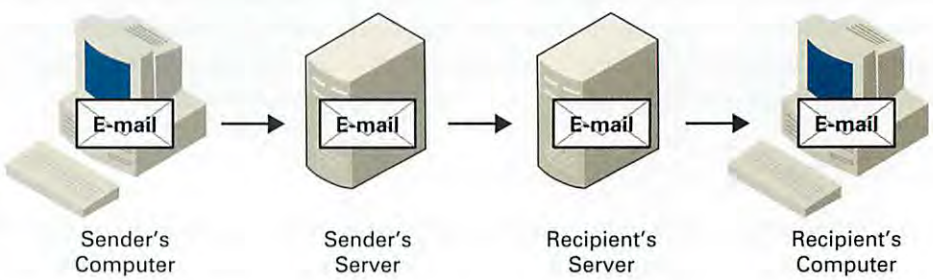
As you're probably already aware, e-mail is completely insecure. E-mail content might as well be written on a postcard for all the privacy it has. Not only that, but each e-mail you send results in at least three or four copies being stored on different computers (see Figure 8.2). It's stored first in the computer you're using. Second, it's stored by the e-mail server, the computer through which it gets onto the Internet. Third, it's stored on the recipient's computer, and may also be archived on the recipient's e-mail server.

While you probably realize that your e-mail is not totally private, do you realize that other electronic output leaves its mark too? For example, if you use a color laser printer, your printouts have patterns of yellow dots on the back that are not visible unless you have a blue light and a microscope. These dots identify the model and serial number of your printer and the time the printout was made. Printer manufacturers introduced this feature at the request of the Secret Service, which is the agency responsible for investigating counterfeit currency.

Another example is those photos you take with your digital camera. With the right software you can load the photo and see a whole block of information like the date the photo was taken, the camera type and serial number, whether the owner of the camera signed up for a warranty, and various other details. Your CD burner leaves a distinct signature on the CDs you burn. That is, any CD that your computer burns can be traced back to your CD drive. Of course, it stands to reason that your cell phone, when it's on,

Figure 8.2

The E-Mail You Send Is Stored on Many Computers



that you are diverted to the fake site either before or after you access the real one. It works so well because it's very hard to spot the fake site.

One of the most worrying types of identity theft is medical record theft. Someone who steals your medical records to get medical care will most likely add to or change your records so that when you need care your records are not accurate. This could lead to your getting medication that you're allergic to or not getting a procedure that you need. According to the World Privacy Forum (WPF) almost 20,000 people filed complaints about theft of their medical records between January 1992 and April 2006. Again, according to the WPF, about $100 billion dollars of health care costs are the result of health care fraud. More than 600 health identity theft cases were tried in 2005 and 516 of those people were convicted. See Figure 8.4 for some advice from the Federal Trade Commission regarding identity theft.

PRIVACY AND EMPLOYEES

Companies need information about their employees and customers to be effective in the marketplace. But people often object to having so many details about their lives available to others. If you're applying for a job, you'll most likely fill out a job application, but that's not the only information a potential employer can get about you. For a small fee, employers, or anyone else, can find out about your credit standing, your telephone usage, your insurance coverage, and many other interesting things. An employer can also get information on what you said on the Internet from companies who collect and collate

Some Facts on Phishing . . .

- In January 2004 there were 198 phishing sites, but by February 2005 that number had risen to 2,625, according to the Anti-Phishing Working Group.
- The same group says that the number of unique phishing e-mails reached 13,141 in February of 2004.
- Symantec says that its Brightmail spam filters blocked an average of 33 million phishing attempts per week in December 2004, compared to an average of only 9 million during the previous July.
- The Phemon Institute says consumers lost $500 million to phishers in 2004.
- Also from the Phemon Institute: Of 1,335 people surveyed, about 70 percent visited a fake site, and as many as 15 percent said they had provided personal information to the fake site.

. . . And What to Do If You Suspect You're at Risk

The FTC says that if you believe your personal information may have been compromised, you should:

- Close your credit-card accounts (using an ID Theft Affidavit form) and change all your passwords.
- Place a fraud alert on your credit reports with one of the major credit bureaus (Equifax, Experian, and TransUnion).
- Ask government agencies like the Department of Motor Vehicles to flag your file so that no one can get documents in your name.

Figure 8.4

Phishing Facts and What to Do If You're at Risk

chat room exchanges. And an employer can ask a job applicant to take drug and psychological tests, the results of which are the property of the company.

After you're hired, your employer can monitor where you go, what you do, what you say, and what you write in e-mails—at least during working hours. The American Management Association says that as of March 2005, 60 percent of employers monitored employee e-mails, both incoming and outgoing. That figure is up from 47 percent in 2001.[13] One reason that companies monitor employees' e-mail is that they can be sued for what their employees send to each other and to people outside the company.

Chevron Corporation and Microsoft settled sexual harassment lawsuits for $2.2 million each because employees sent offensive e-mail to other employees and management didn't intervene. Other companies such as Dow Chemical Company, Xerox, the New York Times Company, and Edward Jones took preemptive action by firing people who sent or stored pornographic or violent e-mail messages.[14]

About 70 percent of Web traffic occurs during work hours, and this is reason enough for companies to monitor what, and for how long, employees are surfing the Web. The FBI reports that 78 percent of surveyed companies indicated that employees had abused Internet privileges by downloading pornography, pirating software, or some other activity that wasn't work related. Also, 60 percent of employees said that they visit Web sites or surf for personal use at work. Again, various software packages are available to keep track of people's Web surfing. Some software actually blocks access to certain sites.

Businesses have good reasons for seeking and storing personal information on employees. They

- Want to hire the best people possible and to avoid being sued for failing to adequately investigate the backgrounds of employees.
- Want to ensure that staff members are conducting themselves appropriately and not wasting or misusing company resources. Financial institutions are even required by law to monitor all communications including e-mail and telephone conversations.
- Can be held liable for the actions of employees.

MONITORING TECHNOLOGY Numerous vendors sell software products that scan e-mail, both incoming and outgoing. The software can look for specific words or phrases in the subject lines or in the body of the text. An e-mail-scanning program can sneak into your computer in Trojan-horse software. That is, it can hide in an innocent-looking e-mail or some other file or software.

Some companies use an approach less invasive than actually reading employees' e-mail. Their e-mail inspection programs just check for a certain level of e-mail to and from the same address. When this indicates that there may be a problem, the employee is informed of the situation and asked to remedy it. No intrusive supervisory snooping is necessary.[15]

An employer can track your keyboard and mouse activity with the type of key logger software that you read about in the previous section. An alternative that's sometimes harder to detect is a hardware key logger. A ***hardware key logger*** is a hardware device that captures keystrokes on their journey from the keyboard to the motherboard. These devices can be in the form of a connector on the system-unit end of the cable between the keyboard and the system unit. There's another type of hardware key logger that you can install into the keyboard. Both have enough memory to store about a year's worth of typing. These devices can't capture anything that's not typed, but they do capture every keystroke, including backspace, delete, insert, and all the others. To defeat them you'd have to copy the password (or whatever you want kept secret) and paste it into its new

INDUSTRY PERSPECTIVE

THE CASINO CHIPS ARE WATCHING YOU

Everyone knows that the casinos in Las Vegas have numerous cameras that track all activity on the floor. But the Hard Rock Hotel and Casino has gone one better by keeping track of individual betting tokens in its high-limit blackjack room where minimum bets are $100. Managers know where each high denomination token is at all times and can better guard against token theft and counterfeiting.

