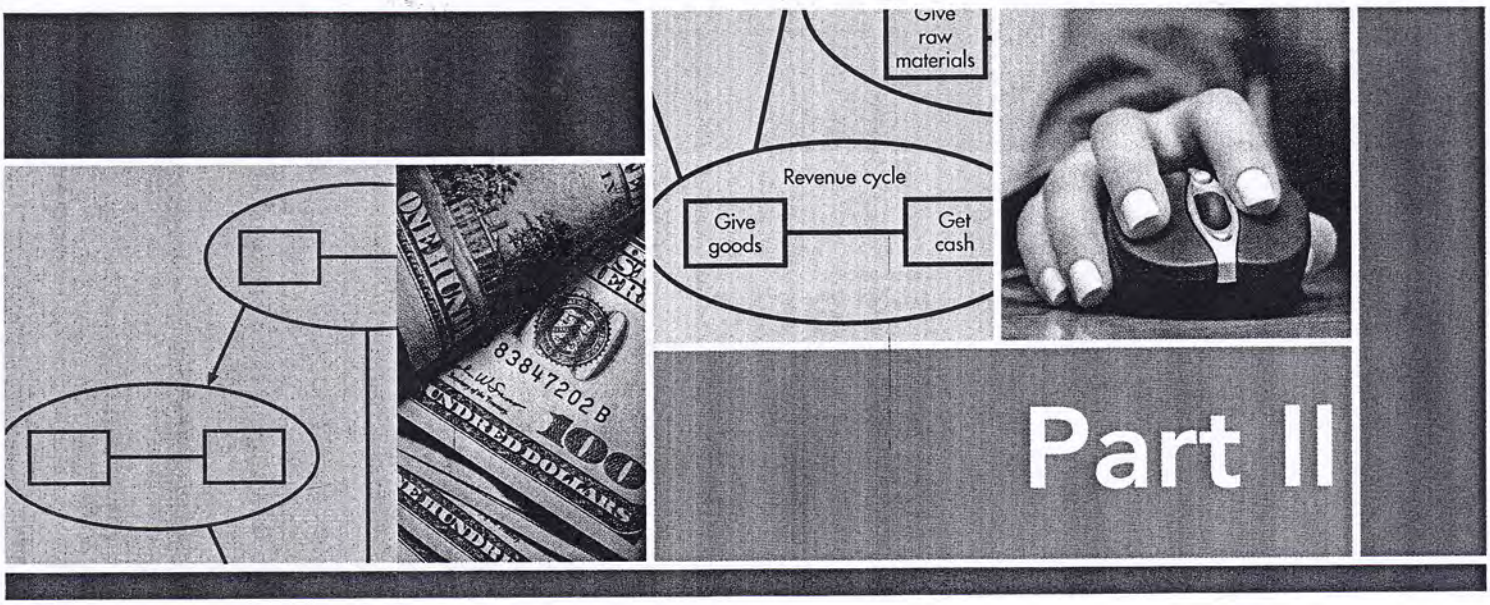


Control and Audit of Accounting Information Systems

Chapter 5

Computer Fraud

Learning Objectives

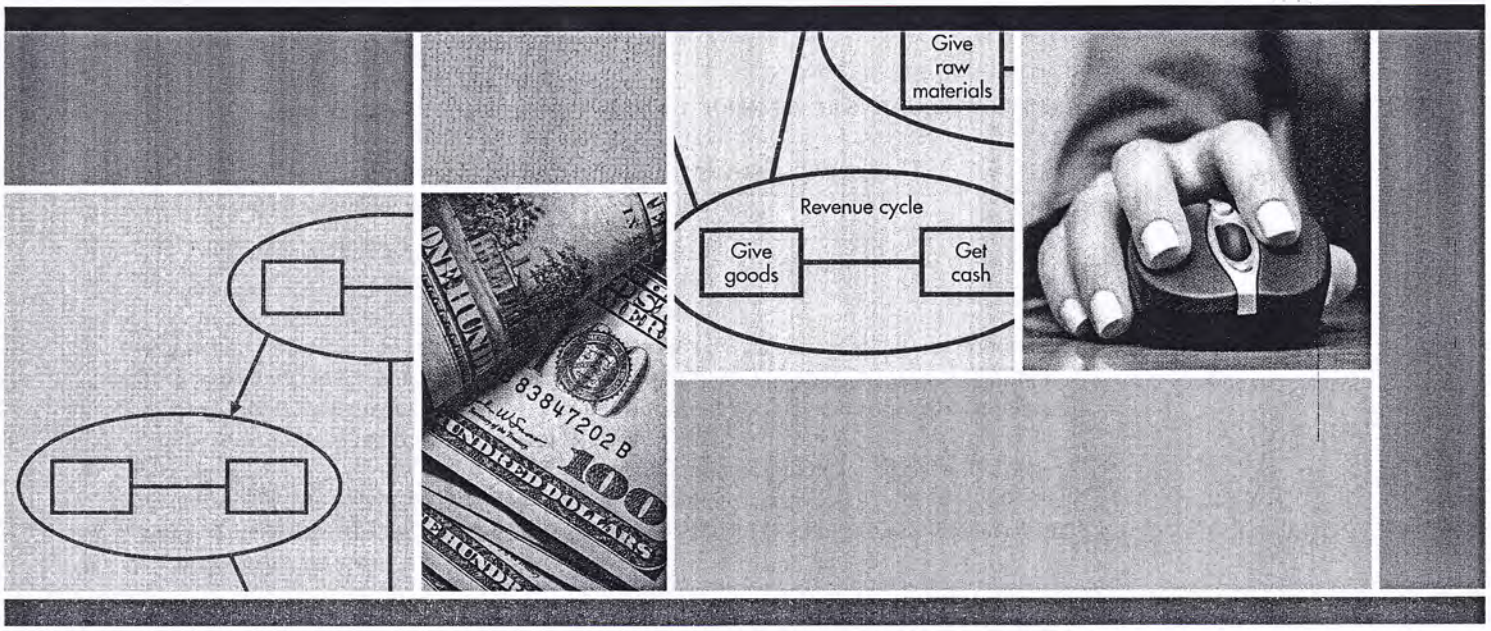
After studying this chapter, you should be able to:

1. Explain the threats faced by modern information systems.
2. Define *fraud* and describe the process one follows to perpetuate a fraud.
3. Discuss who perpetrates fraud and why it occurs, including the pressures, opportunities, and rationalizations that are present in most frauds.
4. Define *computer fraud* and discuss the different computer fraud classifications.
5. Explain how to prevent and detect computer fraud and abuse.

INTEGRATIVE CASE NORTHWEST INDUSTRIES

Jason Scott is an internal auditor for Northwest Industries, a forest products company. On March 31, he reviewed his completed tax return and noticed that the federal income tax withholding on his final paycheck was $5 more than the amount indicated on his W-2 form. He used the W-2 amount to complete his tax return and made a note to ask the payroll department what happened to the other $5. The next day, Jason was swamped, and he dismissed the $5 difference as immaterial.

On April 16, a coworker grumbled that the company had taken $5 more from his check than he was given credit for on his W-2. When Jason realized he was not the only one with the $5 discrepancy, he investigated and found that all 1,500 employees had the same $5 discrepancy. He also discovered that the W-2 of Don Hawkins, the payroll programmer, had thousands of dollars more in withholdings reported to the IRS than had been withheld from his paycheck.



