PART FOUR

CONTROLS, SECURITY, PRIVACY, AND ETHICS FOR ACCOUNTING INFORMATION SYSTEMS

Managers have many responsibilities within an organization and one of the most important is to safeguard the assets of the firm. This is no small task. Although people normally think first about safeguarding cash and other physical assets, the huge electronic data repositories of most firms might well be their most valuable assets. Protecting this sensitive information is critical.

Chapter 10 discusses the important topic of computer crime and fraud. This is a growing problem that requires the attention of management at all levels in an organization. We include examples of real world cases of computer crime in this chapter and also describe procedures that organizations can implement to protect their assets. For example, to prevent and detect fraudulent acts within the environment of computerized AISs, firms can perform audit procedures, train employees to recognize symptoms of fraud, and implement stronger security measures.

In practice, organizations with computerized AISs may encounter difficulties with their internal control systems. Chapter 11 introduces the subject of internal control by analyzing the components and control activities within organizations' internal control systems. We provide examples of control procedures throughout this chapter. We also introduce the concept of enterprise-wide risk management, which must be considered first to determine what controls are necessary to mitigate the risks that are identified.

Chapter 12 examines various types of computer controls that are commonly used within AISs: general controls for organizations, general controls for IT, and application controls for transaction processing. This chapter also includes a discussion of business continuity planning. In light of the fact that natural and man-made disasters are becoming more frequent, firms and organizations of all sizes must now become more intentional about developing and testing a disaster recovery plan in support of general controls.

Chapter 10

Computer Crime, Ethics, and Privacy

After reading this chapter, you will:

1. *Understand* why it is difficult to define computer crime.
2. *Know* why there is an absence of good data on computer crime.
3. *Be able to provide reasons* why computer crime might be growing.
4. *Be familiar with* several computer crime cases and the proper controls for preventing them.
5. *Be able to describe* a profile of computer criminals.
6. *Understand* the importance of ethical behavior within the environment of computerized AISs.

"Our personal experiences, along with a host of anecdotal evidence . . . [indicates that occupational fraud has] a massive impact on all sectors of the economy . . . .—approximately $994 billion in fraud losses."

James D. Ratley, President, Association of Certified Fraud Examiners,
2008 Report to the Nation on Occupational Fraud and Abuse,
available at: www.acfe.com/resources/publications.asp.

INTRODUCTION

The connection between AISs and computer crime and fraud is both straightforward and important. Managers, accountants, and investors all use computerized information to control valuable resources, help sell products, authenticate accounting transactions, and make investment decisions. But the effectiveness of these activities can be lost if the underlying information is wrong, incomplete, or seriously compromised. This is why digital information is itself a valuable asset that must be protected. The more managers and accountants know about computer crime and fraud, the better they can assess risks and implement controls to protect organizational assets.

This chapter describes computer crime, fraud, and other irregularities that have occurred in the past and that may also occur in the future. In the first section, we take a closer look at computer crime, abuse, and fraud. In the second section, we examine three specific cases involving computer crime. The third section of this chapter identifies what organizations can do to protect themselves from computer crime and abuse. For example, this section describes ways of recognizing potential problems and what organizations can do to control them.

Not all computer-related offenses are illegal—some are simply unethical. Because of the importance of ethical behavior within the environment of computerized AISs, we also discuss the topic of computers and ethical behavior here. Finally, the last section of our chapter addresses the importance of privacy and identity theft. The dramatic increase in the number of individuals, companies, and organizations using the Internet draws our attention to the question of personal privacy. What information is collected about us and how much of it is authorized? We focus on the issue of collection and protection of this information.

COMPUTER CRIME, ABUSE, AND FRAUD

Articles in *Fortune, Business Week, The Wall Street Journal, Computerworld, Security Focus*, and *WIRED* all testify to the high level of public interest in computer crime, abuse, and fraud. Although data on computer crime and fraud are limited, at least three reputable organizations conduct surveys that help us understand the breadth and depth of these crimes. First, the **Computer Security Institute (CSI)** conducts an annual survey to help determine the scope of computer crime in the United States. The respondents to this survey are computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions, and universities.

Second, KPMG, a global network of professional firms providing audit, tax, and advisory services, conducts surveys on fraud and business integrity. Survey participants are the business professionals who work for one of the top 2,000 companies listed in Dun and Bradstreet. Third, the **Association of Certified Fraud Examiners (ACFE)**—an international professional organization committed to detecting, deterring, and preventing fraud and white-collar crime—conducts a biannual survey and publishes the results in its *Report to the Nation on Occupational Fraud and Abuse*. The participants in this survey are its members, each of whom provides detailed information on one occupational fraud case he or she had personally investigated within the past two years.

Distinguishing Between Computer Crime, Computer Abuse, and Fraud

Although the terms ''computer crime'' and ''computer abuse'' seem to describe the same problem, there is a subtle difference between them. C**omputer crime** involves the manipulation of a computer or computer data, by whatever method, to dishonestly obtain money, property, or some other advantage of value, or cause a loss. In contrast, **computer abuse** means the unauthorized use of, or access to, a computer for purposes contrary to the wishes of the computer's owner.[1] Thus, a perpetrator commits a computer crime when he or she gains an illegal financial advantage or causes measurable loss to a person, company, or organization, and computer abusers are mischievous pests with such motives as ''revenge'' or ''challenge.''

Case-in-Point 10.1 In September 2003, armed with an arrest warrant, the FBI searched for Adrian Lamo. The 22-year old had become well-known for exposing gaping security holes at large corporations and then voluntarily helping the companies fix the vulnerabilities he exploited. At the *New York Times* site, Lamo obtained access to the names and Social Security numbers of employees, as well as confidential information on customers and business operations at the *Times*. Lamo told the *Times* of their vulnerability through a *SecurityFocus* reporter. Unfortunately for Lamo, the *New York Times* was not grateful and initiated an investigation.[2]

The term ''computer crime'' is really a misnomer because *computers* do not commit crimes—people do. Figure 10-1 describes several cases that might qualify as computer crimes or abuses. In the first case, the primary objective was to disrupt a computer network—not personal gain. The second case is neither a computer crime nor an abuse. Rather, ''misrepresentation'' would probably more accurately describe the problem. In the third case, a computer screen was damaged but the loss would probably not be a criminal charge. In the fourth case, the attempt to sell credit information would be a criminal offense. In the fifth case, no computer was used, so it is difficult to call this a ''computer crime.'' Finally, although the sixth case involved a computer and resulted in personal gain, it is perhaps more accurate to describe this as ''fraud.''

Another example of a computer offense that could be either a crime or an abuse is a **logic bomb**. This is a computer program that remains dormant until some specified circumstance or date triggers the program to action. Once ''detonated,'' a logic bomb program sabotages a system by destroying data and/or disrupting computer operations.

Case-in-Point 10.2 Donald Burleson was a disgruntled computer programmer who set off a logic bomb that erased 168,000 sales commission records at his former company.

[1] Vogon International website: www.vogon-international.co.uk.

[2] Kevin Poulsen, *Security Focus*, September 2003.

1. A graduate student infected a computer network with a virus that eventually disrupted over 10,000 separate systems.
2. A company accused a computer-equipment vendor of fraudulently representing the capabilities of a computer system, charging that the full system was never delivered and that the software was inadequate.
3. In a fit of resentment, a keyboard operator shattered an LCD screen with her high-heeled shoe.
4. Some employees of a credit bureau sent notices to some of the individuals listed as bad risks in its files. For a fee, the employees would withhold the damaging information, thereby enhancing the credit worthiness of the applicants.
5. A computer dating service was sued because referrals for dates were few and inappropriate. The owner eventually admitted that no computer was used to match dates, even though the use of a computer was advertised.
6. A programmer changed a dividends-payment program to reduce the dividends of selected stock-holders, and to issue a check to himself for the sum of the reductions—$56,000.

FIGURE 10-1 Examples of computer crimes.

Consequently, company paychecks were held up for a month. He embedded the logic bomb in a legitimate program, which he designed to go off periodically to erase still more records. But a fellow programmer who was testing a new employee bonus system discovered the bomb before it could execute again. The company's computers were shut down for two days while the bomb was located and diffused.

The type of computer crime with which most professional accountants are familiar is financial fraud. Statement on Auditing Standards No. 99 identifies two types of such fraud: (1) fraudulent financial reporting and (2) misappropriation of assets.[3] *Fraudulent financial reporting* (‘‘cooking the books’’) happens when corporate officials such as senior-ranking executives intentionally falsify accounting records to mislead analysts, creditors, or investors. As a result, the annual financial statements do not fairly represent the true financial condition of the firm. The corporate scandals discussed in Chapter 1 are examples of this type of fraud.

Misappropriation of assets is usually committed by employees within an organization, although individuals can collude with outside conspirators to perform such acts as well. The ACFE calls this type of crime *occupational fraud* and has developed a ‘‘fraud tree’’ to describe the many ways that employees can misappropriate assets from an organization. Examples (Figure 10-2) include skimming, larceny, payroll tampering, and check tampering. Most of these activities directly involve accounting information systems.

Case-in-Point 10.3 Computer programmers use the **salami technique** to steal small amounts of money from many accounts over time. In one instance, the frustrated chief accountant for a California produce grower systematically increased each of the company's production costs by a fraction of a percent, which he subsequently raised over time. Because all business expenses were rising during the same period, no single account or expense called attention to the fraud, and the accountant was able to enter these small amounts into the accounts of dummy customers, which he then pocketed. He was eventually caught when an alert bank teller brought a check to her manager's attention that the accountant tried to cash because she did not recognize the payee's name on it.

[3] Statement on Auditing Standards (SAS) No. 99, *Consideration of Fraud in a Financial Statement Audit* (AICPA 2003).

Asset Class	Type of Fraud	Example
Cash	Larceny	Direct theft or removal from bank deposit
	Skimming	Non-reporting or under-reporting of sales
		Write-offs of legitimate receivables as bad debts
		Lapping schemes
	Fraudulent disbursements	Payments to ghost companies or employees
		Payments for fictitious goods or services
		Multiple payments for the same bill
		Forged checks
		Altered payee on legitimate check
		False refunds
Inventory and all other assets	Misuse	Use of corporate limousine or jet for personal travel
	Larceny	Theft of raw materials or finished goods
		Fictitious inventory adjustments
		Non-reporting or under-reporting of received goods

FIGURE 10-2 Examples of asset misappropriation.

Computer Crime Legislation

A strict definition of computer crime must be found in the law. Such definitions are important because they determine what law enforcement officials can prosecute as well as how statistics on such crimes are accumulated. Both federal and state statutes govern computer usage.

Federal Legislation.