The way the casino does this is to fit the plastic tokens that are about the size of a half-dollar with RFID (radio frequency identification) chips like the ones that Wal-Mart uses to track its products all the way from the factory to the store shelves. It's also the same technology that's used to keep track of health care supplies, aerospace parts, and many other products.

Up until now, casinos have been able to track slot-machine players by means of "frequent player" cards that players insert into the machines. Table games, however, were more difficult since the only objective option was video cameras, and otherwise it was up to dealers and pit bosses to estimate how much money gamblers were wagering. The level of betting by customers determines the type and number of freebies and/or discounts customers are entitled to.

With RFID chips embedded into the gambling tokens, pit bosses can keep track of players, their average bets, the denomination of chips they're using, and a wealth of other information.

It works like this: The gambling chips with RFID are sold to a gambler, and when the chips hit the table, sensors below the surface of the table read the data and send it to the computer system. The pit boss then just has to watch the monitor to keep track of how the players are betting and how much they're winning or losing.[16]

location. The key logger keeps a record of the keystrokes you use, if any, in your copy-and-paste operation, but not what you copied and pasted.

There is little sympathy in the legal system for the estimated 27 million employees whom the American Management Association says are under surveillance. Employers have the legal right to monitor the use of their resources and that includes the time they're paying you for. In contrast to your home, you have no expectation of privacy when using the company's resources.

The most recent federal bill that addressed electronic monitoring of employees is the Electronic Communications Privacy Act of 1986. Although, in general, it forbids the interception of wired or electronic communications, it has exceptions for both prior consent and business use.

Some state laws have addressed the issue of how far employers can go and what they can do to monitor employees. Connecticut has a law that took effect in 1999 that requires employers in the private sector to notify employees in writing of electronic monitoring. And Pennsylvania, a year earlier, permitted telephone marketers to listen in on calls for quality control purposes as long as at least one of the parties is aware of the action.[17]

PRIVACY AND CONSUMERS

Businesses face a dilemma.

- Customers want businesses to know who they are, but, at the same time, they want them to leave them alone.
- Customers want businesses to provide what they want, but, at the same time, they don't want businesses knowing too much about their habits and preferences.
- Customers want businesses to tell them about products and services they might like to have, but they don't want to be inundated with ads.

Like it or not, massive amounts of personal information are available to businesses from various sources. A relatively large Web site may get about 100 million hits per day, which means that the site gets about 200 bytes of information for each hit. That's about 20 gigabytes of information per day.[18] This level of information load has helped to make customer relationship management (CRM) systems one of the fastest growing areas of software development. Part of managing customer relationships is personalization. Web sites that greet you by name and Amazon.com's famous recommendations that "People who bought this product also bought . . ." are examples of personalization, which is made possible by the Web site's knowledge about you.[19]

Apart from being able to collect its own information about you, a company can readily access consumer information elsewhere. Credit card companies sell information, as do the Census Bureau and mailing list companies. Web traffic tracking companies such as DoubleClick follow you (and other surfers) around the Web and then sell the information about where you went and for how long. DoubleClick can collect information about you over time and provide its customers with a highly refined profile on you. DoubleClick is also an intermediary for companies that want to advertise to Web surfers. When hired by a company wanting to sell something, DoubleClick identifies people who might be receptive and sends the ad to them as a banner or pop-up ad. Proponents of this practice claim that it's good for the surfers because they get targeted advertising and less unwanted advertising. You can judge for yourself how true this claim is. DoubleClick, at first, undertook to track consumers without attaching their identity to the information. Then, in 1999, DoubleClick changed its policy and announced that it would attach consumer names to personal information and e-mail addresses. However, in response to negative consumer reaction, DoubleClick withdrew its proposed change. Interestingly, DoubleClick didn't state it would never resume the abandoned policy, but agreed only to wait until standards for such activity are in place.[20]

COOKIES The basic tool of consumer Web monitoring is the cookie. A ***cookie*** is a small file that contains information about you and your Web activities, which a Web site you visit places on your computer. A cookie has many uses. For example, it's used to keep ID and password information so that you don't have to go through the whole verification process every time you log onto a Web site. It's also used to store the contents of electronic shopping carts, so that the next time you log on, the Web site will be able to see your wish list (which is stored on your computer in a cookie).

A cookie can also be used to track your Web activity. It can monitor and record what sites you visit, how long you stay there, what Web pages you visited, what site you came from and the next site you went to. This type of cookie is called a *unique cookie.* Some cookies are temporary and some stay on your computer indefinitely.

Third-party or *common cookies* are the ones that have many privacy advocates disturbed. These are different from the unique cookies that a Web site you visit puts onto your hard disk. A common cookie is one that started out as a unique cookie, but the original site sold access to it to a third party, like DoubleClick, that can then change the cookie so that the third party can track the surfer's activity across many sites. The third party collects information about surfers without names or other identifiable personal information. They usually collect an IP address, which they then link to a random identifying ID so that the surfer can be identified at other sites. Surveys have shown that the vast majority of people (91 percent) don't like the idea of unknown companies gathering information about them that they have provided to sites with whom they chose to interact.[21]

You have two options if you want to block cookies. First, you can set your browser to accept or reject all cookies. Or you can get it to warn you when a site wants to put a

cookie on your computer. Second, you can get cookie management software with additional options that are not available on your browser. For example, CookieCop 2, from *PC Magazine,* will let you accept or reject cookies on a per-site basis. It also allows you to replace banner ads with the image of your choice and to block ads for sites you find offensive. With this or other cookie-stopper software, you can disable pop-up windows, and stipulate that certain cookies can stay on your hard drive for the duration of one session only.

SPAM ***Spam*** is unsolicited e-mail (electronic junk mail) from businesses that advertise goods and services. Often spam mass mailings advertise pornography, get-rich-quick schemes, and miracle cures. If you haven't been inundated with spam, you're either very lucky or you don't use the Internet much. Spam has become a severe irritant to consumers and a costly matter for businesses, who must sort through hundreds of e-mail messages every day deleting spam and hoping that they don't delete e-mail messages that are actually legitimate customer orders.

You can get spam filters to block out spam, but spammers are clever about including nonprinting characters in their subject lines and addresses that fool the filters into letting them pass. For example, say a spammer wanted to send out a message about a new weight loss drug called *Off.* The spammer would alter the spelling of the word or add invisible HTML tags so that the subject line would be: O*F*F or OF<u></u>F. The HTML tags and <u> would normally italicize and underline text, respectively, and the and </u> would undo the italicizing and bolding, but since there's no text in between the tags do nothing except evade the filter.