Jason knew that when he reported the situation, management was going to ask questions, such as:

1. What constitutes a fraud, and is the withholding problem a fraud?
2. How was the fraud perpetrated? What motivated Don to commit it?
3. Why did the company not catch these mistakes? Was there a breakdown in controls?
4. How can the company detect and prevent fraud?
5. How vulnerable is the company's computer system to fraud?

Introduction

As accounting information systems grow more complex to meet our escalating needs for information, companies face the growing risk that their systems may be compromised. Recent surveys show that 67% of companies had a security breach, over 45% were targeted by organized crime, and 60% reported financial losses.

The four types of AIS threats a company faces are summarized in Table 5-1.

AIS Threats

Natural and political disasters—such as fires, floods, earthquakes, hurricanes, tornadoes, blizzards, war, and attacks by terrorists—can destroy an information system and cause many companies to fail. For example:

- Terrorist attacks on the World Trade Center in New York City and on the Federal Building in Oklahoma City destroyed or disrupted all the systems in those buildings.
- A flood in Chicago destroyed or damaged 400 data processing centers. Hurricanes on the East coast of the United States have destroyed many computer systems.
- The Mississippi and Missouri rivers overflowed and flooded parts of eight states. Many organizations lost their systems, including the city of Des Moines, Iowa, whose computers were buried under eight feet of water.

TABLE 5-1 Threats to Accounting Information Systems

Threats	Examples
Natural and political disasters	Fire or excessive heat
	Floods, earthquakes, landslides, hurricanes, tornadoes, blizzards, snowstorms, and freezing rain
	War and attacks by terrorists
Software errors and equipment malfunctions	Hardware or software failure
	Software errors or bugs
	Operating system crashes
	Power outages and fluctuations
	Undetected data transmission errors
Unintentional acts	Accidents caused by human carelessness, failure to follow established procedures, and poorly trained or supervised personnel
	Innocent errors or omissions
	Lost, erroneous, destroyed, or misplaced data
	Logic errors
	Systems that do not meet company needs or cannot handle intended tasks
Intentional acts (computer crimes)	Sabotage
	Misrepresentation, false use, or unauthorized disclosure of data
	Misappropriation of assets
	Financial statement fraud
	Corruption
	Computer fraud—attacks, social engineering, malware, etc.

- Earthquakes in Los Angeles and San Francisco destroyed numerous computer systems and severed communication lines. Other systems were damaged by falling debris, water from ruptured sprinkler systems, and dust.
- Attacks on government information systems by foreign countries, espionage agents, and terrorists are widespread. Military contractors and businesses are also targets.

Software errors, operating system crashes, hardware failures, power outages and fluctuations, and undetected data transmission errors constitute a second type of threat. Of special concern are vulnerabilities in Microsoft Windows; in a recent survey, 30% of companies had moved systems off Windows to reduce security risks.

A federal study estimated yearly economic losses due to software bugs at almost $60 billion. More than 60% of companies studied had significant software errors in. For example:

- As a result of tax system bugs, California failed to collect $635 million in business taxes.
- Defective software caused massive power failures that left hundreds of thousands of people and businesses without power.
- A bug in Burger King's software resulted in a $4,334.33 debit card charge for four hamburgers. The cashier accidentally keyed in the $4.33 charge twice, resulting in the overcharge.

A third type of threat, unintentional acts such as accidents or innocent errors and omissions, is the greatest risk to information systems and causes the greatest dollar losses. The Computing Technology Industry Association estimates that human errors cause 80% of security problems. Forrester Research estimates that employees unintentionally create legal, regulatory, or financial risks in 25% of their outbound e-mails.

Unintentional acts are caused by human carelessness, failure to follow established procedures, and poorly trained or supervised personnel. Users lose or misplace data and accidentally erase or alter files, data, and programs. Computer operators and users enter the wrong input or erroneous input, use the wrong version of a program or the wrong data files, or misplace data files. Systems analysts develop systems that do not meet company needs, that leave them

vulnerable to attack, or that are incapable of handling their intended tasks. Programmers make logic errors. Examples of unintentional acts include the following:

- A data entry clerk at Mizuho Securities mistakenly keyed in a sale for 610,000 shares of J-Com for 1 yen instead of the sale of 1 share for 610,000 yen. The error cost the company $250 million.
- A programmer made a one-line-of-code error that priced all goods at Zappos, an online retailer, at $49.95—even though some of the items it sells are worth thousands of dollars. The change went into effect at midnight, and by the time it was detected at 6:00 A.M., the company had lost $1.6 million on goods sold far below cost.
- A bank programmer mistakenly calculated interest for each month using 31 days. Before the mistake was discovered, over $100,000 in excess interest was paid.
- A Fannie Mae spreadsheet error misstated earnings by $1.2 billion.
- UPS lost a box of computer tapes containing sensitive information on 3.9 million Citigroup customers.
- Jefferson County, West Virginia released a new online search tool that exposed the personal information of 1.6 million people.
- McAfee, the antivirus software vendor, mistakenly identified svchost.exe, a crucial part of the Windows operating system, as a malicious program in one of its updates. Hundreds of thousands of PCs worldwide had to be manually rebooted—a process that took 30 minutes per machine. A third of the hospitals in Rhode Island were shut down by the error. One company reported that the error cost them $2.5 million.

A fourth threat is an intentional act such as a computer crime, a fraud, or **sabotage**, which is deliberate destruction or harm to a system. Information systems are increasingly vulnerable to attack. Symantec estimates that hackers attack computers more than 8.6 million times per day. It is estimated that Internet fraud cost its victims over $600 million a year. In a recent three-year period, the number of networks that were compromised rose 700%. That is just the tip of the iceberg: Experts believe the actual number of incidents is six times higher because companies tend not to report security breaches.

Consider the case of OpenTable, a restaurant reservation service that did not properly design its **cookie** (data a Web site stores on your computer to identify the Web site to your computer so that you do not have to log on each time you visit the site). An experienced programmer opened an account at OpenTable and, in less than an hour, wrote a program that downloaded most of the company's database. Many other companies have had problems with the same type of system vulnerability.

The seven chapters in Part II focus on control concepts. Fraud is the topic of this chapter. Computer fraud and abuse techniques are the topic of Chapter 6. Chapter 7 explains general principles of control in business organizations and describes a comprehensive business risk and control framework. Chapter 8 introduces five basic principles that contribute to systems reliability and then focuses on security, the foundation on which the other four principles rest. Chapter 9 discusses two of the other four principles of systems reliability: confidentiality and privacy. Chapter 10 discusses the last two principles: processing integrity and availability. Chapter 11 examines the processes and procedures used in auditing computer-based systems.

This chapter discusses fraud in four main sections: an introduction to fraud, why fraud occurs, approaches to computer fraud, and how to deter and detect computer fraud.