Figure 10-3 lists some important federal legislation governing activities involving computers. Of these acts, the most important is probably the **Computer Fraud and Abuse Act of 1986** (CFAA), which was amended in 1994 and 1996. This act defines computer fraud as any illegal act for which knowledge of computer technology is essential for its perpetration, investigation, or prosecution. The following paragraphs identify the fraudulent acts found in the Computer Fraud and Abuse Act and give examples of each type of crime.

1. ***Unauthorized Theft, Use, Access, Modification, Copying, or Destruction of Software or Data.*** The PC manager at a King Soopers supermarket in Colorado was called repeatedly to correct computer errors that were thought to be responsible for a large number of sales voids and other accounting errors. Eventually, the company discovered that this manager was in fact the cause of these problems. Over the course of five or more years, officials estimate that he and two head clerks used a number of simple methods to steal more than $2 million from the company—for example, by voiding sales transactions and pocketing the customers' cash payments.
2. ***Theft of Money by Altering Computer Records or the Theft of Computer Time.*** To commit an inventory fraud, several employees at an east coast railroad entered data into their company's computer system to show that more than 200 railroad cars were scrapped or destroyed. These employees then removed the cars from the railroad system, repainted them, and sold them.

Fair Credit Reporting Act of 1970. This act requires that an individual be informed why he or she is denied credit. The act also entitles the individual to challenge information maintained by the credit-rating company and to add information if desired. Seven years after this law was put into effect, the annual number of complaints filed under it exceeded 200,000.

Freedom of Information Act of 1970. This is a federal ‘‘sunshine law’’ guaranteeing individuals the right to see any information gathered about them by federal agencies.

Federal Privacy Act of 1974. This act goes further than the Freedom of Information Act of 1970 by requiring that individuals be able to correct federal information about themselves, by requiring that agency information not be used for alternate purposes without the individual’s consent, and by making the collecting agency responsible for the accuracy and use of the information. Under this act, an individual may ask a federal judge to order the correction of errors if the federal agency does not do so.

Small Business Computer Security and Education Act of 1984. This act created an educational council that meets annually to advise the Small Business Administration on a variety of computer crime and security issues affecting small businesses.

Computer Fraud and Abuse Act of 1986. This act makes it a federal crime to intentionally access a computer for such purposes as (1) obtaining top-secret military information, personal financial or credit information; (2) committing a fraud; or (3) altering or destroying federal information.

Computer Fraud and Abuse Act (1996 amendment). This act prohibits unauthorized access to a protected computer, and illegal possession of stolen ‘‘access devices,’’ which includes passwords and credit card numbers.

Computer Security Act of 1987. This act requires more than 550 federal agencies to develop computer security plans for each computer system that processes sensitive information. The plans are reviewed by the National Institute of Standards and Technology (NIST).

USA Patriot Act of 2001. This act gives federal authorities much wider latitude in monitoring Internet usage and expands the way such data is shared among different agencies. However, a judge must oversee the FBI’s use of an email wiretap and the FBI must disclose what was collected, by whom, and who had access to the information that was collected.

Cyber Security Enhancement Act of 2002. This act permits the United States Sentencing Commission to review, and if appropriate, amend guidelines and policy statements applicable to persons convicted of a computer crime to reflect the serious nature of (1) the growing incidence of computer crimes, (2) the need for an effective deterrent, and (3) appropriate punishment to help prevent such offenses.

CAN-SPAM Act of 2003. This act requires unsolicited commercial email messages to be labeled, to include opt-out instructions, and to include the sender’s physical address. It prohibits the use of deceptive subject lines and false headers in messages. This law took effect on January 1, 2004.

FIGURE 10-3 Federal legislation affecting the use of computers.

3. ***Intent to Illegally Obtain Information or Tangible Property Through the Use of Computers.*** One case of industrial espionage involved Reuters Analytics, whose employees were accused of breaking into the computers of their competitor, Bloomberg, and stealing lines of programming code. These instructions were supposedly used in software that provides financial institutions with the capability to analyze historical data on the stock market.

4. ***Use or the Conspiracy to Use Computer Resources to Commit a Felony.*** Paul Sjiem-Fat used desktop publishing technology to perpetrate one of the first cases of computer forgery. Sjiem-Fat created bogus cashier’s checks and used these checks to buy computer equipment, which he subsequently sold in the Caribbean. He was caught while trying to steal $20,000 from the Bank of Boston. The bank called in the Secret Service, which raided his apartment and found nine bogus checks totaling almost $150,000. Sjiem-Fat was prosecuted and sent to prison.

5. ***Theft, Vandalism, or Destruction of Computer Hardware.*** A disgruntled tax payer became enraged over his tax bill. He was arrested for shooting at an IRS computer through an open window of the building.
6. ***Trafficking in Passwords or Other Login Information for Accessing a Computer.*** Two former software developers of Interactive Connection (now known as Screaming Media) were arrested for breaking into Interactive's computer system one night. They allegedly stayed on the system for about four hours and copied proprietary files and software.
7. ***Extortion that Uses a Computer System as a Target.*** A disgruntled employee of a European company removed all of the company's tape files from the computer room. He then drove to an off-site storage location and demanded half a million dollars for their return. He was arrested while trying to exchange the data files for the ransom money.

State Legislation. Every state now has at least one computer crime law. Most of the laws have provisions that (1) define computer terms (many of which vary from state to state), (2) define some acts as misdemeanors (minor crimes), and (3) declare other acts as felonies (major crimes). These laws also require willful intent for convictions. Thus, words like *maliciously, intentionally*, or *recklessly* often appear in the wording of the computer-crime laws, and willful intent must be established for a successful prosecution. The National Center for Computer Crime Data (NCCCD), a collector of computer-crime statistics, reports that 77% of computer cases brought to state courts end in guilty pleas and that another 8% of the defendants are found guilty at trials.

Computer Crime Statistics

No one really knows how much is lost each year as the result of computer crime and abuse. One reason for this is the fact that a large proportion of computer crime and abuse takes place in private companies, where it is handled as an internal matter. We have no laws that require organizations to report computer offenses. According to the 2005 Computer Crime and Security Survey, fewer than 40% of the respondents who had experienced computer intrusions in the past 12 months reported them. The principal reason managers gave for not reporting intrusions was negative publicity that might negatively impact their stock price or image (43%), and the next most important reason was their fear that competitors would use the information to advantage (33%). The 2008 ACFE Report to the Nation suggests that the number of occupational fraud cases referred to law enforcement is somewhat higher—almost 69%.[4]

The most important reason we know so little about computer offenses is because we believe that most of it is not discovered. Recently, for example, the FBI estimated that only 1% of all computer crime is detected. Other estimates of computer crime detection are between 5–20%. We mostly catch computer criminals through luck, chance, or accident. This is why experts believe the computer crime that is detected is only the tip of the iceberg.

Despite our lack of complete statistics, there are several reasons why we believe computer crime is growing. One reason is the exponential growth in the use of computer resources—e.g., microcomputers, computer networks, and the Internet. As more people become knowledgeable about how to use computers, more people are in a position to compromise computer systems.

[4] Source: http://www.acfe.com/fraud/report.

Another reason why we believe computer crime is growing is because of continuing lax security. There are millions of microcomputer users in the world, but many of them are not aware of, or conscientious about, computer security. Then, too, some users are dishonest and have a new tool with which to commit frauds. Lastly, many websites now give step-by-step instructions on how to perpetrate computer crimes. For example, an Internet search found more than 17,000 matches for ‘‘denial of service,’’ and there are now thousands of websites that detail how to break into computer systems or disable web servers.

Case-in-Point 10.4 Dan Farmer, who wrote SATAN (a network security testing tool), tested 2,200 high-profile websites at governmental institutions, banks, newspapers, and so forth. Only three of these websites detected his probes and contacted him to find out what he was trying to do. His conclusion: two out of every three websites have serious vulnerabilities and most of the control procedures at these sites are ineffective.[5]

The FBI, in partnership with the National White Collar Crime Center, established the Internet Fraud Complaint Center (IFCC) in May 2000 to provide cyber crime victims a point of contact for reporting computer crime and abuses. The IFCC changed its name in December 2003 to the Internet Crime Complaint Center (IC3—see www.ic3.gov) to reflect the broad nature of complaints that it handles, including international money laundering, online extortion, intellectual property theft, identity theft, online scams, and computer intrusions. In 2008, almost 275,300 online fraud complaints were reported, compared to only 75,000 in 2002. The majority of the complaints in 2008 concerned non-delivered merchandise purchased on the Internet (32.9% of complaints), followed by auction fraud (25.5% of complaints).[6]

The Importance of Computer Crime and Abuse to AISs

The absence of good computer-crime statistics does not detract from the importance of computer crime and abuse on accounting information systems. One reason for this is because AISs help control financial resources and thus are often the favored targets of external crooks or dishonest employees. Also, as noted previously, AISs are prized targets for disgruntled employees seeking to compromise computer systems for revenge. A third reason is because accountants are responsible for designing, selecting, or implementing the control procedures that protect AISs.

Finally, computer crime is important because both the government and the investing public can be misled if such crime compromises the accuracy and completeness of corporate financial statements. Using a computer, fraud perpetrators are able to steal more, in much less time, with much less effort, and leave little or no evidence. Consequently, computer fraud is typically much more difficult to detect than other types of fraud. At any point in time, the FBI is investigating approximately 800 separate incidents of economic espionage.

Computer crime and abuse are also significant because of the large proportion of firms that suffer million-dollar losses due to frauds, computer viruses, unauthorized access, and denial of service attacks. As stated in the opening quote of this chapter, the 2008 ACFE Report to the Nation estimates that the annual total losses from occupational fraud are almost $1 trillion (not all of which is computer-based). The 2008 annual survey of the Computer Security Institute estimates that the average cost to target organizations from a computer-abuse incident is about $500,000—an amount whose financial impact can range from ‘‘substantial’’ to ‘‘catastrophic’’ to the victim.

[5] Source: http://www.g4tv.com/techtvvault/features/3392/Interview_SATANs_Dan_Farmer.html.

[6] Source: http://www.ic3.gov/media/annualreports.

THREE EXAMPLES OF COMPUTER CRIME

Computer crime is perhaps best understood by studying selected cases. As one reads the fascinating accounts of different computer crimes, a pattern begins to emerge. One type of crime depends mostly on the falsification of input data, while others depend on unauthorized access to computerized files. This section of the chapter examines three specific cases of computer crime.

Compromising Valuable Information: The TRW Credit Data Case

A major class of computer crime involves illegal access to, or misuse of, the information stored in an AIS, and is thus valuable-information computer crime. In the TRW Credit Data case, the valuable information involved was computerized credit data. TRW (now called Experian) was one of several large credit-rating companies in the United States. When the fraud was discovered, the company was collecting and disseminating credit information on approximately 50 million individuals. Clients of TRW included banks, retail stores, and such credit-conscious concerns as Diner's Club, American Express, MasterCard, Visa, Sears, and several leasing establishments.