Experts estimate that up to 70 percent of e-mail traffic in 2004 was spam and in June and July of 2004 spam reached the staggering figure of over 85 percent.[22] And now its at more than 86 percent with no end in sight, according to experts. In Europe, it's not quite as bad at 62 percent, which amounts to 16 billion messages per day. An individual spammer can send out 80 million or so spams per day. AOL and Microsoft say that their servers block a billion spam messages every day.[23] Many states have passed laws to regulate spam and the Federal Government passed an anti-spam law in 2003 called the CAN-Spam Act (see Figure 8.6 on page 366), which was widely criticized by anti-spam activists as legitimizing spam, since it set down rules for spamming rather than banning it altogether.

Most experts doubt that the CAN-Spam Act hurts the spammers who are the source of most of the spam. They say that it just costs legitimate businesses time and money since they have to maintain do-not-spam lists and follow the legal guidelines when sending out e-mails to customers. Since the bulk of spam comes from spammers who spoof (disguise) the origin of the e-mail, they can usually operate for a long time in defiance of the law. Irate spam trackers, some of whom have become cyber vigilantes, have gone so far as to "out" spammers and publicize information about them on the Web in an effort to stop them.

One trick that spammers use to collect addresses for spamming is to send out e-mail purporting to add you to a general do-not-spam list if you reply. In fact, what it does is add your e-mail address to the list of "live" ones.

ADWARE AND SPYWARE If you've downloaded a game or other software from the Web for free, you may have noticed that it came with banner ads. These ads are collectively known as adware. ***Adware*** is software to generate ads that installs itself on your computer when you download some other (usually free) program from the Web (see Figure 8.5 on the next page). Adware is a type of ***Trojan horse software,*** meaning that it's software you don't want hidden inside software you do want. There's usually a disclaimer, buried somewhere in the multiple "I agree" screens, saying that the software

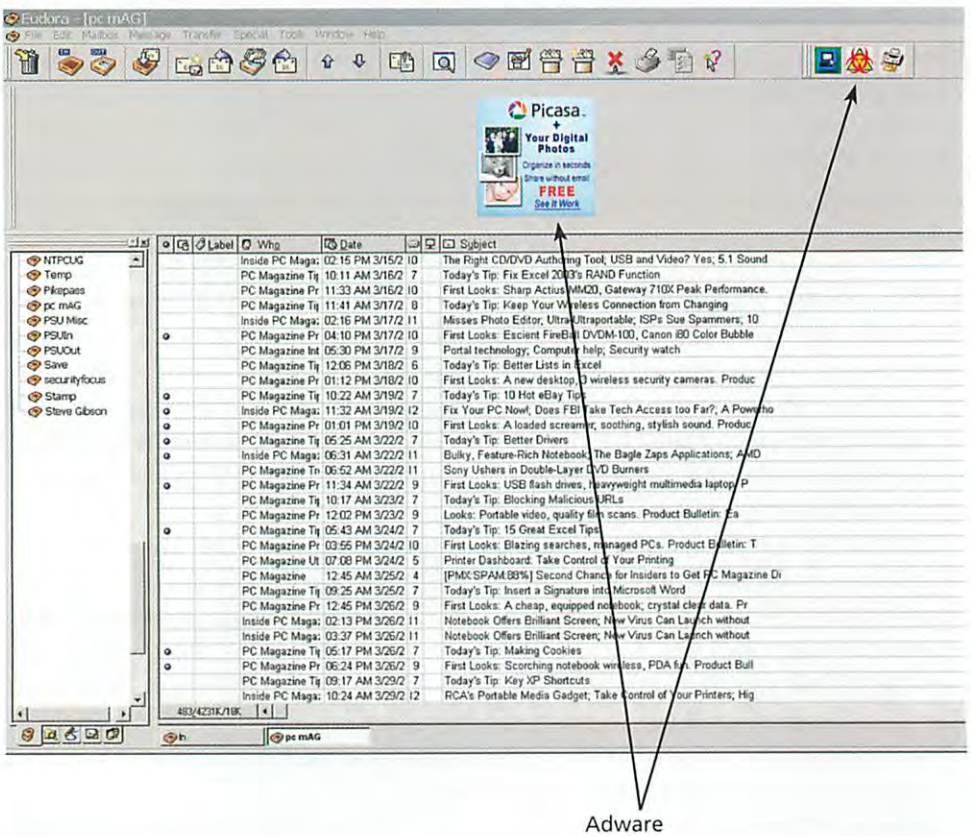


Figure 8.5

Adware in a Free Version of Eudora, an E-Mail Application from Qualcomm

includes this adware. At the bottom of several small-print screens you're asked to agree to the terms. Very few people read the whole agreement, and advertisers count on that. This sort of product is sometimes called *click-wrap* because it's like commercial software that has an agreement that you agree to by breaking the shrink-wrap.

Most people don't get upset about pure adware, since they feel it's worth having to view ads to get software for free. However, there's a more insidious extra that's often bundled with free downloadable software called spyware. ***Spyware*** (also called ***sneakware*** or ***stealthware***) is malicious software that collects information about you and your computer and reports it to someone without your permission. It usually comes hidden in downloadable software and tracks your online movements and/or mines the information stored on your computer. The first release of RealNetworks' RealJukebox sent information back to the company about what CDs the people who downloaded the software were playing on that computer. This information collection was going on when the customer wasn't even on the Web.[24]

Spyware is fast becoming the hidden cost of free software. Software such as Kazaa Media Desktop and Audiogalaxy, the successors to Napster for sharing music and other files online, includes spyware. If you download free software and it has banner ads, it's quite possible that it has spyware, too. There's usually something in the "I agree" screens telling you about spyware, but it can be hard to find. Spyware can stay on your computer long after you've uninstalled the original software.

You can detect various kinds of Trojan horse software with The Cleaner from www.moosoft.com. Also check out www.wilders.org for Trojan First Aid Kit (TFAK). The best-known spyware detection programs, also called stealthware blockers, are Ad-Aware (free from www.lavasoftUSA.com) and PestPatrol. The software scans your whole

INDUSTRY PERSPECTIVE

IS YOUR MUSIC CD HIJACKING YOUR COMPUTER?

When you buy a shrink-wrapped CD at a reputable music store, you don't expect it to open up your computer to every hacker with evil in mind. That's exactly what happened to a lot of people in 2005 when Sony, as part of a copy protection scheme, embedded a rootkit in its music CDs. A *rootkit* is software that gives you administrator rights to a computer or network and its purpose is to allow you to conceal processes, files, or system data from the operating system. You can read more about rootkits in *Extended Learning Module H, Computer Crime and Digital Forensics.*

Sony's rootkit was designed to transfer itself to your computer surreptitiously. The CD would play only from the player included on the CD. Other players didn't recognize it as an audio CD, and instead opened the CD as a data CD.

The original intent was twofold: first, to allow consumers to make up to three copies to play on different platforms, but to prevent P2P distribution and large-scale copying; second, to relay back to Sony what people were doing with Sony's CDs. What it also did was open up a backdoor for anyone who knew about it to get into your system and do whatever they wanted, like using it to send out millions of spam messages or to spread viruses.