Introduction to Fraud

Fraud is gaining an unfair advantage over another person. Legally, for an act to be fraudulent there must be:

1. A *false statement, representation, or disclosure*
2. A *material fact*, which is something that induces a person to act
3. An *intent to deceive*
4. A *justifiable reliance;* that is, the person relies on the misrepresentation to take an action
5. An *injury or loss* suffered by the victim

No one knows the total losses to fraud each year. Income tax fraud (the difference between what taxpayers owe and what they pay) is estimated to be almost $400 billion a year. Fraud in the health care industry is estimated to exceed $100 billion a year. The Association of Certified Fraud Examiners estimates that:

- Fraud and abuse costs the United States $994 billion a year.
- The average organization loses 7% of its annual revenues to fraud.
- The median fraud loss is $175,000. Financial statement fraud is the most costly fraud, with a median loss of $2 million.
- The average fraud lasted two years.
- The most common frauds are corruption and fraudulent billing schemes.
- Small businesses are especially vulnerable, with check tampering and fraudulent billings the most common frauds.
- Frauds are more likely to be detected by a tip than by audits, controls, or other means.
- The industries most commonly victimized were banking and financial services, government, and health care. The largest median losses occurred in manufacturing ($441,000), banking ($250,000), and insurance ($216,000).
- People in accounting departments committed 29% of frauds; executives or upper management committed 18%. Frauds committed by executives were particularly costly, resulting in a median loss of $853,000.
- Most fraudsters are first-time offenders. Only 7% had prior convictions, and only 12% had been previously terminated by an employer for fraud-related conduct.
- Fraud perpetrators often display behavioral traits related to living beyond their means or struggling to overcome financial difficulties. In financial statement fraud, excessive organizational pressure to perform is a particularly strong warning sign.

An estimated 75% to 90% of computer fraud perpetrators are knowledgeable insiders with the requisite access, skills, and resources. Because employees understand a company's system and its weaknesses, they are better able to commit and conceal a fraud. The controls used to protect corporate assets make it more difficult for an outsider to steal from a company. Fraud perpetrators are often referred to as **white-collar criminals.**

Fraud takes two forms: misappropriation of assets and fraudulent financial reporting.

Misappropriation of Assets

Misappropriation of assets is the theft of company assets. Examples include the following:

- Albert Milano, a manager at *Reader's Digest* responsible for processing bills, embezzled $1 million over a five-year period. He forged a superior's signature on invoices for services never performed, submitted them to accounts payable, forged the endorsement on the check, and deposited it in his account. Milano used the stolen funds to buy an expensive home, five cars, and a boat.
- A bank vice president approved $1 billion in bad loans in exchange for $585,000 in kickbacks. The loans cost the bank $800 million and helped trigger its collapse.
- A manager at a Florida newspaper went to work for a competitor after he was fired. The first employer soon realized its reporters were being scooped. An investigation revealed the manager still had an active account and password and regularly browsed its computer files for information on exclusive stories.

The most significant contributing factor in most misappropriations is the absence of internal controls and/or the failure to enforce existing internal controls. A typical misappropriation has the following important elements or characteristics. The perpetrator:

- Gains the trust or confidence of the entity being defrauded.
- Uses trickery, cunning, or false or misleading information to commit fraud.
- Conceals the fraud by falsifying records or other information.
- Rarely terminates the fraud voluntarily.
- Sees how easy it is to get extra money, need or greed impels the person to continue. Some frauds are self-perpetuating; if perpetrators stop, their actions are discovered.
- Spends the ill-gotten gains. Rarely does the perpetrator save or invest the money. Some perpetrators come to depend on the "extra" income, and others adopt a lifestyle that

requires even greater amounts of money. For these reasons, there are no small frauds—only large ones that are detected early.

- Gets greedy and takes ever-larger amounts of money at intervals that are more frequent, exposing the perpetrator to greater scrutiny and increasing the chances the fraud is discovered. The sheer magnitude of some frauds leads to their detection. For example, the accountant at an auto repair shop, a lifelong friend of the shop's owner, embezzled ever-larger sums of money over a seven-year period. In the last year of the fraud, the embezzler took over $200,000. Facing bankruptcy, the owner eventually laid off the accountant and had his wife take over the bookkeeping. When the company immediately began doing better, the wife investigated and uncovered the fraud.
- Grows careless or overconfident as time passes. If the size of the fraud does not lead to its discovery, the perpetrator eventually makes a mistake that does lead to the discovery.

Fraudulent Financial Reporting

The National Commission on Fraudulent Financial Reporting (the Treadway Commission) defined **fraudulent financial reporting** as intentional or reckless conduct, whether by act or omission, that results in materially misleading financial statements. Financial statements are falsified to deceive investors and creditors, increase a company's stock price, meet cash flow needs, or hide company losses and problems. The Treadway Commission studied 450 lawsuits against auditors and found undetected fraud to be a factor in half of them.

Through the years, many highly publicized financial statement frauds have occurred. In each case, misrepresented financial statements led to huge financial losses and a number of bankruptcies. The most frequent "cook the books" schemes involve fictitiously inflating revenues, holding the books open (recognizing revenues before they are earned), closing the books early (delaying current expenses to a later period), overstating inventories or fixed assets, and concealing losses and liabilities.

The Treadway Commission recommended four actions to reduce fraudulent financial reporting:

1. Establish an organizational environment that contributes to the integrity of the financial reporting process.
2. Identify and understand the factors that lead to fraudulent financial reporting.
3. Assess the risk of fraudulent financial reporting within the company.
4. Design and implement internal controls to provide reasonable assurance of preventing fraudulent financial reporting.

The Association of Certified Fraud Examiners found that an asset misappropriation is 17 times more likely than fraudulent financial reporting but that the amounts involved are much smaller. As a result, auditors and management are more concerned with fraudulent financial reporting even though they are more likely to encounter misappropriations. The following section discusses an auditors' responsibility for detecting material fraud.

SAS No. 99: The Auditor's Responsibility to Detect Fraud

Statement on Auditing Standards (SAS) No. 82, *Consideration of Fraud in a Financial Statement Audit*, was adopted in 1997 to clarify the auditor's responsibility to detect fraud. It was revised as SAS No. 99, with the same title, and became effective in December 2002. SAS No. 99 requires auditors to:

- ***Understand fraud.*** Because auditors cannot effectively audit something they do not understand, they must understand fraud and how and why it is committed.
- ***Discuss the risks of material fraudulent misstatements.*** While planning the audit, team members discuss among themselves how and where the company's financial statements are susceptible to fraud.
- ***Obtain information.*** The audit team gathers evidence by looking for fraud risk factors; testing company records; and asking management, the audit committee of the board of

directors, and others whether they know of past or current fraud. Because many frauds involve revenue recognition, special care is exercised in examining revenue accounts.

- ***Identify, assess, and respond to risks.*** The evidence is used to identify, assess, and respond to fraud risks by varying the nature, timing, and extent of audit procedures and by evaluating carefully the risk of management overriding internal controls.
- ***Evaluate the results of their audit tests.*** Auditors must evaluate whether identified misstatements indicate the presence of fraud and determine its impact on the financial statements and the audit.
- ***Document and communicate findings.*** Auditors document and communicate their findings to management and the audit committee.
- ***Incorporate a technology focus.*** SAS No. 99 recognizes the impact technology has on fraud risks and provides commentary and examples recognizing this impact. It also notes the opportunities auditors have to use technology to design fraud-auditing procedures.

Who Perpetrates Fraud and Why

When researchers compared the psychological and demographic characteristics of white-collar criminals, violent criminals, and the public, they found significant differences between violent and white-collar criminals. They found few differences between white-collar criminals and the public. Their conclusion: Fraud perpetrators look just like you and me.

Some fraud perpetrators are disgruntled and unhappy with their jobs and seek revenge against employers. Others are dedicated, hard-working, and trusted employees. Most have no previous criminal record; they were honest, valued, and respected members of their community.