TRW advised its clients of bad credit risks on the basis of the information maintained in its databases. However, that information could be changed. The fraud began when six company employees, including a key TRW clerk in the consumer relations department, realized this fact and began selling good credit to individuals with bad credit ratings. The names and addresses of the bad credit risks were already on file. It merely remained to contact these individuals and inform them of a newfound method of altering their records. Accordingly, the perpetrators approached individuals with bad credit ratings and offered them a clean bill of health in return for a ''management fee.''

Those people who decided to buy good credit ratings paid TRW employees ''under the table,'' and the clerk in the consumer relations department then inserted into TRW's credit files whatever false information was required to reverse the individual's bad credit rating. In some cases, this required deleting unfavorable information that was already stored in the individual's credit record. In others, it required adding favorable information. Fees for such services varied from a few hundred dollars to $1,500 per individual. Ironically, the TRW clerk who ultimately input the false information to the computer system received only $50 for each altered record. However, the losses resulting from these activities were not so inconsequential. Independent estimates have placed this figure at close to $1 million.

The principal victims of the fraud were TRW's clients who acted on credit information that ultimately turned out to be inaccurate. Exactly how many file records were altered is difficult to say. Lawyers for the prosecution documented 16 known cases of altered file records, but had reason to believe the number exceeded 100 cases. Paradoxically, the prosecution had difficulty acquiring testimonies because the buyers of good credit standing as well as the TRW sellers were technically in violation of the law by conspiring to falsify credit-rating information.

Analysis. **Data diddling** means changing data before, during, or after they are entered into a computer system. The change can delete, alter, or add important system data, especially the data stored in corporate databases. This is a problem because most such data are (1) proprietary, (2) may give a firm a competitive advantage, and (3) are sometimes an organization's most valuable asset (think eBay, for example). Finally, because the data processing tasks in most computerized AIS job streams are automated, the data that are input manually to a system are particularly vulnerable to compromise.

There have been many cases of computer crime involving the alteration of corporate data. In one instance, a clerk for a Denver brokerage altered a transaction to record 1,700 shares of Loren Industries stock worth about $2,500, as shares in Long Island Lighting worth more than $25,000. In a second case, a ring of travel agents in California received prison sentences for compromising an American Airlines reservations system and stealing $1.3 million worth of frequent-flier tickets.

The TRW case involves two key issues: (1) the propriety of the input information used in updating a specific AIS, and (2) the protection afforded both consumers and users in the accuracy and use of credit information that is gathered by a private company. With regard to the first point, it is clear that the fraud was successful only because the perpetrators were able to enter false information into the computer system. This observation points to the importance of control procedures (e.g., the authorization and validation of credit changes) that safeguard the accuracy and completeness of file information. As with many cases of computer crime, the six TRW employees involved in the fraud were caught only by chance: an individual approached with an offer to buy a good credit rating for $600 became angry and called the FBI. Later, the TRW clerk in the consumer relations department decided to turn state's evidence.

The second point involving the protection of the consumer and user of credit information encompasses a much larger issue. In 1970, Congress passed the **Fair Credit Reporting Act**, which requires that an individual be told why he or she is denied credit. The consumer also has the right to contest the information maintained by the credit-rating company, although there is clearly a vast difference between the right to *challenge*, versus the right to *change*, credit information.

Directly after the Fair Credit Reporting Act went into effect, TRW reported consumer inquiries increased a hundred fold, and at the time the fraud was detected, approximately 200,000 consumers annually were complaining about their credit ratings. The fact that, by TRW's own admission, fully one third of these inquiries resulted in a file change or update is unsettling. Moreover, it is not known how much more information collected by TRW is still inaccurate but simply not challenged—for example, because an individual is not aware of an inaccuracy, or because the consumer does not know his or her rights under the law.

Wire Fraud and Computer Hacking: Edwin Pena and Robert Moore[7]

Voice over Internet Protocol (VoIP) is a technology that allows you to make telephone calls using a broadband Internet connection instead of a regular telephone line. This technology converts your voice signal into digital ones that travel over the Internet and are then converted back to audio ones at the receiver's end.

Edwin Pena, who owned two Florida VoIP wholesale companies, was arrested on June 7, 2006 for hacking into other providers' networks, routing his customers' calls onto those platforms, billing those companies, and then pocketing the proceeds. He was charged with one count of wire fraud and one count of computer hacking. The government claimed that Pena embezzled over $1 million from this scheme, which he used to purchase real estate, cars, and a 40-foot boat. To avoid attention, Pena apparently purchased these items in someone else's name.

[7] Source: http://www.technologynewsdaily.com/node/3252.

The federal government also filed a criminal complaint against Robert Moore of Spokane, Washington, the professional **hacker** who penetrated the networks for Pena. However, Moore admitted his part in the fraud, disclosing that Pena paid him $20,000 for his work. Apparently, Moore scanned a lot of other companies' computer networks searching for vulnerable network ports with which to route calls. For instance, he made over 6 million scans of just AT&T ports between June and October of 2005. After Moore obtained proprietary codes (known as prefixes), he and Pena allegedly flooded providers with test calls until they were able to match up prefixes. Once they matched prefixes, Pena programmed the networks of other companies to use his prefix to route his customers' calls.

Analysis. Hacking is a widespread problem. This is due, in part, to the fact that many computer applications now run on local and wide area networks, where computer files become accessible to unauthorized users. Then, too, the Internet enables users to log onto computers from remote sites, again increasing vulnerability to hacking.

Computer hacking is common in universities, where students often view the activity as a harmless game of ''beating the system.'' Recently, for example, a group of student hackers called the ''Legion of Doom'' stole data from the BellSouth Telephone Company and disrupted its 911 emergency phone system just to see if they could do it. Educational institutions view hacking as a particularly perplexing problem because the need for tight system security conflicts with the objective of providing easy and simple computer access to bona fide users.

Many hackers brag that they can compromise any type of file information once they have successfully logged into a computer system. One way they achieve this is to elevate their system status to that of a ''privileged user'' or ''network manager,'' which is a security level that gains the hackers access to password files, system control data, and other high-security information. These activities are thwarted by using system programming routines that test for, and deny, such bootstrapping and that also immediately communicate such attempts to computer supervisors as possible security violations.

Case-in-Point 10.5 When hackers invaded NDA (a consulting firm in Woburn, Massachusetts), the hackers installed a program that enabled them to record users' passwords and access the network freely. The invaders copied files containing ID codes for cellular phones, gathered sensitive information on NDA's business customers, and then launched similar attacks on those companies.[8]

The maximum penalty for wire fraud is 20 years in prison and a $250,000 fine, and the penalty for computer hacking is a maximum of 5 years in prison and a $250,000 fine. Provisions of the USA Patriot Act of 2001 may help discourage computer hacking by helping federal authorities locate and prosecute hackers. However, the most effective deterrents are likely to be preventive rather than punitive. One helpful tactic is user education—i.e., making potential hackers aware of the ethics of computer usage and the inconvenience, lost time, and costs incurred by victim organizations. Another safeguard is to require user passwords, which limit computer access to bona fide users. But passwords are not foolproof mechanisms, because at present, computers cannot distinguish between authorized employees using their own passwords and unauthorized users entering compromised passwords. Thus, until bio-authorizations such as retina or fingerprint scanners or other cost-effective intrusion detection systems replace them, protecting passwords is paramount. We will review some methods for this in the next section of the chapter.

[8] Source: http://findarticles.com/p/articles/mi_m1154/is_n11_v85/ai_19969629.

Denial of Service: The 2003 Internet Crash[9]

A number of computer viruses and computer worms have gained media attention, but none have been as swift or as ''deadly'' as the Slammer worm. In 2003, this computer worm nearly shut down the Internet in less than 15 minutes. Internet service providers (ISPs) on the east coast of the United States were the first to recognize the problem, but the full impact of this computer worm quickly spread to other countries.

How did this happen? The Slammer worm took advantage of a weakness in Microsoft's SQL Server 2000 software—a weakness that allowed applications to automatically find the right database. As a result, just after midnight on January 25, 2003, over 55 million meaningless database server requests were crossing the globe. The Slammer worm was able to spread hundreds of times faster than any prior worm attack. The unfortunate part is that the total cost to fix the problem was estimated at over $1 billion, and we still do not know who did it or when it might happen again.

Analysis. **Denial of service (DOS) attacks** take many forms, including (1) computer viruses, (2) computer worms, or (3) distributed systems. A **computer virus** is an attachment to other files or programs that destroys computer files, disrupts operating system activities, or damages program software. A computer worm is a separate entity (often considered a type of virus program) that makes working replicas of itself to infect more systems and/or to flood computer networks with excessive email traffic.[10] As suggested by Figure 10-4, ''viruses'' continue to be the number one security problem for modern organizations. A recent survey of 300 private and public computer sites conducted by the International Computer Security Association, in Carlisle, Pennsylvania, found viruses in more than 3% of the survey sites.

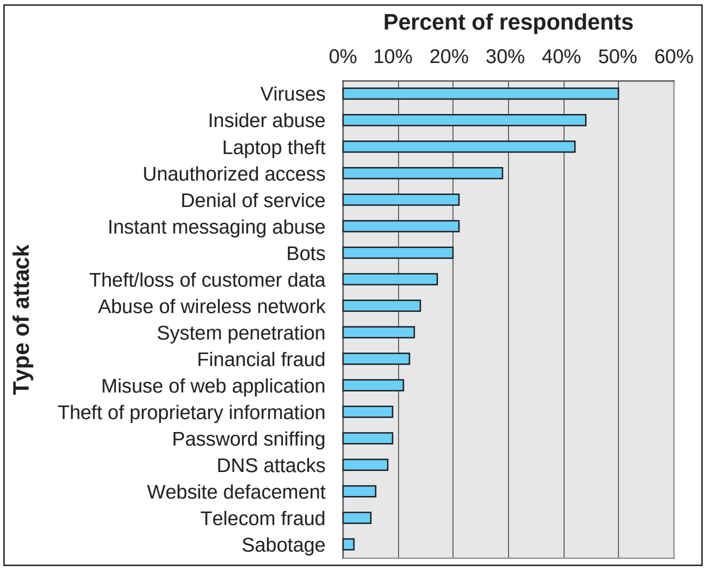

FIGURE 10-4 Percentage of respondents experiencing common types of computer crime and abuse. (Source: 2008 CSI Survey).

[9] Source: P. Boutin, *WIRED*, Issue 11.07, July 2003 (www.wired.com).

[10] Source: J. Elizabeth Strohm, *The America's Intelligence Wire*, August 25, 2003.