The fallout from this scheme was a nightmare for Sony. The company lost millions of dollars when it had to pull 4.7 million copy-protected discs that represented 52 titles including Van Zant, Celine Dion, Neil Diamond, and Bette Midler. Lawsuits rained down on Sony. There were several class action suits and a large number of small claims court actions; states, including Texas filed lawsuits, as did Canada and various countries in Europe. A Sony spokesman, questioned about the rootkit shortly after it was first discovered, said that since no one even knows what a rootkit is, he didn't think it would be a problem. Well, a lot more people know about it now!

computer, identifies spyware programs, and offers to delete them. If you want to check out free software for spyware before you download it, go online to www.spychecker.com, a site that will tell you if particular free software includes adware or spyware.

Even without spyware, a Web site can tell a lot about its Web visitors from its Web log. A ***Web log*** consists of one line of information for every visitor to a Web site and is usually stored on a Web server. At the very least, a Web log can provide a Web site company with a record of your clickstream.

A ***clickstream*** records information about you during a Web surfing session such as what Web sites you visited, how long you were there, what ads you looked at, and what you bought. If, as a consumer, you want to protect information about your surfing habits, you can use various software packages to do so. Apart from cookie management software you can avail yourself of ***anonymous Web browsing (AWB)*** services, which, in effect, hide your identity from the Web sites you visit. An example is Anonymizer at www.anonymizer.com. This site, and others like it, sends your Web browsing through its server and removes all identifying information. Some of the ABW services that are available include disabling pop-up promotions, defeating tracking programs, and erasing browsing history files. If you don't want to go through an outside server, you can download software to do the job. SurfSecret is a shareware antitracking package available from www.surfsecret.com.

As a final note on the subject, remember that even if a company promises, and fully intends, to keep its customer information protected, it may not be possible. When faced with a subpoena, the company will have to relinquish customer records. Furthermore, courts have ruled in bankruptcy cases that customer files are assets that may be sold to pay debts.

PRIVACY AND GOVERNMENT AGENCIES

Government agencies have about 2,000 databases containing personal information on individuals.[25] The various branches of government need information to administer entitlement programs, such as social security, welfare, student loans, law enforcement, and so on.

LAW ENFORCEMENT You've often heard about someone being apprehended for a grievous crime after a routine traffic stop for something like a broken taillight. The arrest most likely ensued because the arresting officer ran a check on the license plate and driver's license. The officer probably checked the National Crime Information Center (NCIC) database and found the outstanding warrant there. Timothy McVeigh and others responsible for the bombing of the Federal building in Oklahoma City were caught in this way.

The NCIC database contains information on the criminal records of more than 20 million people. It also stores information on outstanding warrants, missing children, gang members, juvenile delinquents, stolen guns and cars, and so on. The NCIC has links to other government and private databases, and guardians of the law all over the country can access NCIC information. Sometimes they do so in response to something suspicious, and other times it's just routine. For example, Americans returning from outside the country are routinely checked through the NCIC when they come through customs.

Given its wealth of information and accessibility, it's not surprising that NCIC system has been abused. Several police departments have found that a significant number of employees illegally snooped for criminal records on people they knew or wanted to know.

The Federal Bureau of Investigation (FBI) has caused a stir lately because of its electronic surveillance methods. First there was Carnivore, a rather unfortunate name, which has since been changed to DCS-1000. DCS-1000 connects hardware to an ISP to trap all e-mail sent to or received by the target of the investigation. It takes a court order to use DCS-1000, and, of course, the target is typically unaware of the surveillance. Intercepting communications is not new: The FBI put the first tap on a phone in 1885, just four years after the invention of the telephone.[26] DCS-1000, with a court order, traps all communications involving the individual named in the court order.

Because it can be hard to identify the data packets of one individual's e-mail amongst all the other Internet traffic, it's entirely possible that other people's e-mail might be scooped up in the net. And this is what happened in March 2000 when FBI agents were legally intercepting messages of a suspect, but someone else was caught in the trap. The information on the innocent party was obtained under the Freedom of Information Act. The FBI said the incident was an honest mistake and a result of miscommunication between it and the ISP.[27] But this is the sort of mistake that scares people. Most people want law enforcement to be able to watch the bad guys—that's necessary for our collective safety. But the prospect of information being collected on law-abiding citizens who are minding their own business worries a lot of people.

In 2001, the FBI acknowledged an enhancement to DCS-1000 called Magic Lantern, which is key logger software. The FBI installs it by sending the target an innocent-looking Trojan-horse e-mail, which contains the key logger software. The hidden software then sends information back to the FBI periodically.[28]

Another federal agency, the National Security Agency (NSA), uses a system called Echelon that uses a global network of satellites and surveillance stations to trap phone, e-mail, and fax transmissions. The system then screens all this information looking for certain keywords and phrases and analyzes the messages that fit the search criteria.

At the local level, the actions of the Tampa Police Department at the 2001 Super Bowl caused an outcry from privacy advocates. Police, with the agreement of the NFL,

focused video cameras on the faces of tens of thousands of spectators as they entered the stadium. The images were sent to computers which, using facial recognition software, compared the images to a database of pictures of suspected criminals and terrorists. The police spokesperson said that the action was legal since it's permissible to take pictures of people in public places. That's true in so far as you have no expectation of privacy in a public place. Indeed surveillance of people has been going on for years without much protest in gambling casinos, Wal-Mart stores, and other businesses in the private sector. But the American Civil Liberties Union (ACLU) protested the surveillance of Super Bowl spectators on the grounds that it was surveillance by a government agency without court-ordered authorization. The fact that the state was involved made it unacceptable to the ACLU.

OTHER FEDERAL AGENCIES The Internal Revenue Service (IRS) gets income information from taxpayers. But the agency has access to other databases, too. For example, the IRS keeps track of vehicle registration information so that it can check up on people buying expensive cars and boats to make sure they're reporting an income level that corresponds to their purchases. The IRS can go to outside government databases as well. Verizon says that it gets 22,000 requests for phone records from the IRS, FBI, and other government agencies per year. It seldom informs the customer of the request. America Online (AOL) has a special fax number reserved just for subpoenas.

The Census Bureau collects information on all the U.S. inhabitants it can find every 10 years. All citizens are requested to fill out a census form, and some people get a very long and detailed form requiring them to disclose a lot of personal information. The information that the Census Bureau collects is available to other government agencies and even to commercial enterprises. The bureau doesn't link the information to respondents' names but sells summarized information about geographic regions. Some of these regions are relatively small, however, consisting of fewer than 100 city blocks.

It's fairly safe to assume that anytime you have contact with any branch of government, information about you will be subsequently stored somewhere. For example, if you get a government-backed student loan, you provide personal information such as your name, address, income, parents' income, and so on. Some of the information nuggets attached to the loan would be the school you're attending, the bank dispersing the loan, your repayment schedule, and later, your repayment pattern.

LAWS ON PRIVACY

The United States doesn't have a comprehensive or consistent set of laws governing the use of information. However, some laws are in place. Recent legislation includes the Health Insurance Portability and Accountability Act (HIPAA) and the Financial Service Modernization Act. HIPAA, enacted in 1996, requires that the health care industry formulate and implement the first regulations to keep patient information confidential. The act seeks to

- Limit the release and use of your health information without your consent.
- Give you the right to access your medical records and find out who else has accessed them.
- Overhaul the circumstances under which researchers and others can review medical records.
- Release health information on a need-to-know basis only.
- Allow the disclosure of protected health information for business reasons as long as the recipient undertakes, in writing, to protect the information.