Computer fraud perpetrators are younger and possess more computer experience and skills. Some are motivated by curiosity, a quest for knowledge, the desire to learn how things work, and the challenge of beating the system. Some view their actions as a game rather than as dishonest behavior. Others commit computer fraud to gain stature in the hacking community.

A large and growing number of computer fraud perpetrators seek to turn their actions into money. Malicious software is a big business and a huge profit engine for the criminal underground, especially for digitally savvy hackers in Eastern Europe. They break into financial accounts and steal money. They sell data to spammers, organized crime, hackers, and the intelligence community. They market malware, such as virus-producing software, to others. Some work with organized crime. A recently convicted hacker was paid $150 for every 1,000 computers he infected with his adware and earned hundreds of thousands of dollars a year.

Cyber-criminals are a top FBI priority because they have moved from isolated and uncoordinated attacks to organized fraud schemes targeted at specific individuals and businesses. They use online payment companies to launder their ill-gotten gains. To hide their money, they take advantage of the lack of coordination between international law enforcement organizations.

The Fraud Triangle

Three conditions are present when fraud occurs: a pressure, an opportunity, and a rationalization. This is referred to as the fraud triangle, and is the middle triangle in Figure 5-1.

PRESSURES A **pressure** is a person's incentive or motivation for committing fraud. Three types of pressures that lead to misappropriations are shown in the Employee Pressure Triangle in Figure 5-1 and are summarized in Table 5-2.

Financial pressures often motivate misappropriation frauds by employees. Examples of such pressures include living beyond one's means, heavy financial losses, or high personal debt. Often, the perpetrator feels the pressure cannot be shared and believes fraud is the best way out of a difficult situation. For example, Raymond Keller owned a grain elevator where he stored grain for local farmers. He made money by trading in commodities and built a lavish house overlooking the Des Moines River. Heavy financial losses created a severe cash shortage and high debt. He asked some farmers to wait for their money, gave others bad checks, and sold grain that did not belong to him. Finally, the seven banks to which he owed over $3 million began to call their loans. When a state auditor showed up unexpectedly, Raymond took his life rather than face the consequences of his fraud.

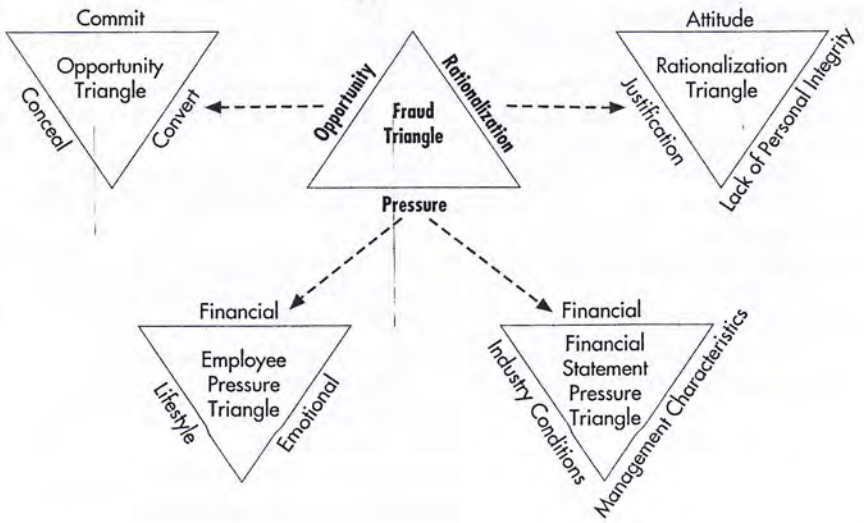


FIGURE 5-1
Fraud Triangles

TABLE 5-2 Pressures That Can Lead to Employee Fraud

Financial	Emotional	Lifestyle
Living beyond one's means	Greed	Gambling habit
High personal debt/expenses	Performance not recognized	Drug or alcohol addiction
"Inadequate" salary/income	Job dissatisfaction	Sexual relationships
Poor credit ratings	Fear of losing job	Family/peer pressure
Heavy financial losses	Need for power or control	
Bad investments	Excessive pride or ambition	
Tax avoidance	Overt, deliberate nonconformity	
Unreasonable quotas/goals	Inability to abide by or respect rules	
	Challenge of beating the system	
	Envy or resentment against others	

A second type of pressure is emotional. Many employee frauds are motivated by greed. Some employees turn to fraud because they have strong feelings of resentment or believe they have been treated unfairly. They may feel their pay is too low, their contributions are not appreciated, or the company is taking advantage of them. A California accountant, passed over for a raise, increased his salary by 10%, the amount of the average raise. He defended his actions by saying he was only taking what was rightfully his. When asked why he did not increase his salary by 11%, he responded that he would have been stealing 1%.

Other people are motivated by the challenge of "beating the system" or subverting system controls and breaking into a system. When a company boasted that its new system was impenetrable, a team of individuals took less than 24 hours to break into the system and leave a message that the system had been compromised.

A third type of employee pressure is a person's lifestyle. The person may need funds to support a gambling habit or support a drug or alcohol addiction. Some people commit fraud to keep pace with other family members. A plastic surgeon, making $800,000 a year, defrauded his clinic of $200,000 to compete in the family "game" of financial one-upmanship.

Three types of organizational pressures that motivate management to misrepresent financial statements are shown in the Financial Statement Pressure triangle in Figure 5-1 and summarized in Table 5-3. A prevalent financial pressure is a need to meet or exceed earnings expectations to keep a stock price from falling. Managers create significant pressure with unduly aggressive earnings forecasts or unrealistic performance standards or with incentive programs that motivate employees to falsify financial results to keep their jobs or to receive stock options and other incentive payments. Industry conditions such as new regulatory requirements or significant market saturation with declining margins can motivate fraud.

TABLE 5-3 Pressures That Can Lead to Financial Statement Fraud

Management Characteristics	Industry Conditions	Financial
Questionable management ethics, management style, and track record	Declining industry	Intense pressure to meet or exceed earnings expectations
Unduly aggressive earnings forecasts, performance standards, accounting methods, or incentive programs	Industry or technology changes leading to declining demand or product obsolescence	Significant cash flow problems; unusual difficulty collecting receivables, paying payables
Significant incentive compensation based on achieving unduly aggressive goals	New regulatory requirements that impair financial stability or profitability	Heavy losses, high or undiversified risk, high dependence on debt, or unduly restrictive debt covenants
Management actions or transactions with no clear business justification	Significant competition or market saturation, with declining margins	Heavy dependence on new or unproven product lines
Oversensitivity to the effects of alternative accounting treatments on earnings per share	Significant tax changes or adjustments	Severe inventory obsolescence or excessive inventory buildup
Strained relationship with past auditors		Economic conditions (inflation, recession)
Failure to correct errors on a timely basis, leading to even greater problems		Litigation, especially management vs. shareholders
High management/employee turnover		Impending business failure or bankruptcy
Unusual/odd related-party relationships		Problems with regulatory agencies
		High vulnerability to rise in interest rates
		Poor or deteriorating financial position
		Unusually rapid growth or profitability compared to companies in same industry
		Significant estimates involving highly subjective judgments or uncertainties

OPPORTUNITIES As shown in the Opportunity Triangle in Figure 5-1, **opportunity** is the condition or situation that allows a person or organization to do three things:

1. *Commit the fraud.* The theft of assets is the most common type of misappropriation. Most instances of fraudulent financial reporting involve overstatements of assets or revenues, understatements of liabilities, or failures to disclose information.
2. *Conceal the fraud.* To prevent detection when assets are stolen or overstated, perpetrators must keep the accounting equation in balance by inflating other assets or decreasing liabilities or equity. Concealment often takes more effort and time and leaves behind more evidence than the theft or misrepresentation. Taking cash requires only a few seconds; altering records to hide the theft is more challenging and time-consuming.