Computer worms do not actually destroy data, but merely replicate themselves repeatedly until the user runs out of internal memory or disk space. Unfortunately, the Internet facilitates the spread of virus and worm programs from one system to another, making them the most popular form of computer crime or abuse. Finally with **distributed denial-of-service (DDoS) attacks**, a single virus or worm program manages to enlist the aid of innocent ''zombie computers'' which then send email messages to, or request services from, the target system. The barrage of incoming mail or service requests then overwhelms the target system, typically requiring its owners to disable it.

Most computer viruses reside on secondary storage media, where they hide until finding an opportunity to execute. There are several variations of these viruses. **Boot-sector viruses** hide in the boot sectors of a disk, where the operating system accesses them every time it accesses the disk itself. **Trojan horse programs** reside in legitimate copies of computer programs, for example, spreadsheet programs. Logic bomb programs are similar to Trojan horse programs, except that they remain dormant until the computer system encounters a specific condition, such as a particular day of the year or a particular Social Security number in a file. (Trojan horse and logic bomb programs are termed ''programs'' rather than ''viruses'' because they sometimes contain code to defraud users rather than viruses that destroy or disrupt computer resources.)

The Internet is a perfect environment for computer viruses because so many people use it for email, conducting research, and downloading files or software. For example, a virus might be stored in a java **applet** (i.e., a small program that is stored in a web page and designed to run by web browser software). Friendly applets animate web pages, allow users to play games, or perform processing tasks. But unfriendly applets contain viruses that can infect other computers and cause damage.

Once a programmer stores a computer virus program on the file server of a computer network, the program can affect thousands of other computers or disks before it is detected and eradicated. Estimating the business costs of recovering from a virus infection is difficult. The costs can be small—for example, limited to the inconveniences of reformatting a hard disk and reloading a few software programs. On the other hand, some experts estimate such costs in the billions of dollars annually.

There are a number of ways to thwart computer viruses. These include, but are not limited to: (1) **firewalls**, which limit external access to company computers, (2) anti-virus software, and (3) anti-virus control procedures. **Anti-virus software** are computer programs that scan computer inputs for virus-like coding, identify active viruses that are already lodged in computer systems, clean computer systems already infected, or perform some combination of these activities. Recent versions of Microsoft's Windows operating system incorporate software of this type. Generally speaking, however, anti-virus programs provide less than complete protection because misguided individuals continuously write new, more powerful viruses that can avoid current detection schemes. Even worse, some older anti-virus programs have themselves contained virus routines.

Perhaps one of the most vulnerable areas for many firms and universities is email. Consider the number of emails you send and receive every day, and then multiply that by the number of people at your university—the risk of passing a virus around is very high. Unfortunately, viruses can hide in emails from friends and colleagues because their computer systems have been infected. To help mitigate this problem, your university most likely uses an anti-spam software solution in addition to anti-virus software.

For many microcomputer users, anti-virus control procedures are often better safeguards. These include: (1) buying shrink-wrapped software from reputable sources, (2) avoiding illegal software copying, (3) not downloading suspicious Internet files, (4) deleting email messages from unknown sources before opening them, and (5) maintaining complete backup files in the event you must rebuild your system from scratch. Additional safeguards include loading operating systems only from your own disks, being wary of public-domain software available on Internet bulletin boards, and being suspicious of unusual activity on your computer system—for example, spontaneous disk writing that you did not initiate.

In organizational settings, effective control procedures against computer viruses include educating users about viruses and encouraging computer users to follow the virus prevention and detection techniques just discussed. Additional control procedures include (1) adopting policies that discourage the free exchange of computer disks or externally acquired computer programs, (2) requiring strong passwords that limit unauthorized access to computing resources, and (3) using anti-virus filters on local and wide-area networks.

MITIGATING COMPUTER CRIME AND FRAUD

What can organizations do to protect themselves against computer abuse? Experts note that, for all their intricacy and mystique, we can protect computer systems from crimes, abuses, and fraud just as well as we can manual systems, and sometimes better. For example, computers can be programmed to automatically search for anomalies and to print exception conditions on control reports. These computerized monitoring systems are often superior to manual surveillance methods because they are automatic and can screen 100%, instead of merely a sample, of the target population data. An illustration is the New York Stock Exchange, which now uses an **Integrated Computer-Assisted Surveillance System (ICASS)** to search for insider trading activities. This section of the chapter discusses several methods for thwarting computer crimes, abuses, and fraud.

Enlist Top-Management Support

Most experts agree that computer security begins with top management and security policies. Without such policies, for example, organizations can only expect limited employee (1) compliance with security procedures, (2) sensitivity to potential problems, or (3) awareness of why computer abuse is important. Unfortunately, many top managers are not fully aware of the dangers of computer crime, abuse, and fraud, and therefore are not sufficiently concerned about this type of offense. Computer safeguards are only effective if management takes computer crime seriously and chooses to financially support and enforce control procedures to stop, or at least minimize, computer crimes. The complaint of many mid-level security managers is that they must justify their funding requests for investments in appropriate levels of computer security for a firm. Thus, the importance management places on computer safeguards might be measured by the level of funding allocated to IT security.

Increase Employee Awareness and Education

Ultimately, controlling computer crime means controlling people. But which people? The idea that computer crimes are ‘‘outside jobs’’ is a myth. With the exception of hackers, most computer abusers are the employees of the same companies at which the crimes take place. Many retail firms have clear prosecution policies regarding shoplifting. In contrast, prosecution policies associated with other types of employee fraud are notable for their absence in most organizations. Yet, the evidence suggests that prosecuting computer crimes may be one of the most effective restraints on computer crime.

In fairness, employees cannot be expected to automatically understand the problems or ramifications of computer crime. Thus, another dimension of preventing computer crime is employee education. Informing employees of the significance of computer crime and abuse, the amount it costs, and the work disruption it creates helps employees understand why computer offenses are serious matters. Studies suggest that informal discussions, periodic departmental memos, and formal guidelines are among the most popular educational tools for informing employees about computer crime and abuse. Requiring new hires to sign security statements indicating that they have received, read, and understand policy statements can also help.

According to the 2005 – 2006 KPMG Integrity Survey,[11] companies with comprehensive ethics and compliance programs have more favorable results across the board than companies without such programs. For example, organizations with these programs reported fewer observations of misconduct and higher levels of employee confidence in management's integrity. These programs were also cited as mitigating a number of conditions that might foster misconduct, such as: (1) pressure to do whatever it takes to meet targets, (2) belief that policies and procedures are easy to bypass or override, and (3) belief that rewards are based on results, regardless of the method used.

One final idea regarding employee conduct comes from the 2008 Association of Certified Fraud Examiners *Report to the Nation*. This survey revealed that almost half of all the fraud discussed in the report was first discovered by tips from fellow employees, customers, or vendors. Providing formal channels through which individuals can inform management of suspect activity—for example, through company websites—as well as rewarding those who provide such information, seem to be two of the most effective things that organizations can do to curb occupational fraud and embezzlement.

Assess Security Measures and Protect Passwords

Common sense dictates that organizations should regularly survey their computer security measures and assess potential areas of vulnerability. Nearly all organizations use firewalls, anti-virus software, and access controls, but many are not as conscientious about performing periodic security reviews. An important security process that organizations should consider is evaluating employee practices and educating users to protect their own computers. Figure 10-5 provides a list of ten recommended steps for safeguarding personal computers.

Protecting passwords is an important dimension of computer security because they are the ''keys to the kingdom'' (of valuable corporate data). Hackers use a variety of tactics to steal such passwords, including (1) posing as a legitimate user and ''borrowing'' them from unsuspecting employees, (2) creating phishing websites that pose as surveys that ask users to input their passwords for security purposes, or (3) using simulation programs that try all the words in a standard dictionary as potential passwords. To thwart these strategies, users should (1) be trained to not ''loan'' their passwords to others or tape them to their monitors, (2) understand that most businesses will not ask for their passwords on a web screen, and (3) use **strong passwords**—i.e., passwords that are difficult to guess. Examples are long passwords (e.g., 20 characters), nonsense words (e.g., non-English words not found in dictionaries) or words with embedded capitals or random numbers. Another control is to require employees to change their passwords periodically. A third control is to install password-checking software in file servers that test passwords for such requirements.

[11] KPMG Forensic Integrity Survey 2005 – 2006, http://www.us.kpmg.com/news/index.asp?cid = 2051.

1. **Keep your firewall turned on**. Firewalls help protect your computer from hackers who might try to gain access to it, delete information, or steal passwords or other sensitive information.
2. **Install or update your anti-virus software**. Anti-virus software helps protect your computer from such malicious code as viruses or worms, and can be set to update automatically.
3. **Install or update your anti-spyware technology**. Spyware is just that—software that is secretly installed on your computer and that allows others to observe your activities on it. Inexpensive anti-spyware software is readily available for download on the Internet or at local computer stores.
4. **Keep your operating system up to date**. Software developers regularly update their operating systems to stay current with technology requirements and fix security holes.
5. **Do not provide personal information online**. Hackers create phishing websites to lure visitors into providing their personal information and therefore steal their identity. Most companies will not ask you to provide your login name, password, account number, or similar personal information online.
6. **Be careful what you download**. Downloading email attachments can thwart even the most vigilant anti-virus software. Never open an email attachment from someone you don't know, and be wary of forwarded attachments from anyone.
7. **Turn off your computer at night**. Although it's nice to always have your computer ready for action, the downside of ''always on'' is that it makes it more susceptible to hacker attacks. The safest computer is one that isn't on.
8. **Create backups often**. Computers are not infallible, and all hard disk drives eventually fail. Creating duplicate copies of your important files and storing them offsite enables you to easily recover from such problems. The authors recommend the automated backup services of a cloud service provider, as discussed in Chapter 2.
9. **Use surge protectors**. Power surges can ''fry'' your computer, but even the least-expensive surge protector can guard against most such events.
10. **Protect passwords**. Many websites and computer systems now require logon names and passwords, but writing them on sticky notes stuck to your computer's monitor or keyboard is not a good idea. Try to find safer places to store the ones you can't commit to memory.

FIGURE 10-5 Ten simple steps to safer personal computers.

Hackers often use a tactic called **social engineering** to gain access to passwords (i.e., posing as bona fide employees and convincing network administrators to give them passwords over the phone). In general, the practice of giving passwords to unknown employees over the telephone compromises standard security procedures, and therefore should not be allowed.

Two additional password safeguards are lock-out systems and dialback systems. **Lock-out systems** disconnect telephone users after a set number of unsuccessful login attempts, thereby thwarting microcomputer users from using dictionary programs. Similarly, **dialback systems** first disconnect all login users but reconnect legitimate users after checking their passwords against lists of bona fide user codes. Dialback systems may be even more effective than lock-out systems because only authorized users at already-recognized stations are reconnected. Dialback security is also a useful strategy against social engineering, because hackers are unwilling to reveal their identities when making bogus requests for passwords.