- **Identity Theft and Assumption Deterrence Act,** 1998, strengthened the criminal laws governing identity theft, making it a federal crime to use or transfer identification belonging to another. It also established a central federal service for victims.
- **USA Patriot Act,** 2001 and 2003, allows law enforcement to get access to almost any information, including library records, video rentals, bookstore purchases, and business records when investigating any act of terrorism or hostile intelligence activities. In 2003 Patriot II broadened the original law.
- **Homeland Security Act,** 2002, provided new authority to government agencies to mine data on individuals and groups including e-mails and Web site visits; put limits on the information available under the Freedom of Information Act; and gave new powers to government agencies to declare national heath emergencies.
- **Sarbanes-Oxley Act,** 2002, sought to protect investors by improving the accuracy and reliability of corporate disclosures and requires companies to (1) implement extensive and detailed policies to prevent illegal activity within the company and (2) respond in a timely manner to investigate illegal activity. (You'll find more about the business implications of Sarbanes-Oxley in *Extended Learning Module H: Computer Crime and Digital Forensics.*)
- **Fair and Accurate Credit Transactions Act,** 2003, included provisions for the prevention of identity theft including consumers' right to get a credit report free each year, requiring merchants to leave all but the last five digits of a credit card number off a receipt, and requiring lenders and credit agencies to take action even before a victim knows a crime has occurred when they notice any circumstances that might indicate identity theft.
- **CAN-Spam Act,** 2003, sought to regulate interstate commerce by imposing limitations and penalties on businesses sending unsolicited e-mail to consumers. The law forbids deceptive subject lines, headers, return addresses, etc., as well as harvesting e-mail addresses from Web sites. It requires businesses that send spam to maintain a do-not-spam list and to include a postal mailing address in the message.

Figure 8.6
Recent Information-Related Laws

The Financial Services Modernization Act requires that financial institutions protect personal customer information and that they have customer permission before sharing such information with other businesses. However, the act contains a clause that allows the sharing of information for "legitimate business purposes." See Figure 8.6 for recent information-related laws.

LEARNING OUTCOME 4

Security

So, what can put your important information resource in jeopardy? Well, countless things. Hard disks can crash, computer parts can fail, hackers and crackers can gain access and do mischief, thieves engaged in industrial espionage can steal your information, and disgruntled employees or associates can cause damage. The FBI estimates that computer sabotage costs businesses somewhere close to $10 billion every year. Companies are increasing their spending on Internet security software, a fact that Symantec Corp. can attest to. Symantec is the largest exclusive developer of computer security software and has a market value of $19 billion, making it one of the most valuable software companies in the world.[29]

SECURITY AND EMPLOYEES

Most of the press reports are about outside attacks on computer systems, but actually, companies are in far more danger of losing money from employee misconduct than they are from outsiders. It's estimated that 75 percent of computer crime is perpetrated by insiders, although this is not a problem that's restricted to computer misuse. A 300-restaurant chain with 30 employees in each location loses, on average, $218 per employee.

But white-collar crime is where the big bucks are lost (see Figure 8.7). White-collar crime in general, from Fortune 100 firms to video stores to construction companies, accounts for about $400 billion in losses every year—$400 billion is $108 billion more than the whole federal defense budget—and information technology makes it much easier to accomplish and conceal the crime. Of all white collar fraud, the biggest losses are those incurred by management misconduct. Manager theft of various kinds is about four times that of other employees. Take embezzlement, for example. The average cost of a nonmanagerial employee's theft is $60,000, while that for managerial employees is $250,000. The most astonishing aspect of this is that most insider fraud (up to two-thirds) is never reported to the legal authorities, according to the Association of Certified Fraud Examiners (ACFE).

Computer-aided fraud includes the old standby crimes like vendor fraud (sending payment to a nonexistent vendor or payment for goods not delivered), writing payroll checks to fictitious employees, claiming expense reimbursements for costs never incurred, and so on. In addition, there are newer crimes such as stealing security codes, credit card numbers, and proprietary files. Intellectual property is one of the favorite targets of theft by insiders. In fact, the companies that make surveillance software say that employers are buying and installing the software not so much to monitor employees as to track how intellectual property, like product design sketches, schematics, and so on, is moving around the network.

Fraud examiners have a rule of thumb that in any group of employees, about 10 percent are completely honest, 10 percent will steal, and, for the remaining 80 percent, it will depend on circumstances. Most theft is committed by people who are strapped for cash, have access to funds that are poorly protected, and perceive a low risk of getting caught.

SECURITY AND OUTSIDE THREATS

In 2006, companies spent, on average, $5 million each to recover corporate data that was lost or stolen. That's 30 percent more than in 2005. The losses are the result of many problems such as someone breaking into their systems, malicious insider activity,

	Who's Committing Fraud
61%	Fraud committed by men
39%	Fraud committed by women
$250,000	Median loss from fraud committed by men
$102,000	Median loss from fraud committed by women
41%	Fraud committed by managers
39.5%	Fraud committed by employees
19.3%	Fraud committed by owners/executives

Figure 8.7

Figures on Fraud

Source: 2006 ACFE Report to the Nation on Occupational Fraud and Abuse.

malware like spyware and viruses, and the theft of USB devices, notebook computers, and flash memory cards. The average cost per record that was compromised was $140.[30]

The threats from outside are many and varied. Competitors could try to get your customer lists or the prototype for your new project. Cyber vandals could be joyriding in cyberspace looking for something interesting to see, steal, or destroy. You could become the victim of a generalized attack from a virus or worm, or could suffer a targeted attack like a denial-of-service attack. If you have something worth stealing or manipulating on your system, there could be people after that, too. For example, the online gambling industry is plagued by attacks where hackers have illicitly gained access to the servers that control the gambling, corrupting games to win millions of dollars. Exploiting well-known system weaknesses accounts for a large part of hacker damage, while only 5 percent results from breaking into systems in new ways.[31]

The people who break into the computer systems of others are "hackers" (see Figure 8.8). ***Hackers*** are generally knowledgeable computer users who use their knowledge to invade other people's computers. They have varying motives. Some just do it for the fun of it. Others (called hacktivists) have a philosophical or political message they want to share, and still others (called crackers) are hired guns who illegally break in, usually to steal information, for a fee. The latter can be a very lucrative undertaking. Some highly skilled crackers charge up to $1 million per job. There are also "good guys," called white-hat hackers, who test the vulnerability of systems so that protective measures may be taken.

Cyber Crime

TYPES OF CYBER CRIME Cyber crimes range from electronically breaking and entering to cyberstalking and murder. In October 1999, a 21-year-old woman was shot and killed outside the building where she worked. Her killer had been electronically stalking her for two years. He became obsessed with the young lady and had even posted a Web site dedicated to her on which he announced his intention to kill her. He got her Social Security number online, found out where she worked, tracked her down, and shot her, after which he shot himself.