   One way to hide a theft is to charge the stolen item to an expense account. The perpetrator's exposure is limited to a year or less, because expense accounts are zeroed out at the end of each year. Perpetrators who hide a theft in a balance sheet account must continue the concealment. In a **lapping** scheme, a perpetrator steals the cash or checks customer A mails in to pay its accounts receivable. Later, funds from customer B are used to pay off customer A's balance. Funds from customer C are used to pay off customer B's balance, and so forth. Because the theft involves two asset accounts (cash and accounts receivable), the cover-up must continue indefinitely unless the money is replaced.

   In check **kiting**, cash is created using the lag between the time a check is deposited and the time it clears the bank. Suppose a fraud perpetrator opens accounts in banks A, B, and C. The perpetrator "creates" cash by depositing a $1,000 check from bank B in bank C and withdrawing the funds. If it takes two days for the check to clear bank B, he has created $1,000 for two days. After two days, the perpetrator deposits a $1,000 check from bank A in bank B to cover the created $1,000 for two more days. At the appropriate time, $1,000 is deposited from bank C in bank A. The scheme continues—writing checks and making deposits as needed to keep the checks from bouncing.
3. *Convert the theft or misrepresentation to personal gain.* In a misappropriation, fraud perpetrators who do not steal cash or use the stolen assets personally must convert them to

a spendable form. For example, employees who steal inventory or equipment sell the items or otherwise convert them to cash. In cases of falsified financial statements, perpetrators convert their actions to personal gain through indirect benefits; that is, they keep their jobs, their stock rises, they receive pay raises and promotions, or they gain more power and influence.

Table 5-4 lists frequently mentioned opportunities. Many opportunities are the result of a deficient system of internal controls, such as deficiencies in proper segregation of duties, authorization procedures, clear lines of authority, proper supervision, adequate documents and records, safeguarding assets, or independent checks on performance. Management permits fraud by inattention or carelessness. Management commits fraud by overriding internal controls or using a position of power to compel subordinates to perpetrate it. The most prevalent opportunity for fraud results from a company's failure to design and *enforce* its internal control system.

Companies who do not perform a background check on potential employees risk hiring a "phantom controller." In one case, the company president stopped by the office one night, saw a light on in the controller's office, and went to see why he was working late. The president was surprised to find a complete stranger at work. An investigation showed that the controller was not an accountant and had been fired from three jobs over the prior eight years. Unable to do the accounting work, he hired someone to do his work for him at night. What he was good at was stealing money—he had embezzled several million dollars.

Other factors provide an opportunity to commit and conceal fraud when the company has unclear policies and procedures, fails to teach and stress corporate honesty, and fails to prosecute those who perpetrate fraud. Examples include large, unusual, or complex transactions; numerous adjusting entries at year-end; questionable accounting practices; pushing accounting principles to the limit; related-party transactions; incompetent personnel, inadequate staffing, rapid turnover of key employees, lengthy tenure in a key job, and lack of training.

Frauds occur when employees build mutually beneficial personal relationships with customers or suppliers, such as a purchasing agent buying goods at an inflated price in exchange for a vendor kickback. Fraud can also occur when a crisis arises and normal control procedures are ignored. A Fortune 500 company had three multimillion-dollar frauds the year it disregarded standard internal control procedures while trying to resolve a series of crises.

TABLE 5-4 Opportunities Permitting Employee and Financial Statement Fraud

Internal Control Factors	Other Factors
Failure to enforce/monitor internal controls	Large, unusual, or complex transactions
Management's failure to be involved in the control system	Numerous adjusting entries at year-end
Management override of controls	Related-party transactions
Managerial carelessness, inattention to details	Accounting department that is understaffed, overworked
Dominant and unchallenged management	Incompetent personnel
Ineffective oversight by board of directors	Rapid turnover of key employees
No effective internal auditing staff	Lengthy tenure in a key job
Infrequent third-party reviews	Overly complex organizational structure
Insufficient separation of authorization, custody, and record-keeping duties	No code of conduct, conflict-of-interest statement, or definition of unacceptable behavior
Too much trust in key employees	Frequent changes in auditors, legal counsel
Inadequate supervision	Operating on a crisis basis
Unclear lines of authority	Close association with suppliers/customers
Lack of proper authorization procedures	Assets highly susceptible to misappropriation
No independent checks on performance	Questionable accounting practices
Inadequate documents and records	Pushing accounting principles to the limit
Inadequate system for safeguarding assets	Unclear company policies and procedures
No physical or logical security system	Failing to teach and stress corporate honesty
No audit trails	Failure to prosecute dishonest employees
Failure to conduct background checks	Low employee morale and loyalty
No policy of annual vacations, rotation of duties	

RATIONALIZATIONS A **rationalization** allows perpetrators to justify their illegal behavior. As shown in the Rationalization Triangle in Figure 5-1, this can take the form of a justification ("I only took what they owed me"), an attitude ("The rules do not apply to me"), or a lack of personal integrity ("Getting what I want is more important than being honest"). In other words, perpetrators rationalize that they are not being dishonest, that honesty is not required of them, or that they value what they take more than honesty and integrity. Some perpetrators rationalize that they are not hurting a real person, but a faceless and nameless computer system or an impersonal company that will not miss the money. One such perpetrator stole no more than $20,000, the maximum loss the insurance company would reimburse.

The most frequent rationalizations include the following:

- I am only "borrowing" it, and I will repay my "loan."
- You would understand if you knew how badly I needed it.
- What I did was not that serious.
- It was for a good cause. (The Robin Hood syndrome: robbing the rich to give to the poor)
- In my very important position of trust, I am above the rules.
- Everyone else is doing it.
- No one will ever know.
- The company owes it to me; I am taking no more than is rightfully mine.

Fraud occurs when people have high pressures; an opportunity to commit, conceal, and convert; and the ability to rationalize away their personal integrity. Fraud is less likely to occur when people have few pressures, little opportunity, and high personal integrity. Usually all three elements of the fraud triangle must be present to some degree before a person commits fraud.

Likewise, fraud can be prevented by eliminating or minimizing one or more fraud triangle elements. Although companies can reduce or minimize some pressures and rationalizations, their greatest opportunity to prevent fraud lies in reducing or minimizing opportunity by implementing a good system of internal controls. This is discussed in Chapters 7 through 10.

Computer Fraud

Computer fraud is any fraud that requires computer technology knowledge to perpetrate, investigate, or prosecute it.. Examples include the following:

- Unauthorized theft, use, access, modification, copying, or destruction of software or data
- Theft of assets by altering computer records
- Theft of computer time
- Theft or destruction of hardware or software
- Use of computer resources to commit a felony
- Intent to obtain information or tangible property illegally using computers

Millions of dollars can be stolen in less than a second, leaving little or no evidence. Therefore, computer fraud can be much more difficult to detect than other types of fraud.