Implement Controls

Most computer crime and abuse succeeds because of the absence of controls rather than the failure of controls. There are many reasons why businesses do not implement control procedures to deter computer crime. One is the all-too-common belief of those managers who have not suffered a computer crime that they have nothing to fear. Further, charities and not-for-profit organizations often believe that their missions somehow insulate them from such crimes. Then, too, those businesses that do not have a specific computer security officer have no one to articulate this concern or to argue for specific control procedures. Finally, at least some businesses do not feel that security measures are cost-effective—until they incur a problem!

Case-in-Point 10.6 To execute a disbursement fraud, one man used a desktop publishing package to prepare fictitious bills for office supplies that he then mailed to companies across the country. He kept the dollar amount on each bill less than $300, and found that an amazingly large percentage of the companies paid the bills without question—probably because many organizations automatically pay vendor invoices for small amounts.

The solution to the computer-security problems of most organizations is straightforward: design and implement controls. This means that organizations should install control procedures to deter computer crime, managers should enforce them, and both internal and external auditors should test them. Experts also suggest that employee awareness of computer controls and the certainty of prosecution may also act as deterrents to computer crime. Certainly, the enactment of the Sarbanes-Oxley Act of 2002 has placed a much greater emphasis on strong internal controls, including criminal offenses for senior executives who knowingly disregard such precautions. We talk more about internal controls in Chapters 11 and 12, and cover the Sarbanes-Oxley Act in more depth in Chapter 14.

In the United States, a disproportionate amount of security break-ins occur during the end-of-the-year holiday season. Reasons for this include: (1) extended employee vacations and therefore fewer people to ‘‘mind the store,’’ (2) students are out of school and consequently have more free time on their hands, and (3) counterculture hackers get lonely at year-end and increase their attacks on computer systems. Thus, it is especially important to make sure that effective control procedures are in place during the holidays.

Identify Computer Criminals

To prevent specific types of crimes, criminologists often look for common character traits that can be used to screen potential culprits. What are the characteristics of individuals who commit computer crimes or abuse, and what can be done to create a composite profile that organizations can use to evaluate job applicants?

Non-Technical Backgrounds. A company’s own employees—not external hackers—perpetrate most computer crime and abuse. How technically competent are such employees? Figure 10-6 identifies the job occupations of computer criminals and abusers from a survey performed by Hoffer and Straub. Although this figure suggests that some computer offenses are committed by those with strong technical backgrounds, this study found that almost as many computer offenses are perpetrated by clerical personnel, data-entry clerks, and similar individuals with limited technical skills. A similar study by the U.S. Sentencing Commission (USSC) found that most of the 174 computer criminals convicted under the Computer Crime and Abuse Act of 1986 were corporate insiders with only ‘‘pedestrian levels’’ of computer expertise. There is good reason for this. It is usually easier and safer to alter data before they enter a computer than midway through automated processing cycles. Then too, input data can often be changed anonymously, whereas most computerized data cannot. These facts explain why many computer criminals are not even computer literate, and also why computer security must extend beyond IT personnel.

Programmers and systems analysts	27%
Clerical, data entry, and machine operators	23%
Managers and top executives	15%
Other system users	14%
Students	12%
Consultants	3%
Other information processing staff	3%
All others	3%
Total	100%

FIGURE 10-6 Occupations of computer-abuse offenders.

Non-Criminal Backgrounds. The USSC study also found that most of the convicted computer criminals had no prior criminal backgrounds. In addition, most computer criminals tend to view themselves as relatively honest. They argue, for example, that ''beating the system'' is not the same as stealing from another person or that they are merely using a computer to take what other employees take from the supply cabinet. Furthermore, many perpetrators think of themselves as long-term borrowers rather than thieves, and several have exercised great care to avoid harming individuals when committing their computer offenses.

Education, Gender, and Age. Although most media reports suggest that computer offenders are uniformly bright, motivated, talented, and college-educated individuals, the average computer criminal often does not fit this profile. In the ACFE 2008 Report to the Nation, for example, over half of the perpetrators did not have a college degree. But, according to the report, highly-educated fraudsters were able to steal more—see Figure 10-7. Because we believe that most computer crime and abuse are not detected—or prosecuted when it is detected—we do not know how representative these observations are for the ''general population'' of computer offenders.

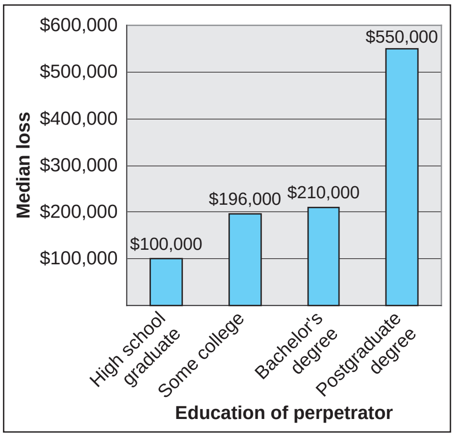

FIGURE 10-7 Median fraud losses, classified by the education level of the perpetrator. Source: *2008 ACFE Report to the Nation*.

Don’t Forget Physical Security

An old adage in the computer security industry is that ‘‘a good hammer beats a strong password every time.’’ What this means is that physical safeguards can be even more important than logical ones in deterring computer crime and abuse. Examples of physical security include protecting LAN servers and administrative work stations, enforcing ‘‘clean-desk policies’’ for employees, and protecting employee laptops against theft (see again Figure 10-4).

Case-in-Point 10.7 The administrators at one university believed that their desktop computers were safe as long as employees locked their individual office doors at night. But the university usually kept the buildings unlocked. The folly of this thinking became clear one morning when officials discovered that thieves had simply brought a ladder that allowed them to climb through the false ceiling of a building to steal over 30 PCs from one of the computer labs on campus.[12]

Organizations must also be able to recover from computer security breaches or losses when they do occur. One safeguard is to implement backup procedures, which we cover in more detail in the next chapter. Another safeguard is to develop and test a disaster recovery plan that enables a business to replace its critical computer systems in a timely fashion, which we discuss more comprehensively in Chapter 12. As suggested by the Case-in-Point above, monitoring cameras, motion detectors, and ‘‘insurance’’ are also important security measures.

Finally, organizations should be careful about how they dispose of outdated computers. Although state and federal environmental laws affect such disposals, our primary concern is the sensitive data stored on the hard drives of these PCs. Reformatting these drives is usually not enough—the data may still be retrieved with software tools available on the web. A better approach is either to use specialized file deletion software programs or to physically destroy the disk drives themselves.

Case-in-Point 10.8 In 2003, two MIT graduate students reported in an industry journal that, after purchasing 129 used hard drives, they found more than a third of them still contained “significant personal information,” such as credit card numbers and a year’s worth of transactions and account numbers from an ATM.[13]

Recognize the Symptoms of Employee Fraud

The clues that signal some computer offenses can be subtle and ambiguous, but many are rather obvious. For example, the study conducted by KPMG concluded that nearly half the employee fraud would have been detected more quickly if obvious telltale symptoms had not been ignored. Although recognizing the symptoms of computer offenses will not prevent computer crime, knowing the telltale signs may help individuals detect and report it, which will help minimize the potential damage to the victim organization. Consider, for example, Case-in-Point 10.9.

Case-in-Point 10.9 The Elgin Corporation was a manufacturing company that had created its own health care plan for its employees. The plan was self-insured for medical claims under

[12] Source: From the authors.

[13] Source: http://www.whitecanyon.com/used-hard-drives-pc-05-2003.php.

> $50,000, which it handled internally, but plan administrators forwarded claims for larger amounts to an independent insurance company. The managers of Elgin Corporation believed that the company had excellent control procedures for its system, which included both internal and external audits. Yet, over a period of four years, the manager of the medical claims department was able to embezzle more than $12 million from the company.

Although the ''Elgin'' name is fictitious, the events described above are not. How can such events be avoided? Here are five typical symptoms of computer fraud that actually occurred at the Elgin Corporation.

Accounting Irregularities. To embezzle funds successfully, employees commonly alter, forge, or destroy input documents, or perform suspicious accounting adjustments. An unusually high number of such irregularities are cause for concern. At the Elgin Corporation, no one noticed that payments to 22 of the physicians submitting claims to the company were sent to the same two addresses.

Internal Control Weaknesses. Control procedures are often absent, weak, or ignored in computer fraud. At the Elgin Corporation, the medical claims manager had not taken a vacation for years, those employees submitting claims were never sent confirmation notices of the medical payments made in their behalf, and the physicians receiving these payments were never first investigated or approved.

Unreasonable Anomalies. Perhaps the most important clue to computer fraud is the presence of many odd or unusual anomalies that somehow go unchallenged. Examined critically, such anomalies are unreasonable and require observers to suspend common sense. At the Elgin Corporation, for example, why were 100% of the medical payments to those 22 physicians all paid from the self-insured portion of the company program? Why were checks to those 22 physicians always endorsed by hand and deposited in the same two checking accounts? And why did some of the medical claims include hysterectomies for male employees?

Lifestyle Changes. Employees who miraculously solve pressing financial problems or suddenly begin living extravagant lifestyles are sometimes merely broadcasting fraud. At the Elgin Corporation, why did the medical claims manager announce that she had inherited a lot of money but never took a vacation? And why did she treat her employees to lunches in chauffeured limousines?

Behavioral Changes. Employees who experience guilt or remorse from their crimes, or who fear discovery, often express these feelings in unusual behavior. At the Elgin Corporation, employees joked that the medical claims manager had recently developed a ''Jekyll and Hyde personality,'' including intense mood swings that were unusual even for her.

Employ Forensic Accountants

When an organization suspects an ongoing computer crime or fraud, it can hire **forensic accountants** to investigate its problems, document findings, and make recommendations. Many such individuals are professional accountants who have passed the two-day certified fraud examiner (CFE) examination administered by the ACFE.

Forensic accountants have the required technical and legal experience to research a given concern, follow leads, establish audit trails of questionable transactions, document their findings, organize evidence for external review and law enforcement bodies, and (if necessary) testify in court. Most use specialized software tools to help them perform their tasks—for example, **Audit Command Language (ACL)** for auditing tasks, and **EnCase** for file copying, custody documentation, and other forensic activities. Forensic accounting is one of the fastest-growing areas of accounting, and there are now more than 27,000 CFEs working in organizations such as the FBI, CIA, law firms, and CPA firms.

ETHICAL ISSUES, PRIVACY, AND IDENTITY THEFT

Computerized AISs often raise ethical issues that we did not have to face under manual AISs. An example is the practice of unauthorized software copying. Thus, thwarting computer crime, abuse, or fraud is sometimes more dependent on ethical behavior than observing legal restrictions. Ethics is a set of moral principles or values. Therefore, ethical behavior involves making choices and judgments that are morally acceptable and then acting accordingly. Ethics can govern organizations as well as individuals. In the context of an organization, an underlying ethical principle is that each individual in the organization has responsibility for the welfare of others within the organization, as well as for the organization itself. For example, the managers of a company should make decisions that are fair to the employees as well as beneficial to the organization.