Most cyber crimes are not as bad as murder, but they can be serious nonetheless. Computer viruses and denial-of-service attacks are the two most common types of cyber crime against which companies need to protect themselves.

A ***computer virus*** (or simply a ***virus***) is software that is written with malicious intent to cause annoyance or damage. A virus can be benign or malicious. The benign ones

Figure 8.8

Hacker Types

- White-hat hackers find vulnerabilities in systems and plug the holes. They work at the request of the owners of the computer systems.
- Black-hat hackers break into other people's computer systems and may just look around, or they may steal credit card numbers or destroy information, or otherwise do damage.
- Hacktivists have philosophical and political reasons for breaking into systems. They often deface a Web site as a protest.
- Script kiddies, or script bunnies, find hacking code on the Internet and click-and-point their way into systems, to cause damage or spread viruses.
- Crackers are hackers for hire and are the hackers who engage in corporate espionage.
- Cyberterrorists are those who seek to cause harm to people or to destroy critical systems or information. They try to use the Internet as a weapon of mass destruction.

GLOBAL PERSPECTIVE

ONLINE BLACKMAIL

"You can ignore this e-mail and try to keep your site up, which will cost you tens of thousands of dollars in lost customers, or you can send us $10K bank wire to make sure that your site experiences no problems + we will give you our protection for a year."

Above is the message that the managers of Protx, an online-payment processing firm in London, received by e-mail. The incident was the third time the company had been attacked within the year, and it was the most savage attack. At one point, the Protx network was bombarded by a blitz of traffic, to the tune of 500 megabits per second (that's about five times more traffic per second than a large ISP would handle). This barrage came from thousands of computers whose power had been commandeered by the attackers in what's called a distributed denial-of-service attack, and it knocked the company offline.

As is often the case, the attacks were conducted with bot viruses. A bot virus is a program that attackers plant in someone else's computer that allows the perpetrator to use the resources—the CPU or hard disk, for example—for their own purposes.

In the case of Protx, computer security experts were called in to stop the attacks and prevent the same sort of thing from happening in the future. They found that as soon as they shut down one stream of attacks, another one would start from a different hijacked network. It cost Protx about $500,000 to secure its network against future attacks. Such costs are usually annual expenses and don't include the cost of shutting down the original attacks or the cost of the business lost by the victim company.[32]

just display a message on the screen or slow the computer down, but don't do any damage. The malicious kind targets a specific application or set of file types and corrupts or destroys them.

Today, worms are the most prevalent type of virus. Worms are viruses that spread themselves; they don't need your help, just your carelessness.

A ***worm*** is a type of virus that spreads itself, not just from file to file, but from computer to computer via e-mail and other Internet traffic. It finds your e-mail address book and helps itself to the addresses and sends itself to your contacts, using your e-mail address as the return address. The Love Bug worm was one of the early worms that did a lot of damage and got major press coverage. It's estimated that the Love Bug and its variants affected 300,000 Internet host computers and millions of individual PC users causing file damage, lost time, and high-cost emergency repairs costing about $8.7 billion.[33,34] Ford Motor Company, H. J. Heinz, Merrill Lynch, AT&T, Capitol Hill, and the British Parliament all fell victim to the Love Bug worm. Newer versions of worms include Klez, a very rapidly spreading worm, Nimda, and Sircam.

A ***denial-of-service attack (DoS)*** floods a server or network with so many requests for service that it slows down or crashes. The objective is to prevent legitimate customers from accessing the target site. E*Trade, Yahoo!, and Amazon.com have all been victims of this type of attack. For more information about viruses and hackers and DoSs see *Extended Learning Module H.*

As well as knowing what viruses can do, you need to know what they can't do. Computer viruses can't

- Hurt your hardware, such as your monitor, or processor.
- Hurt any files they weren't designed to attack. A virus designed for Microsoft's Outlook, for example, generally doesn't infect Qualcomm's Eudora, or any other e-mail application.

SECURITY PRECAUTIONS

In Chapter 7, Enterprise Infrastructure, Metrics, and Business Continuity Planning, you learned about business contigency plans and in *Extended Learning Module E: Network Basics* you read about intrusion detection. These are both very important components of any company's computer system security. There are also standard precautions that a company, and any individual who wants protection from the computer-based attacks, should take.

The most basic protection is to have anti-virus software running on your computer. ***Anti-virus software*** detects and removes or quarantines computer viruses. New viruses are created every day and each new generation is more deadly (or potentially more deadly) than the previous one. You should update your anti-virus software regularly and make sure it's running all the time so that it kicks in when you download e-mail and other files.

Many of the anti-virus software packages on the market also protect you against other cyber evils, like spyware and adware. They will also block cookies, pop-up ads, and embedded objects and scripts such as you get if you download a Flash file, for instance.

Spam protection is theoretically good to have, although it may let some spam through and may mark as spam something that isn't. You can usually choose to have the spam deleted, quarantined (in its own folder), or marked so that it stands out when you look in your Inbox. *Anti-phishing software* is also available to protect you from identity theft. The MyVault feature of ZoneAlarm, for example, will block data such as Social Security Number, credit card numbers, and passwords from leaving your computer. Anti-phishing toolbars warn you when you arrive at a known phishing site. Symantec's anti-phishing software places a toolbar beneath the Address Bar which turns red if you land at a phishing site.

ZoneAlarm, which is a firewall program with additional features, will let you know if a program is trying to access the Internet for whatever reason, as spyware on your computer may be attempting to do ZoneAlarm from www.zonealarm.com is a very popular software firewall. ZoneAlarm also offers protection from ads and cookies. A ***firewall*** is hardware and/or software that protects a computer or network from intruders. The firewall examines each message as it seeks entrance to the network, like a border guard checking passports. Unless the message has the "right" markings, the firewall will block it from entering. You can set your firewall so that it identifies certain programs that are always allowed to visit a Web site. Your e-mail program would be an example. Any competent network administrator will have at least one firewall on the network to keep out unwelcome guests. Protection against rootkits, for example, which we discussed in the Industry Perspective box, "Is Your Music CD Hijacking Your Computer?" on page 353.

There are other issues you might think about, *Rootkit finders* are available from Kaspersky's and F-Secure security software. There are also free programs available. Removing rootkits is a tricky task and different software packages meet with varying degrees of success.

There are also programs that will block certain sites, which is useful if you have underage children. Some people suggest using FireFox or Opera as your default browser since Microsoft's Internet Explorer has long been a favorite target of hackers.

ACCESS AUTHENTICATION While firewalls keep outsiders out, they don't necessarily keep insiders out. In other words, unauthorized employees may try to access computers or files. One of the ways that companies try to protect computer systems is with authentication systems that check who you are before they let you have access.

There are three basic ways of proving your access rights: (1) what you know, like a password; (2) what you have, like an ATM card; (3) what you look like (more specifically what your fingerprint or some other physical characteristic looks like).