The Rise in Computer Fraud

Computer systems are particularly vulnerable for the following reasons:

- People who break into corporate databases can steal, destroy, or alter massive amounts of data in very little time. One bank lost $10 million in cash in a single day.
- Perpetrators can steal many more assets with much less time and effort.
- Some organizations grant employees, customers, and suppliers access to their system. The number and variety of these access points significantly increase the risks.
- Computer programs need to be modified illegally only once for them to operate improperly for as long as they are in use.
- Personal computers (PCs) are vulnerable to security risks. It is difficult to control physical access to each PC that accesses the network. The more legitimate users there are, the greater the risk of an attack on the network. PC users are generally less aware of the

importance of security and control. Segregation of systems duties is difficult because PCs are located in user departments, and one person may be responsible for both development and operations. PCs and their data can be lost, stolen, or misplaced.

- Computer systems face a number of unique challenges: reliability, equipment failure, environmental dependency (i.e., power, damage from water or fire), vulnerability to electromagnetic interference and interruption, eavesdropping, and misrouting.

As early as 1979, *Time* magazine labeled computer fraud a "growth industry." Most businesses have been victimized by computer fraud. During a one-year period, the estimated dollar losses from unauthorized employee computer fraud and abuse in the United States increased 15-fold, from $181,400 to $2.81 million per incident. A few years ago, it was estimated that U.S. Defense Department computers were attacked more than a half million times per year, with the number of incidents increasing 50% to 100% per year. Defense Department staffers and outside consultants made 38,000 "friendly hacks" on their networks to evaluate security. Almost 70% were successful, and the Defense Department detected only 4% of the attacks; the others went unnoticed. The Pentagon, which has the U.S. government's most advanced hacker-awareness program, detected and reported only 1 in 500 break-ins. The Defense Department estimates that more than 100 foreign spy agencies are working to gain access to U.S. government computers as well as an unknown number of criminal organizations. Recently, a spy network in China hacked into 1,300 government and corporate computers in 103 countries.

The number of incidents, the total dollar losses, and the sophistication of the perpetrators and the schemes used to commit computer fraud are increasing rapidly for several reasons:

1. ***Not everyone agrees on what constitutes computer fraud.*** Many people, for example, do not believe that copying software constitutes computer fraud. Software publishers think otherwise and prosecute those who make illegal copies. Some people do not think it is a crime to browse someone else's computer files if they do no harm, whereas companies whose data are browsed feel much differently.
2. ***Many instances of computer fraud go undetected.*** At one time, the FBI estimated that only 1% of computer crime is detected; other estimates are between 5% and 20%.
3. ***A high percentage of frauds is not reported.*** Many companies believe the adverse publicity would result in copycat fraud and a loss of customer confidence, which could cost more than the fraud itself.
4. ***Many networks are not secure.*** Dan Farmer, who wrote SATAN (a network security testing tool), tested 2,200 high-profile Web sites at government institutions, banks, and newspapers. Only three sites detected and contacted him.
5. ***Internet sites offer step-by-step instructions on how to perpetrate computer fraud and abuse.*** For instance, an Internet search found thousands of sites telling how to conduct a "denial of service" attack, a common form of computer abuse.
6. ***Law enforcement cannot keep up with the growth of computer fraud.*** Because of lack of funding and skilled staff, the FBI investigates only 1 in 15 computer crimes.
7. ***Calculating losses is difficult.*** It is difficult to calculate total losses when information is stolen, Web sites are defaced, and viruses shut down entire computer systems.

This increase in computer fraud created the need for the cyber sleuths discussed in Focus 5-1.

Computer Fraud Classifications

As shown in Figure 5-2, computer fraud can be categorized using the data processing model.

INPUT FRAUD The simplest and most common way to commit a computer fraud is to alter or falsify computer input. It requires little skill; perpetrators need only understand how the system operates so they can cover their tracks. For example:

- A man opened a bank account in New York and had blank bank deposit slips printed that were similar to those available in bank lobbies, except that his account number was encoded on them. He replaced the deposit slips in the bank lobby with his forged ones. For three days, bank deposits using the forged slips went into his account. The perpetrator withdrew the money and disappeared. He was never found.

FOCUS 5-1 Cyber Sleuths

Two forensic experts, disguised as repair people, entered an office after hours. They took a digital photograph of three employee desks, made a copy of each employee's hard drive, and used the photo to leave everything as they found it. When the hard drive copy was analyzed, they found evidence of a fraud and notified the company who had hired them. The company turned the case over to law enforcement for investigation and prosecution.

The forensic experts breaking into the company and copying the data worked for a Big Four accounting firm. The accountants, turned cyber sleuths, specialize in catching fraud perpetrators. Cyber sleuths come from a variety of backgrounds, including accounting, information systems, government, law enforcement, military, and banking.

Cyber sleuths need the following skills:

- **Ability to follow a trail, think analytically, and be thorough.** Fraud perpetrators leave tracks, and a cyber sleuth must think analytically to follow paper and electronic trails and uncover fraud. They must be thorough so they do not miss or fail to follow up on clues.
- **Good understanding of information technology (IT).** Cyber sleuths need to understand data storage, data communications, and how to retrieve hidden or deleted files and e-mails.
- **Ability to think like a fraud perpetrator.** Cyber sleuths must understand what motivates perpetrators, how they think, and the schemes they use to commit and conceal fraud.
- **Ability to use hacking tools and techniques.** Cyber sleuths need to understand the tools computer criminals use to perpetrate fraud and abuse.

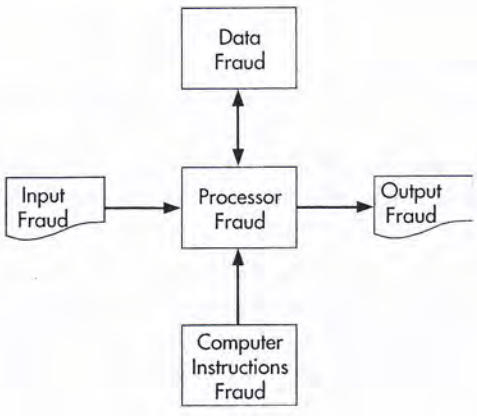
Another way to fight crime is to develop software to examine bank or accounting records for suspicious transactions. Pattern recognition software searches millions of bank, brokerage, and insurance accounts and reviews trillions of dollars worth of transactions each day. Some companies, such as PayPal, use the software to lower their fraud rates significantly.

This software is based on a mathematical principle known as Benford's Law. In 1938, Frank Benford discovered that one can predict the first or second digit in a set of naturally occurring numerical data with surprising accuracy. Benford found that the number 1 is the first digit 31% of the time, compared to only 5% for the number 9. Pattern recognition software uses Benford's Law to examine company databases and transaction records to root out accounting fraud.

Students seeking to find their niche in life should be aware that if playing James Bond sounds appealing, then a career as a computer forensics expert might be the way to go.

- A man used desktop publishing to prepare bills for office supplies that were never ordered or delivered and mailed them to companies across the country. The perpetrator kept the invoice total below $300, an amount that in many companies does not require purchase orders or approvals. A high percentage of the companies paid the bills.
- A Milwaukee woman electronically filed over $13,000 of federal and state income tax refunds for 10 fictitious people.
- An employee at the Veteran's Memorial Coliseum sold customers full-price tickets, entered them as half-price tickets, and pocketed the difference.