Ethical Issues and Professional Associations

Ethical concerns are often a part of of computer abuse. In cases involving hacking, for example, ‘‘ignorance of proper conduct’’ or ‘‘misguided playfulness’’ may be the problem. To some, the challenge of defrauding a computer system and avoiding detection is irresistible because success brings recognition, notoriety, and even heroism. In these cases, ethical issues are overlooked and the costs of recovering from the abuse are ignored. The acceptability of these motives comes down to issues of morality. But ‘‘morality’’ in corporate cultures is typically a relative value. In one case, for example, a man named Fred Darm stole a computer program from a rival firm through his computer terminal. At his trial, the defense argued that it was common practice for programmers of rival firms to ‘‘snoop’’ in each other’s data files to obtain competitive information. Thus, when he was apprehended for his offense, Darm was not only surprised, he was quite offended!

Such professional associations as the Institute of Management Accountants (IMA), the American Institute of Certified Public Accountants (AICPA), the Institute of Internal Auditors (IIA), the Information Systems Audit and Control Association (ISACA), the Association of Informaton Technology Professionals (AITP), and the Association for Computer Machinery (ACM) have developed codes of ethics or codes of professional conduct. These codes are self-imposed and self-enforced rules of conduct. One of the most important goals of a code of ethics or conduct is to aid professionals in selecting among alternatives that are not clear-cut. Included within professional association codes are rules pertaining to independence, technical competence, and proper practices during audits and consulting engagements involving information systems. The certification programs of these associations increase awareness of the codes of ethics and are essential in developing professionalism. Figure 10-8 provides a few examples of ethical issues in computer usage.

Ethical Issue	Example in Computer Usage
Honesty	Organizations expect employees to perform their own work, to refrain from accessing unauthorized information, and to provide authentic results of program outputs.
Protecting Computer Systems	Examples include tying up network access ports with multiple logins, sending voluminous (but useless) emails and computer files to others, complaining to system administrators about fictitious hardware or software failures, introducing computer viruses into networks, or giving unauthorized users access to private computer systems.
Protecting Confidential Information	Allowing unauthorized individuals to view private information—for example, financial data on a mortgage loan application or the results of diagnostic medical tests stored in the files of local area networks.
Social Responsibility	Sometimes, social responsibility conflicts with other organizational goals. For example, suppose a programmer discovers a possible error in a software program that controls a missile guidance system. His boss tells him to ignore it—the design team is already over budget and this is only a possible error.
Acceptable Use	The availability of computer hardware and software in workplaces does not automatically convey unrestricted uses of them. At universities, for example, ethical conduct forbids downloading microcomputer software for personal applications or using free mainframe time for personal gain.
Rights of Privacy	Do organizations have the right to read the personal email of their employees? Do employees have the right to use their business email accounts for personal correspondence? In 2002, the state of Montana decided that monitoring computer activity on state-owned computers at state universities is legal. Officials at colleges and universities in Montana are hoping to decrease the incidence of illegal activity by individuals who are using campus property.

FIGURE 10-8 Examples of ethical issues in computer usage.

In recent years, professional accounting associations at both the national and state level have established ethics committees to assist practitioners in the self-regulation process. These ethics committees provide their members with continuing education courses, advice on ethical issues, investigations of possible ethics violations, and instructional booklets covering a variety of ethics case studies. Some of the ethics committees provide their members with a ‘‘hot line’’ to advise them on the ethical and moral dilemmas experienced in the workplace. These committees also encourage the instruction of ethics in accounting curricula at colleges and universities.

Meeting the Ethical Challenges

Because a significant amount of business activity and data communications now takes place on the Internet, it is not surprising that an increasing amount of computer crime and abuse also happens within the Internet's environment. Examples include thieves supplying fake credit card numbers to buy everything from investment securities to Internet access time itself, copying web pages without permission, denying legitimate users Internet access, and posing as someone else for any number of illegal or dishonest purposes.

How we respond to the ethical issues above is determined not so much by laws or organizational rules as by our own sense of ‘‘right’’ and ‘‘wrong.’’ Ethical standards of behavior are a function of many things, including social expectations, culture, societal norms, and even the times in which we live. More than anything else, however, ethical behavior requires personal discipline and a commitment to ''do the right thing.''

How can organizations encourage ethical behavior? Some argue that morals are only learned at an early age and in the home—they cannot be taught to adults. However, others suggest that it helps to (1) inform employees that ethics are important, (2) formally expose employees to relevant cases that teach them how to act responsibly in specific situations, (3) teach by example, that is, by managers acting responsibly, and (4) use job promotions and other benefits to reward those employees who act responsibly.

> ***Case-in-Point 10.10*** The ethical principles that apply to everyday community life also apply to computing. At the University of Northern Colorado, every member has two basic rights: privacy and a fair share of resources. It is unethical for any other person to violate these rights. This code of ethics lays down general guidelines for the use of computing and information resources. Failure to observe the code may lead to disciplinary action.

Privacy

Although Americans are concerned about various privacy issues, the events of September 11, 2001, changed our focus in some respects. For example, we are willing to accept less privacy at airports, and to submit to increased security measures at various points in airport terminals. On a day-to-day basis, we freely give our name, address, phone number and similar information to receive **value cards** at a variety of retail establishments. In return, we receive discounts, points that may be exchanged for goods or services, or advance information about upcoming sales. But these credit-card-size or key-ring-size cards have a barcode on the back side that also enables merchants to track our purchases.

Privacy also affects our use of the Internet. For example, when we order a book from Amazon.com and the next time we visit that site, we're greeted by name and told about other books we might enjoy. A remarkable marketing tool, but how do they know? They know because most commercial websites deposit a **cookie** on your computer, which is a small text file that stores information about your browsing habits and interests, as well as other information that you may supply by logging onto the site. Of course, cookies are not necessarily bad. If you frequently purchase items from a particular online vendor, it is very convenient to have your credit card and shipping information automatically recalled so that you are not required to enter this information for every purchase.

Some individuals even claim that computers and privacy are mutually exclusive—and that you can't have both. The defining issue is probably whether the invasion of our privacy is with or without our permission. That is, did we agree or authorize the information to be collected? Few object to (for example) Amazon.com tracking their browsing habits on its website, but if we ordered a book or other item from that website, we would most certainly object to unauthorized uses of our credit card information.

Company Policies with Respect to Privacy

Because of the widespread use of computers in business, coupled with the fact that many employees travel and use laptops, employers should develop and distribute a company-wide policy with respect to privacy. The Fair Employment Practices Guidelines suggest that these policies cover such issues as (1) who owns the computer and the data stored on it, and (2) what purposes the computer may be used (e.g., primarily for business purposes), and (3) what uses are unauthorized or prohibited. Further, employers should specifically identify the types of acceptable and unacceptable uses with some examples. Another idea is to have a screen pop-up each time an employee signs on that reminds the employee of the company policy.

> ***Case-in-Point 10.11*** In Oklahoma, police obtained a search warrant to look for downloaded pornography on a professor's computer at Oklahoma State University. As a result, the professor was arrested, prosecuted, and given a 51-month sentence. Although the professor appealed, the court affirmed the sentence based on the University's policy barring employees from using university computers to access obscene materials and stating that such misuse could result in discipline or legal action. In addition, the University used a screen pop-up with a warning that using the system to break the law or university policies was prohibited.[14]

Most commercial websites have a **privacy policy**, although they are sometimes difficult to find. For example, at Amazon.com you need to click on the ''Privacy Notice'' link at the very bottom of its home page. There, you will find a comprehensive list of information that is covered by its privacy policy—including information you provide, cookies it uses, email communications, and information Amazon.com receives about you from other sources. Another online merchant, Lands' End, provides an easy-to-find link to the privacy policy on its home page. Its privacy policy identifies the information it does and does not collect, and offers advice about managing cookies.

An important point to remember is that companies typically are very careful about protecting your personal information. They understand that the future viability of the organization might depend on security of both your information as well as their proprietary data.

Identity Theft

Identity theft refers to an act in which someone wrongfully obtains and uses another person's personal data for fraud or deception. Unlike your fingerprints, which are unique to you and cannot be used by someone else, your personal data can certainly be used by another individual if they have a mind to use it. Your personal data may be any one or a combination of the following pieces of information: your Social Security number, your bank account, your debit card number, your credit card number, your birth date, or your mailing address. It was not until 1998 that Congress passed legislation making identity theft a crime.

Thieves steal identities in a number of ways including **dumpster diving** (stealing personal information from garbage cans), taking delivered or outgoing mail from house mail boxes, or telephone solicitations that ask for personal information. **Phishing** scams use an email or website that claims to be legitimate but that ask you to provide or ''update'' your personal information such as account number, credit card number, or password. **Smishing** is a similar scam using text messages on cell phones.

In the United States and Canada, many people have reported that unauthorized persons have taken funds out of their bank or financial accounts. Even worse, some unscrupulous individuals have gone so far as to take over an individual's identity, incurring huge debts and committing all sorts of crimes. Victims can incur enormous costs attempting to restore their reputation in a community or correcting erroneous information. It is still the case that many individuals do not realize how easily criminals can obtain their personal data. Figure 10-9 identifies a number of ways you can become a victim of identity theft if you are not careful.

[14] Source: A Legal Posting in *Workforce*, June 2002, p. 102.

Method	Examples
Shoulder surfing	• Watching you from a nearby location as you punch in your debit or credit card number • Listening to your conversation if you give your debit or credit card number over the telephone to a hotel or rental car company
Dumpster diving	• Going through your garbage can or a communal dumpster or trash bin to obtain copies of your checks, credit card or bank statements, or other records that typically have your name, address, and telephone number
Applications for ''preapproved'' credit cards	• If you discard them without tearing up the enclosed materials, criminals may retrieve them and try to activate the cards • If your mail is delivered to a place where others have access to it, criminals may simply intercept and redirect your mail to another location
Key logging software	• Loading this type of software on computers in general use areas, such as university computer labs or public libraries to obtain your personal data and other identifying data, such as passwords or banking information
Spam and other emails	• Many people respond to unsolicited email that promises some benefit but requests identifying data, which criminals use to apply for loans, credit cards, fraudulent withdrawals from bank accounts, or other goods

FIGURE 10-9 Examples of methods used by criminals to obtain your personal data.

The news media continues to report instances of compromised personal data. Some of these describe breaches in the computer system of an organization. Other reports suggest that a stolen laptop might have the personal data of hundreds or thousands of individuals. For example, in the summer of 2006, two universities reported incidents in which outsiders may have gained access to personal information, including Social Security numbers, on nearly a quarter-million students.