INDUSTRY PERSPECTIVE

PROTECTING PERSONAL RFID-STORED INFORMATION

Radio frequency ID chips are very small, almost paper-thin chips, in some instances, that store and wirelessly transmit and receive information. For example, Wal-Mart has for several years been implementing RFID for inventory control. The company will eventually require all its suppliers to implement RFID technology. The tags will be on crates and pallets so that they can be tracked through the supply chain. Other applications of RFID include:

- Embedding RFID chips in passports
- Monitoring the temperature of perishable items (DHL)
- Tagging consumer products with RFID instead of bar codes (many companies including Best Buy)
- Contactless credit cards (J.P. Morgan)
- Tagging overseas shipments of suppliers (Australian Department of Defense)
- Tracking cattle

The most controversial use of RFID technology is when people wear it or have it implanted into their bodies. These chips have information, often medical, that can be read in case the person becomes incapacitated. VeriChip makes such a chip and believes that over 40 million people in the United States will someday have them implanted under the skin.

The challenge then becomes one of protecting your personal RFID information. It can be read wirelessly, meaning that people can build reading devices and obtain your medical information by coming within three feet of you. You'll learn more about RFID in Chapter 9.[35,36,37,38]

Passwords are very popular and have been used since there were computers. You can password-protect the whole network, a single computer, a folder, or a file. But passwords are not by any means a perfect way to protect a computer system. People forget their passwords, so someone may have to get them new passwords or find the old one. Banks spend $15 per call to help customers who forget their passwords. Then if a hacker breaks into the system and steals a password list, everyone has to get a new password. One bank had to change 5,000 passwords in the course of a single month at a cost of $12.50 each.[39]

Which brings us to biometrics, or what you look like. ***Biometrics*** is the use of physiological characteristics—such as your fingerprint, the blood vessels in the iris of your eye, the sound of your voice, or perhaps even your breath—to provide identification. Roughly a dozen different types of biometric devices are available at the moment, with fingerprint readers being the most popular. About 44 percent of the biometric systems sold are fingerprint systems. They work just like the law enforcement system where your fingerprint is stored in the database, and when you come along, your finger is scanned, and the scan is compared to the entry in the database. If they match, you're in. See Chapter 9 for more information on biometrics.

ENCRYPTION If you want to protect your messages and files and hide them from prying eyes, you can encrypt them. ***Encryption*** scrambles the contents of a file so that you can't read it without having the right decryption key. There are various ways of encrypting messages. You can switch the order of the characters, replace characters with other characters, or insert or remove characters. All of these methods alter the look of the message, but used alone, each one is fairly simple to figure out. So most encryption methods use a combination.

Companies that get sensitive information from customers, such as credit card numbers, need some way of allowing all their customers to use encryption to send the information. But they don't want everyone to be able to decrypt the message, so they might

use public key encryption. ***Public key encryption (PKE)*** is an encryption system that uses two keys: a public key that everyone can have and a private key for only the recipient. So if you do online banking, the bank will give you the public key to encrypt the information you send them, but only the bank has the key to decrypt your information. It works rather like a wall safe, where anyone can lock it (just shut the door and twirl the knob), but only the person with the right combination can open it again.

Summary: Student Learning Outcomes Revisited

1. **Define ethics and describe the two factors that affect how you make a decision concerning an ethical issue.** ***Ethics*** are the principles and standards that guide our behavior toward other people. How you decide ethical issues must depend especially on your basic ethical structure but also for better or worse on the practical circumstances. Your basic ethics you probably acquired growing up. The practical circumstances that you might allow to affect you include
   - *Consequences.* How much or how little benefit or harm will come from a particular decision?
   - *Society's opinion.* What do you perceive society thinks of your intended action?
   - *Likelihood of effect.* What is the probability of the harm or benefit if you take the action?
   - *Time to consequences.* How long will it take for the benefit or harm to take effect?
   - *Relatedness.* How much do you identify with the person or persons who will receive the benefit or suffer the harm?
   - *Reach of result.* How many people will be affected by your action?
2. **Define and describe intellectual property, copyright, Fair Use Doctrine, and pirated software.** ***Intellectual property*** is intangible creative work that is embodied in physical form. ***Copyright*** is the legal protection afforded an expression of an idea, such as a song or a video game and some types of proprietary documents. The ***Fair Use Doctrine*** says that you may use copyrighted material in certain situations. ***Pirated software*** is the unauthorized use, duplication, distribution or sale of copyrighted software.
3. **Define privacy and describe ways in which it can be threatened.** ***Privacy*** is the right to be left alone when you want to be, to have control over your own personal possessions, and not to be observed without your consent. Your privacy can be compromised by other individuals snooping on you; by employers monitoring your actions; by businesses that collect information on your needs, preferences, and surfing practices; and by the various government agencies that collect information on citizens.
4. **Describe the ways in which information on your computer or network is vulnerable and list measures you can take to protect it.**
   - Employees can embezzle and perpetrate fraud of other types. Most of the financial losses due to computer fraud that is suffered by companies is caused by employees.
   - Hackers and crackers try to break into computers and steal, destroy, or compromise information.
   - Hackers can spread ***computer viruses*** or launch ***denial-of-service attacks (DoS)*** that can cost millions in prevention and cleanup.

   Measures you can take are to install
   - Anti-virus software to find and delete or quarantine viruses
   - Anti-spyware and anti-adware software
   - Spam protection software
   - Anti-phishing toolbar
   - Firewalls
   - Anti-rootkit software
   - Encryption
   - Biometrics

CLOSING CASE STUDY ONE

CAUTIONARY TALES OF INDISCREET E-MAIL

Wrongdoing at Computer Associates and at Enron, once giants in their respective industries, was brought to light by forgotten and/or deleted e-mails. The recovered e-mails brought down guilty individuals, but caused some innocents to suffer as well.

COMPUTER ASSOCIATES

In 2000, Charles Wang, chairman of Computer Associates (CA), a business software development giant, was number one on *Forbes*'s list of wealthiest people with earnings of $650 million, $649 million of which was performance-based. However, early in 2002, federal investigators began investigating Computer Associates for improperly booking more than $2 billion in revenue. It had apparently become common practice for executives to keep quarterly reports open so that later deals could be backdated, making the quarterlies look better. By the end of 2002, Wang had been retired to an honorary, uncompensated position, largely because of the accounting discrepancies being investigated.

Computer Associates' Board of Directors, hoping to avoid the sort of disaster that killed Arthur Andersen, hired experienced criminal lawyers to conduct an investigation to get to the truth. After searching hundreds of employee computers, the investigation turned up e-mails, deleted and saved, that provided evidence of fraud. These e-mails were not on the main system, but rather were stored on individual machines.

By April 2004, three former executives of the company had pled guilty to obstruction of justice charges and by September that number had risen to seven who had pled guilty or been indicted. The obstruction of justice charges came from the top executives' misleading the independent lawyers about the facts of their actions, knowing that the falsehoods would be passed on to federal investigators. Attorney–client privilege did not apply since the outside lawyers were hired to do an independent investigation and did not represent individual executives. By the time the main part of the investigation was over, most of the top-level executives of CA had been fired.

ENRON

When the Federal Energy Regulatory Commission (FERC), which was investigating Enron, unearthed and published confiscated e-mails, not only Enron's employees got a nasty shock when their old e-mails turned up on the Web. Everyone who had sent e-mails to Enron e-mail addresses found themselves caught in the federal net. So, people who were never accused of wrongdoing and didn't even work at Enron suddenly found their e-mail messages displayed for all the world to see, even if the message was as innocent as the confirmation of a golfing date.