FIGURE 5-2
Computer Fraud Classifications



- Railroad employees entered data to scrap over 200 railroad cars. They removed the cars from the railway system, repainted them, and sold them.
- A company providing on-site technical support created exact duplicates of the checks used to pay them, using off-the-shelf scanners, graphics software, and printers. If the double payments were caught, the bank checked their microfiche copies of the two identical checks, assumed a clerical error had occurred, and wrote off the loss as a gesture of maintaining good customer relations.

PROCESSOR FRAUD Processor fraud includes unauthorized system use, including the theft of computer time and services. For example:

- An insurance company installed software to detect abnormal system activity and found that employees were using company computers to run an illegal gambling Web site.
- Two accountants without the appropriate access rights hacked into Cisco's stock option system, transferred over $6.3 million of Cisco stock to their brokerage accounts, and sold the stock. They used part of the funds to support an extravagant lifestyle, including a $52,000 Mercedes-Benz, a $44,000 diamond ring, and a $20,000 Rolex watch.

COMPUTER INSTRUCTIONS FRAUD Computer instruction fraud includes tampering with company software, copying software illegally, using software in an unauthorized manner, and developing software to carry out an unauthorized activity. This approach used to be uncommon because it required specialized programming knowledge. Today, it is more frequent because of the many Web pages that tell users how to create them.

DATA FRAUD Illegally using, copying, browsing, searching, or harming company data constitutes data fraud. It is estimated that, on average, it costs a company $6.6 million, including lost business, to recover from a data breach. The biggest cause of data breaches is employee negligence.

Company employees are much more likely to perpetrate data fraud than outsiders are. A recent study shows that 59% of employees who lost or left a job admitted to stealing confidential company information. Almost 25% of them had access to their former employer's computer system.

In the absence of controls, it is not hard for an employee to steal data. For example, an employee using a small flash drive or an iPod can steal large amounts of data and remove it without being detected. In today's world, you can even buy wristwatches with a USB port and internal memory.

The following are some recent examples of stolen data:

- The office manager of a Wall Street law firm sold information about prospective mergers and acquisitions found in Word files to friends and relatives, who made several million dollars trading the securities.
- A 22-year old Kazakh man broke into Bloomberg's network and stole account information, including that of Michael Bloomberg, the mayor of New York and the founder of the financial news company. He demanded $200,000 in exchange for not using or selling the information. He was arrested in London when accepting the ransom.
- A software engineer tried to steal Intel's new microprocessor plans. Because he could view but not copy or print the plans, he photographed them screen by screen late at night in his office. Unbeknownst to him, one of Intel's controls was to notify security when the plans were viewed after business hours. He was caught red-handed and arrested.
- Cyber-criminals used sophisticated hacking and identity theft techniques to hack into seven accounts at a major online brokerage firm. They sold the securities in those accounts and used the cash to pump up the price of low-priced, thinly traded companies they already owned. Then they sold the stocks in their personal accounts for huge gains. E-trade lost $18 million and Ameritrade $4 million in similar pump-and-dump schemes.
- The U.S. Department of Veterans Affairs was sued because an employee laptop containing the records of 26.5 million veterans was stolen, exposing them to identity theft. Soon thereafter, a laptop with the records of 38,000 people disappeared from a subcontractor's office.

Data can also be changed, damaged, destroyed, or defaced, especially by disgruntled employees and hackers. Vandals broke into the NCAA's Web site before basketball tournament pairings were announced and posted swastikas, racial slurs, and a white-power logo. The Air Force, CIA, and NASA have also been the victims of high-profile Web site attacks. A Computer Security Institute analyst described the problem as "cyberspace vandals with digital spray cans."

Data can be lost as a result of negligence or carelessness. Particularly good sources of confidential data are the hard drives of used computers donated to charity or resold. A professor at a major university bought 10 used computers for his computer forensics class. Using commercially available software, his students found highly confidential data on 8 of the 10 hard drives.

Deleting files does not erase them. Even reformatting a hard drive may not wipe it clean. To erase a hard drive completely, special software must be used. When used computers are to be disposed of, the best way to protect data is to destroy the hard drive.

OUTPUT FRAUD Unless properly safeguarded, displayed or printed output can be stolen, copied, or misused. A Dutch engineer showed that some monitors emit television-like signals that, with the help of some inexpensive electronic gear, can be displayed on a television screen. Under ideal conditions, the signals can be picked up from monitors two miles away. One engineer set up equipment in the basement of an apartment building and read a monitor on the eighth floor.

Fraud perpetrators use computers to forge authentic-looking outputs, such as a paycheck. A fraud perpetrator can scan a company paycheck, use desktop publishing software to erase the payee and amount, and print fictitious paychecks. Losses to check fraud in the United States total more than $20 billion a year.

Preventing and Detecting Fraud and Abuse

To prevent fraud, organizations must create a climate that makes fraud less likely, increases the difficulty of committing it, improves detection methods, and reduces the amount lost if a fraud occurs. These measures are summarized in Table 5-5 and discussed in Chapters 6 through 10.

TABLE 5-5 Summary of Ways to Prevent and Detect Fraud

Make Fraud Less Likely to Occur

- Create an organizational culture that stresses integrity and commitment to ethical values and competence.
- Adopt an organizational structure, management philosophy, operating style, and risk appetite that minimizes the likelihood of fraud.
- Require oversight from an active, involved, and independent audit committee of the board of directors.
- Assign authority and responsibility for business objectives to specific departments and individuals, encourage them to use initiative to solve problems, and hold them accountable for achieving those objectives.
- Identify the events that lead to increased fraud risk, and take steps to prevent, avoid, share, or accept that risk.
- Develop a comprehensive set of security policies to guide the design and implementation of specific control procedures, and communicate them effectively to company employees.
- Implement human resource policies for hiring, compensating, evaluating, promoting, and discharging employees that send messages about the required level of ethical behavior and integrity.
- Effectively supervise employees, including monitoring their performance and correcting their errors.
- Train employees in integrity and ethical considerations, as well as security and fraud prevention measures.
- Require annual employee vacations and signed confidentiality agreements; periodically rotate duties of key employees.
- Implement formal and rigorous project development and acquisition controls, as well as change management controls.
- Increase the penalty for committing fraud by prosecuting fraud perpetrators more vigorously.

Increase the Difficulty of Committing Fraud

- Develop a strong system of internal controls.
- Segregate the accounting functions of authorization, recording, and custody.
- Implement a proper segregation of duties between systems functions.
- Restrict physical and remote access to system resources to authorized personnel.

TABLE 5-5 Continued

- Require transactions and activities to be authorized by appropriate supervisory personnel. Have the system authenticate the person, and their right to perform the transaction, before allowing the transaction to take place.
- Use properly designed documents and records to capture and process transactions.
- Safeguard all assets, records, and data.
- Require independent checks on performance, such as reconciliation of two independent sets of records, where practical.
- Implement computer-based controls over data input, computer processing, data storage, data transmission, and information output.
- Encrypt stored and transmitted data and programs to protect them from unauthorized access and use.
- When disposing of used computers, destroy the hard drive to keep criminals from mining recycled hard drives.
- Fix software vulnerabilities by installing operating system updates, as well as security and application programs.

Improve Detection Methods

- Create an audit trail so individual transactions can be traced through the system to the financial statements and financial statement data can be traced back to individual transactions.
- Conduct periodic external and internal audits, as well as special network security audits.
- Install fraud detection software.
- Implement a fraud hotline.
- Employ a computer security officer, computer consultants, and forensic specialists as needed.
- Monitor system activities, including computer and network security efforts, usage and error logs, and all malicious actions. Use intrusion detection systems to help automate the monitoring process.