Case-in-Point 10.12 In June 2006, Western Illinois University announced that a hacker may have copied the Social Security or credit card numbers of 200,000 to 240,000 current or former students. The credit cards had been used to purchase textbooks online or for stays in a university hotel. The University immediately notified the individuals and advised them to monitor their credit records for any attempts at identity theft.

AIS AT WORK
Fighting Computer Crime at the Bank[15]

When the judge asked Willie Sutton—a habitual bank robber—more than one hundred years ago why he stole from banks, his answer became famous: ''because that's where the money is.'' In some ways, little has changed. Banking frauds in the U.S. total an estimated $39 billion in 2006—and are growing. Credit card fraud touches one out of every 20 credit-card users.

[15] Source: Tommie Singleton, Aaron Singleton, & Geoff Gottlieb, ''Cyber Threats Facing the Banking Industry'' *Accounting and Finance* Vol. 19, No. 2 (February 2006), pp. 26–32.

Having read this chapter, you are already familiar with the major types of computer crimes perpetrated against banks—phishing, identity theft, worms and Trojan horses, spyware, and denial-of-service attacks. Banks can fight computer crime by first performing risk assessments that analyze potential risks and then implementing policies and procedures to mitigate or prevent potential losses. One important control is the development *and test* of a disaster recovery plan, especially a test of a general computer system failure. Another is to develop an incident response plan that includes identifying who should do what in the event of a breach of computer security.

Phishing is an especially important problem for banks because hackers often create bogus websites that trick bank customers into revealing their account numbers and passwords. Raising customer awareness to this problem—for example, in brochures that accompany monthly bank statements—is one possibility. Providing similar information on bank home pages, along with examples of spoofed emails, links to the FTC website on identify theft, and consumer alerts about new threats are more ways to counter this problem.

Because ''people'' are often the weakest link in computer security, banks should pay special attention to employee safeguards. One important practice is ''employee education,'' which includes periodic training and monthly reminders to employees about specific computer security issues—especially guarding against social engineering attacks. Another safeguard is stringent employee hiring practices, including drug and credit checks and requiring employees to acknowledge and follow current security policies. Memos that encourage employees to follow the simple security steps listed in Figure 10-5 to protect individual computers from harm can also help. Finally, of all factors to successfully fight computer crime, none is more important than identifying a security officer to champion and proactively manage all the activities discussed here.

SUMMARY

- We know very little about computer crime because few cases are reported and we believe many more cases go undetected.
- Computer crime is growing and is likely to be expensive for those organizations that suffer from it.
- This chapter discussed cases of real-world computer crime. The subjects of these cases included compromising valuable information, wire fraud and computer hacking, and computer viruses.
- Organizations can use the following methods to protect themselves against computer offenses: (1) solicit top management support, (2) educate users about computer crime and abuse, (3) conduct a security inventory and protect passwords, (4) design and implement control procedures, and (5) recognize the symptoms of computer crime and abuse.
- Organizations can help themselves by knowing which employees are most likely to become computer offenders and by employing forensic accountants to investigate suspected problems.
- Managers can implement a program that focuses on ethical behavior. Examples of ethical behavior include protecting confidential information, being socially responsible, respecting rights of privacy, avoiding conflicts of interest, and understanding unacceptable uses of computer hardware and software.
- Organizations can encourage ethical behavior by educating employees about it, rewarding it, and encouraging employees to join professional associations with ethical codes of conduct.
- Identity theft is a growing problem. Both individuals and organizations must adopt reasonable precautions to protect personal data.

KEY TERMS YOU SHOULD KNOW

anti-virus software applet
Association of Certified Fraud Examiners (ACFE)
Audit Command Language (ACL)
boot-sector virus
computer abuse
computer crime
Computer Fraud and Abuse Act of 1986
Computer Security Institute (CSI)
computer virus
cookie
data diddling
distributed denial of service (DDoS) attack
dialback systems
disposal of outdated computers
dumpster diving
firewall
forensic accounting
hacker
Integrated Computer-Assisted Surveillance System (ICASS)
lock-out systems
logic bomb program
Encase
Patriot Act of 2001
Phishing
privacy policy
salami technique
social engineering
smishing
strong passwords
Trojan horse programs
value cards
voice over Internet protocol (VoIP)
worm program

TEST YOURSELF

Q10-1. A computer program that remains dormant until some specified circumstance or date triggers the program to action is called a ______.

a. Trojan horse

b. Logic bomb

c. Data diddling

d. Cookie

Q10-2. Which of the following is NOT an example of computer fraud?

a. Entering invoices in the AIS for services that were not provided, and depositing the check in a private bank account

b. Sending an email to everyone in your address book asking for a $1 donation

c. Programming a change to decrease the dividend payment to stockholders of a firm and issuing a check to your friend for the total change

d. Using a university computer to set up a realistic looking virtual ‘‘store front’’ to sell toys, although you don’t have any merchandise to sell.

Q10-3. Which of the following pieces of computer legislation is probably the most important?

a. Cyber Security Enhancement Act of 2002

b. Computer Security Act of 1987

c. The Computer Fraud and Abuse Act of 1986

d. Federal Privacy Act of 1974

Q10-4. A computer program that is used to steal small amounts of money from many accounts over a period of time is called a ______.

a. Salami technique

b. Logic bomb

c. Data diddling

d. Cookie

Q10-5. What is it called when someone intentionally changes data before, during, or after they are entered into the computer (with the intent to illegally obtain information or assets)?

a. Trojan horse

b. Logic bomb

c. Data diddling

d. A cookie

Q10-6. Which legislation might help discourage computer hacking?

a. Federal Privacy Act of 1974

b. Computer Fraud and Abuse Act of 1986

c. USA Patriot Act of 2001

d. CAN-SPAM Act of 2003

Q10-7. The TRW Case is notable because:

a. The amount of dollars involved was not significant

b. No one got caught

c. The fraud was detected by a surprise audit

d. The real victims were TRW customers

Q10-8. Which of these is not an acronym?

a. ACFE

b. Byte

c. Worm

d. DOS

e. VoIP

Q10-9. Which of these is not helpful in attempting to thwart computer crime and abuse?

a. Enlist the support of top management

b. Keep employees in the dark so that they cannot perpetrate them

c. Use strong passwords

d. Design and test disaster recovery programs

Q10-10. A local area network administrator receives a call from an employee, requesting his password. The administrator asks for his name and phone number and tells him that he will call back. This is an example of a:

a. DOS system

b. Bad computer security

c. A worm system

d. Dialback system

e. Bad security policy

Q10-11. Most computer criminals:

a. Have non-technical backgrounds

b. Have non-criminal backgrounds

c. Have little college education

d. Are young and bright

e. Have probably not been caught, so we don’t really know much about them

Q10-12. Which of these is the common name for a computer file that is written onto your personal computer by a website?

a. Applet

b. web file

c. Cookie

d. Worm

Q10-13. Which of these is a software tool often used by forensic accountants?

a. MS-DOS

b. ACFE

c. Computer Spy

d. Logic bomb

e. Encase

Q10-14. Smishing is a form of:

a. Dialback system

b. Local area network.

c. Computer worm

d. Identity theft

DISCUSSION QUESTIONS

10-1. The cases of computer crime that we know about have been described as just ''the tip of the iceberg.'' Do you consider this description accurate? Why or why not?

10-2. Most computer crime is not reported. Give as many reasons as you can why much of this crime is purposely downplayed. Do you consider these reasons valid?

10-3. Why have most computer experts suggested that computer crime is growing despite the fact that so little is known about it?

10-4. Does a company have the right to collect, store, and disseminate information about your purchasing activities without your permission?

10-5. What enabled the employees at TRW to get away with their crime? What controls might have prevented the crime from occurring?

10-6. What is hacking? What can be done to prevent hacking?

10-7. What is a computer virus?

10-8. How can educating employees help stop computer crime?

10-9. What computer crimes are committed on the Internet? What assets are involved? What can be done to safeguard these assets?

10-10. How would you define ''ethics?'' What types of ethical issues are involved in computerized accounting information systems? How can organizations encourage their employees to act ethically?

10-11. The Rivera Regional Bank uses a computerized data processing system to maintain both its checking accounts and its savings accounts. During the last three years, several customers have complained that their balances have been in error. Randy Allen, the information systems bank manager, has always treated these customers very courteously and has personally seen to it that the problems have been rectified quickly, sometimes by putting in extra hours after normal quitting time to make the necessary changes. This extra effort has been so helpful to the bank that this year, the bank's top management is planning to give Mr. Allen the Employee-of-the-Year Award. Mr. Allen has never taken a vacation. Comment.

PROBLEMS

10-12. Comment on each of the following scenarios in light of chapter materials. Hint: use the references at the end of this chapter to help you.

a. A legitimate student calls the computer help desk from her cell phone because she has forgotten her password to the university system. The ''tech'' on duty refuses to give it to her as a matter of university policy. The student is unable to complete her assignment and proceeds to file a formal complaint against the university.

b. An employee at a building supply company is caught downloading pornographic materials to his office computer. He is reprimanded by his boss, asked to remove the offending materials, and told never do it again. The employee refuses on the grounds that (1) there is no company policy forbidding these activities, (2) he performed all his downloads during his lunch breaks, (3) his work reviews indicate that he is performing ''above average,'' and (4) the discoveries themselves were performed without a search warrant and therefore violate his right to privacy.

c. The local community college installed a new, campus-wide local area network that requires all staff members to enter a login name and password. Users can choose their own passwords. Some pick the names of their pets or spouses as passwords, while others tape their passwords to their computer monitors to help remember them.

d. An employee in a hospital was hardly ever at his desk, but almost always reachable through his cell phone. When the department replaced his old computer with a new one, his boss scanned the old hard drive and made the startling discovery that this employee had a full-time second job as a beer distributor.

e. A routine audit of the computer payroll records of the local manufacturing plant reveals that the address of over 20 employees in different departments is the same empty lot in the city.

f. An analysis of online bidding on eBay reveals that one seller has bid on several of his own merchandise in an effort to increase the final sales price of his items.

g. A retailer sues a web hosting company when it discovers that the employees of the web company have been visiting sites on which the retailer advertises. The retailer pays a fee of $1 every time someone clicks on these advertising links.

10-13. (Library or Online Journal Research) Newspapers and such journals as *Datamation* and *Computerworld* are prime sources of computer-crime articles. Find a description of a computer crime not already discussed in this chapter and prepare an analysis of the crime similar to the ones in the second section of this chapter.

10-14. Recall that the salami technique means using a computer to skim a small amount of money from hundreds or thousands of accounts, and then diverting the proceeds for personal gain. Suppose that a computer programmer uses this technique to skim a penny from each customer's account at a small bank. Over the course of three months, he takes $200,000 and is never caught. Assuming that this hacker took only one penny per month from each customer, how many accounts did the bank have? If the bank had 100,000 accounts and the hacker stole one penny from each account's interest (which was computed daily), how much could the hacker steal in three months?