FERC gathered a boatload of records, paper and electronic, during its investigation of Enron's alleged energy-market manipulations. In March 2003, FERC posted 1.6 million e-mail messages and other documents on the Web in a searchable database. The e-mails are from the period 2000–2003. So anyone can go to the Web site (www.ferc.gov/industries/electric/indus-act/wem/03-26-03-release.asp) and easily view the e-mails and calendars of 176 current and former Enron employees. The e-mails appear in full—including sender and receiver names.

Among the e-mail messages are lots of personal communications like executives discussing employees and vice versa; romantic messages; discussions of breakups (liaisons and marriages); in-law problems; personal photos, and so on.

FERC said that, since Enron owned the messages, it was incumbent on the company to identify personal communications and request their exclusion.

A couple of days after the e-mail database appeared on the Web, FERC agreed to take off the most sensitive documents, like a document that listed the Social Security number of every employee. In early April, on the order of a U.S. Court of Appeals, the database was shut down for 10 days to allow Enron to examine all the documents and make up a list of documents it wanted removed.

About 100 Enron volunteers spent 350 hours going through hundreds of thousands of e-mails looking for specific terms like "Social Security Number," "credit card number," "kids," and "divorce." FERC removed about 8 percent of the database, which amounted to about 141,000 documents.[40,41]

Questions

1. If you were to give advice to someone who had just started using e-mail, or even someone who's been using e-mail for a while, what would

you tell that person should be the one guiding principle in all their e-mail communications? Put your advice into one sentence.

2. Now expand on your one guiding principle in question 1, and offer 10 rules for writing e-mails. What should those 10 rules be?
3. Imagine you're a manager in a lawn care business and you have an office staff of five people. Your lawyer suggests that you issue guidelines or rules to your staff about storing e-mail on the company's server and on the computers they use in their work for you. What should those guidelines be? What would the rules be? Be sure to explain your rationale.
4. Do you think there should be federal guidelines governing a business's e-mail traffic just as there are regarding a business's financial records? If so, what should they be? If not, why not?

CLOSING CASE STUDY TWO

THE PROBLEM OF INFORMATION PROTECTION

The theft of consumer information—particularly financial information—is causing huge headaches for financial and data companies. This case looks at three incidents that occurred recently at ChoicePoint, Bank of America, and Polo Ralph Lauren.

CHOICEPOINT

The opening case study in this chapter highlighted the Acxiom Corporation, a company that gathers, packages, and sells information about consumers. A direct competitor to Acxiom is ChoicePoint, a company that is a spin-off of Equifax, which is one of the three major credit bureaus.

ChoicePoint has 19 billion records that include information on almost every adult in the United States. ChoicePoint sells this information to customers, such as potential employers, for purposes of verification.

ChoicePoint found itself in the headlines when personal financial information on 145,000 customers was stolen in a very high-profile identity fraud theft. And this time there was no sophisticated electronic attack or break-in; rather the theft was accomplished through old-fashioned "social engineering." Social engineering is getting information that you have no right to by conning people who have access to it. What the identity thieves did was to pose as fake companies buying information on people in every state and the District of Columbia. So far, 750 confirmed cases of identity theft have surfaced from the ChoicePoint security breach.

The U.S. Attorney's Office in Los Angeles charged that ChoicePoint had been scammed previously in 2002 resulting in fraud to the tune of $1 million.

THE BANK OF AMERICA

The Bank of America was also the victim of information theft accomplished in an old-fashioned way. Personal information recorded on tapes belonging to 1.2 million federal employees, including members of Congress, was on a commercial jet en route to a safe backup facility when the tapes were stolen.

Both the Bank of America and ChoicePoint thefts occurred in February 2005 and were followed very quickly by the introduction of privacy legislation at both the state and federal levels.

POLO RALPH LAUREN

Another example of embarrassment and worse involved Polo Ralph Lauren. It seems that between June 2002 and December 2004, the company was storing credit card information on its point-of-sale system instead of deleting it immediately after transactions had been completed. The realization that this data had been compromised led HSBC North America—the issuer of some of the credit cards whose numbers had been stolen—to notify 180,000 consumers of the possibility of identity theft. MasterCard, Visa U.S.A. and Discover Financial Services customers have all been affected. American Express says it has not seen any activity that has looked suspicious.[42,43]

Questions

1. If you were the manager of a company where it was discovered that credit card information had been stolen, what responsibility would you have to the people whose personal information was compromised? What are the pros and cons of notifying and of not notifying possible victims?
2. E*Trade, a leader in online brokerage services, is the first company to go to a two-factor authentication system optionally available to its customers with accounts of $50,000 or more. The first factor is the ID and password that customers have always needed, and second, they use a security token or, as E*Trade calls it, a *Digital Security ID.* This is a little device that you can carry on your key chain that displays a new random six-digit number every minute. E*Trade's host system must, of course, synchronize with the device.

   When you log in, you have to type in this number after your ID and password. Since the number changes so often it's virtually impossible to hack an account with this two-pronged protection. From a consumer's point of view, do you think this is a good idea? What are the advantages and disadvantages of the system to businesses and customers? With which online transactions would you consider it worthwhile to enforce this level of security? Remember that you might have a lot of these tokens if you use a lot of online services.
3. In this case study you saw how personal information can be stolen from huge databases and data warehouses. What other ways are there that thieves can obtain personal information about you that would allow them to steal your identity and run up debts in your name? To what extent would you be liable for these debts? What would you have to do (what steps would you take) to reestablish your financial identity if you discovered your identity had been stolen?
4. In the case of the Bank of America, the data was being shipped on tapes to a safe location. This is very good backup policy to make sure that in the event of a major disaster like a fire or flood, data can be quickly restored enabling the company to be back in operation as soon as possible. However, this procedure leaves the company vulnerable to old-fashioned theft of the physical tapes containing personal information. What are two ways that this information that travels on trucks and planes could be protected?

Key Terms and Concepts

Adware, 351
Anonymous Web browsing (AWB), 353
Anti-virus software, 360
Biometrics, 361
Clickstream, 353
Computer virus (virus), 358
Cookie, 350
Copyright, 342
Denial-of-service attack (DoS), 359
Encryption, 361
Ethics, 340
Fair Use Doctrine, 342
Firewall, 360
Hacker, 358
Hardware key logger, 348
Identity theft, 345
Intellectual property, 342
Key logger software (key trapper software), 342
Pharming, 346
Phishing (carding or brand spoofing), 346
Pirated software, 343
Privacy, 343
Public key encryption (PKE), 362
Spam, 351
Spyware (sneakware or stealthware), 352
Trojan horse software, 351
Web log, 353
Worm, 359

Short-Answer Questions

1. What are ethics, and how do ethics apply to business?
2. What situation would qualify as an exception to the copyright law?
3. What is privacy?
4. What is pirated software?
5. What is identity theft?
6. What does a key logger do?
7. What is spyware?
8. What is a denial-of-service attack?
9. What is public key encryption?