10-15. What company policies or procedures would you recommend to prevent each of the following activities?

a. A clerk at the Paul Yelverton Company faxes a fictitious sales invoice to a company that purchases a large quantity of goods from it. The clerk plans to intercept that particular payment check and pocket the money.

b. The bookkeeper at a construction company has each of the three owners sign a different paycheck for her. Each check is drawn from a separate account of the company.

c. A clerk in the human relations department creates a fictitious employee in the personnel computer file. When this employee's payroll check is received for distribution, the clerk takes and cashes it.

d. A clerk in the accounts receivable department steals $250 in cash from a customer payment, then prepares a computer credit memo that reduces the customer's account balance by the same amount.

e. A purchasing agent prepares an invoice for goods received from a fictitious supplier. She sends a check for the goods to this supplier, in care of her mother's post-office box.

f. A hacker manages to break into a company's computer system by guessing the password of his friend—Champ, the name of the friend's dog.

g. An accounts receivable clerk manages to embezzle more than $1 million from the company by diligently lapping the accounts every day for three consecutive years.

h. The company's local area network administrator traces a virus to an individual who accidentally introduced it when he downloaded a computer game from the Internet.

i. A clerk at a medical lab recognizes the name of an acquaintance as one of those patients whose lab tests are ''positive'' for an infectious disease. She mentions it to a mutual friend, and before long, the entire town knows about it.

10-16. Download a copy of the Association of Certified Fraud Examiners Fraud Prevention Checkup, which is available at www.acfe.com/documents/Fraud_Prev_Checkup_IA.pdf. On a separate piece of paper, list the seven areas, and the maximum number of points suggested for each one. An example is:

1. Fraud Risk Oversight (20 points).

Do you think that this check list is likely to enable organizations to prevent most types of fraud? Why or why not?

10-17. Download a copy of the *ACFE Compensation Guide for Anti-fraud Professionals*, which is available at no charge at: www.acfe.com/documents/2008-comp-guide.pdf. Based on this resource, answer the following questions:

a. How many people participated in the 2008 survey?

b. What is the median total compensation for certified forensic examiners (CFEs) and for non-CFEs?

c. What is the modal years of experience for CFEs and for non-CFEs?

d. What is the modal highest level of education completed for CFEs and for non-CFEs?

e. What is the median total annual compensation for females and males holding CFE certification, and for CFEs versus non-CFEs? How can you explain these differences?

f. Do fraud examiners earn more if they work in one type of industry (e.g., healthcare) than another? How about internal auditors?

g. Do anti-fraud practitioners tend to earn more in some areas of the country than in others? If so, what explains these differences?

CASE ANALYSES

10-18. Ashley Company (Diskless PC System and Security Threats)

To address the need for tighter data controls and lower support costs, the Ashley Company has adopted a new diskless PC system. It is little more than a mutilated personal computer described as a ''gutless wonder.'' The basic concept behind the diskless PC is simple: A

LAN server-based file system of high-powered diskless workstations is spread throughout a company and connected with a central repository or mainframe. The network improves control by limiting user access to company data previously stored on desktop hard disks. Because the user can destroy or delete only the information currently on the screen, an organization's financial data are better protected from user-instigated catastrophes. The diskless computer also saves money in user support costs by distributing applications and upgrades automatically, and by offering online help.

Requirements:

1. What threats in the information processing and storage system do the diskless PC minimize?
2. Do the security advantages of the new system outweigh potential limitations? Discuss.

10-19. Mark Goodwin Resort (A Valuable-Information Computer Offense)

The Mark Goodwin Resort is an elegant summer resort located in a remote mountain setting. Guests visiting the resort can fish, hike, go horseback riding, swim in one of three hotel pools, or simply sit in one of the many lounge chairs located around the property and enjoy the spectacular scenery. There are also three dining rooms, card rooms, nightly movies, and live weekend entertainment.

The resort uses a computerized system to make room reservations and bill customers. Following standard policy for the industry, the resort also offers authorized travel agents a 10% commission on room bookings. Each week, the resort prints an exception report of bookings made by unrecognized travel agents. However, the managers usually pay the commissions anyway, partly because they don't want to anger the travel agencies and partly because the computer file that maintains the list of authorized agents is not kept up to date.

Although management has not discovered it, several employees now exploit these facts to their own advantage. As often as possible, they call the resort from outside phones, pose as travel agents, book rooms for friends and relatives, and collect the commissions. The incentive is obvious: rooms costing as little as $100 per day result in payments of $10 per day to the ''travel agencies'' that book them. The scam has been going on for years, and several guests now book their rooms exclusively through these employees, finding these people particularly courteous and helpful.

Requirements:

1. Would you say this is a ''computer crime?'' Why or why not?
2. What controls would you recommend that would enable the resort's managers to thwart such offenses?
3. How does the matter of ''accountability'' (tracing transactions to specific agencies) affect the problem?

10-20. The Department of Taxation (Data Confidentiality)

The Department of Taxation of one state is developing a new computer system for processing state income tax returns of individuals and corporations. The new system features direct data input and inquiry capabilities. Identification of taxpayers is provided by using the Social Security numbers of individuals and federal identification numbers for corporations. The new system should be fully implemented in time for the next tax season. The new system will serve three primary purposes:

- Data will be input into the system directly from tax returns through computer terminals located at the central headquarters of the Department of Taxation.
- The returns will be processed using the main computer facilities at central headquarters. The processing includes (1) verifying mathematical accuracy; (2) auditing the reasonableness of deductions, tax due, and so forth, through the use of edit routines as well as a comparison of the current year's data with prior years' data; (3) identifying returns that should be considered for audit by revenue agents of the department; and (4) issuing refund checks to taxpayers.
- Inquiry service will be provided to taxpayers on request through the assistance of Tax Department personnel at five regional offices. A total of 50 computer terminals will be placed at the regional offices.

A taxpayer will be able to determine the status of his or her return or to get information from the last three years' returns by calling or visiting one of the department's regional offices. The state commissioner of taxation is concerned about data security during input and processing over and above protection against natural hazards such as fires or floods. This includes protection against the loss or damage of data during data input or processing, and the improper input or processing of data. In addition, the tax commissioner and the state attorney general have discussed the general problem of data confidentiality that may arise from the nature and operation of the new system. Both individuals want to have all potential problems identified before the system is fully developed and implemented so that the proper controls can be incorporated into the new system.

Requirements:

1. Describe the potential confidentiality problems that could arise in each of the following three areas of processing and recommend the corrective action(s) to solve the problems: (a) data input, (b) processing of returns, (c) data inquiry.
2. The State Tax Commission wants to incorporate controls to provide data security against the loss, damage, or improper input or use of data during data input and processing. Identify the potential problems (outside of natural hazards such as fires or floods) for which the Department of Taxation should develop controls, and recommend possible control procedures for each problem identified.
   (CMA adapted)

REFERENCES AND RECOMMENDED READINGS

Brandt, Andres. ''Phishers Put Their Lures on Cell Phones'' *PC World* Vol. 25, No. 1 (January 2007), p. 46.

Cronan, T., C. Foltz, and T. Jones. ''Piracy, Computer Crime, and IS Misuse at the University,'' *Communications of the ACM* 49 (June 2006), pp. 85–90.

Fadaghi, Foad. ''Industry Sights Set on Click Fraud'' *Preview* Vol. 29, No. 1 (January 11, 2007), pp. 60–61.

Feldstein, D. ''Horror Stories of Identity Theft Steal Attention,'' *Houston Chronicle* (June 28, 2004).

Gentile, O. ''Fraud Grows with the Economy,'' *Hartford Courant* (January 16, 2000), pp. B1–B2.

Haines, J. ''New Crimes, New Tools—Old Crimes, New Tools'' *Journal of Financial Crime* Vol. 9, No. 1 (September 2001), pp. 6–7.

Kiernan, V. ''Two Incidents put More than 200,000 Students at Risk of Data Theft,'' *The Chronicle of Higher Education* 52 (June 30, 2006).

Larson, L., R. Larson, and J. Greenlee. ''Privacy Protection on the Internet,'' *Strategic Finance* (June 2003), pp. 48–53.

Ling, B. ''Lines of Defense: Guarding against electronic privacy,'' *Utah Business* (August 2003), pp. 42–43.

Lunsford, D. and W. Robbins. ''Cyber-criminals and Data Sanitization: A Role for Forensic Accountants,'' *Forensic Examiner* 14 (Summer 2005), pp. 50–54.

Macodrum, D., H. Nasheri, and T. O'Hearn. ''Spies In Suits: New Crimes of the Information Age from the United States and Canadian Perspectives,'' *Information & Communications Technology Law*, Vol. 10, No. 2 (June 2001), pp. 139–166.

Mangan, K. ''Computer Security Breach Raises Fears at University of Texas,'' *The Chronicle of Higher Education* 52 (May 2, 2006).

Lim, Nena. ''Crime Investigation: a Course in Computer Forensics'' *Communications of the AIS* Vol. 2006, No. 18 (2006), pp. 2–34.

Nikitkov, Alex, and Darlene Bay. ''Online Auction Fraud: Ethical Perspective'' *Journal of Business Ethics* Vol 79, No. 3 (May 2008), pp. 235–244.

Pearson, Timothy A., and Tommie W. Singleton. ''Fraud and Forensic Accounting in the Digital Environment'' *Issues in Accounting Education* Vol. 23, No. 4 (November 2008), pp. 545–559.

Richardson, Robert. *2008 CSI Computer Crime & Security Survey* Computer Security Institute, 2008.

Samuels, P., and M. Young. ''Phishing and pharming and Trojans - oh my!'' *Utah Bar Journal* 19 (March-April 2006), pp. 28–32.

Scarponi, D. ''Hacker Steals Credit Card Numbers From CT Retailer,'' *Bristol Press* (January 11, 2000), pp. A1–A2.

Singleton, Tommie, Aaron Singleton, and Geoff Gottlieb. ''Cyberthreats Facing the Banking Industry'' *Accounting and Finance* Vol. 19, No. 2 (February 2006), pp. 26–32.

Wallace, R., A. Lusthaus, and J. Kim. ''Computer Crimes: Annual Survey of White Collar Crime,'' *Criminal Law Review* 42 (Spring 2005), pp. 223–276.

Wang, Y., J. Cannady, and J. Rosenbluth. ''Foundations of Computer Forensics: A Technology for the Fight Against Computer Crime,'' *Computer Law & Security Report* 21 (March-April 2005), pp. 119–127.

ANSWERS TO TEST YOURSELF

1. **b** 2. **b** 3. **c** 4. **a** 5. **c** 6. **b** 7. **d** 8. **b** 9. **b** 10. **d** 11. **e** 12. **c** 13. **e** 14. **d**