Reduce Fraud Losses

- Maintain adequate insurance.
- Develop comprehensive fraud contingency, disaster recovery, and business continuity plans.
- Store backup copies of program and data files in a secure off-site location.
- Use software to monitor system activity and recover from fraud.

Summary and Case Conclusion

Needing evidence to support his belief that Don Hawkins had committed a fraud, Jason Scott expanded the scope of his investigation. A week later, Jason presented his findings to the president of Northwest. To make his case hit close to home, Jason presented her with a copy of her IRS withholding report and pointed out her withholdings. Then he showed her a printout of payroll withholdings and pointed out the $5 difference, as well as the difference of several thousand dollars in Don Hawkins's withholdings. This got her attention, and Jason explained how he believed a fraud had been perpetrated.

During the latter part of the prior year, Don had been in charge of a payroll program update. Because of problems with other projects, other systems personnel had not reviewed the update. Jason asked a former programmer to review the code changes. She found program code that subtracted $5 from each employee's withholdings and added it to Don's withholdings. Don got his hands on the money when the IRS sent him a huge refund check.

Don apparently intended to use the scheme every year, as he had not removed the incriminating code. He must have known there was no reconciliation of payroll withholdings with the IRS report. His simple plan could have gone undetected for years if Jason had not overheard someone in the cafeteria talk about a $5 difference.

Jason learned that Don had become disgruntled when he was passed over the previous year for a managerial position. He made comments to coworkers about favoritism and unfair treatment and mentioned getting even with the company somehow. No one knew where he got the money, but Don purchased an expensive sports car in April, boasting that he had made a sizable down payment.

When the president asked how the company could prevent this fraud from happening again, Jason suggested the following guidelines:

1. Review internal controls to determine their effectiveness in preventing fraud. An existing control—reviewing program changes—could have prevented Don's scheme had it been followed. As a result, Jason suggested a stricter enforcement of the existing controls.

2. Put new controls into place to detect fraud. For example, Jason suggested a reconciliation of the IRS report and payroll record withholdings.
3. Train employees in fraud awareness, security measures, and ethical issues.

Jason urged the president to prosecute the case. She was reluctant to do so because of the adverse publicity and the problems it would cause Don's wife and children. Jason's supervisor tactfully suggested that if other employees found out that Don was not prosecuted, it would send the wrong message to the rest of the company. The president finally conceded to prosecute if the company could prove that Don was guilty. The president agreed to hire a forensic accountant to build a stronger case against Don and try to get him to confess.

Key Terms

sabotage 143
cookie 143
fraud 143
white-collar criminal 144
misappropriation of assets 144
fraudulent financial reporting 145
pressure 146
opportunity 148
lapping 148
kiting 148
rationalization 150
computer fraud 150

AIS IN ACTION

Chapter Quiz

1. Which of the following is a fraud in which later payments on account are used to pay off earlier payments that were stolen?
   a. lapping
   b. kiting
   c. Ponzi scheme
   d. salami technique
2. Which type of fraud is associated with 50% of all auditor lawsuits?
   a. kiting
   b. fraudulent financial reporting
   c. Ponzi schemes
   d. lapping
3. Which of the following statements is FALSE?
   a. The psychological profiles of white-collar criminals differ from those of violent criminals.
   b. The psychological profiles of white-collar criminals are significantly different from those of the general public.
   c. There is little to no difference between computer fraud perpetrators and other types of white-collar criminals.
   d. Computer fraud perpetrators often do not view themselves as criminals.
4. Which of the following conditions is/are usually necessary for a fraud to occur? (Select all correct answers.)
   a. pressure
   b. opportunity
   c. explanation
   d. rationalization
5. Which of the following is NOT an example of computer fraud?
   a. theft of money by altering computer records
   b. obtaining information illegally using a computer
   c. failure to perform preventive maintenance on a computer
   d. unauthorized modification of a software program

6. Which of the following causes the majority of computer security problems?
   a. human errors
   b. software errors
   c. natural disasters
   d. power outages

7. Which of the following is NOT one of the responsibilities of auditors in detecting fraud according to SAS No. 99?
   a. Evaluate the results of their audit tests.
   b. Incorporate a technology focus.
   c. Discuss the risks of material fraudulent misstatements.
   d. Catch the perpetrators in the act of committing the fraud.

8. Which of the following control procedures is most likely to deter lapping?
   a. encryption
   b. continual update of the access control matrix
   c. background check on employees
   d. periodic rotation of duties

9. Which of the following is the most important, basic, and effective control to deter fraud?
   a. enforced vacations
   b. logical access control
   c. segregation of duties
   d. virus protection controls

10. Once fraud has occurred, which of the following will reduce fraud losses? (Select all correct answers.)
    a. insurance
    b. regular backup of data and programs
    c. contingency plan
    d. segregation of duties

Discussion Questions

5.1. Do you agree that the most effective way to obtain adequate system security is to rely on the integrity of company employees? Why or why not? Does this seem ironic? What should a company do to ensure the integrity of its employees?

5.2. You are the president of a multinational company in which an executive confessed to kiting $100,000. What is kiting, and what can your company do to prevent it? How would you respond to the confession? What issues must you consider before pressing charges?

5.3. Discuss the following statement by Roswell Steffen, a convicted embezzler: "For every foolproof system, there is a method for beating it." Do you believe a completely secure computer system is possible? Explain. If internal controls are less than 100% effective, why should they be employed at all?

5.4. Revlon hired Logisticon to install a real-time invoice and inventory processing system. Seven months later, when the system crashed, Revlon blamed the Logisticon programming bugs they discovered and withheld payment on the contract. Logisticon contended that the software was fine and that it was the hardware that was faulty. When Revlon again refused payment, Logisticon repossessed the software using a telephone dial-in feature to disable the software and render the system unusable. After a three-day standoff, Logisticon reactivated the system. Revlon sued Logisticon, charging them with trespassing, breach of contract, and misappropriation of trade secrets (Revlon passwords). Logisticon countersued for breach of contract. The companies settled out of court.

Would Logisticon's actions be classified as sabotage or repossession? Why? Would you find the company guilty of committing a computer crime? Be prepared to defend your position to the class.

5.5. Because improved computer security measures sometimes create a new set of problems—user antagonism, sluggish response time, and hampered performance—some people believe the most effective computer security is educating users about good moral conduct. Richard Stallman, a computer activist, believes software licensing is antisocial because it

prohibits the growth of technology by keeping information away from the neighbors. He believes high school and college students should have unlimited access to computers without security measures so that they can learn constructive and civilized behavior. He states that a protected system is a puzzle and, because it is human nature to solve puzzles, eliminating computer security so that there is no temptation to break in would reduce hacking.

Do you agree that software licensing is antisocial? Is ethical teaching the solution to computer security problems? Would the removal of computer security measures reduce the incidence of computer fraud? Why or why not?

Problems

5.1. You were asked to investigate extremely high, unexplained merchandise shortages at a department store chain. You found the following:

a. The receiving department supervisor owns and operates a boutique carrying many of the same labels as the chain store. The general manager is unaware of the ownership interest.
b. The receiving supervisor signs receiving reports showing that the total quantity shipped by a supplier was received and then diverts 5% to 10% of each shipment to the boutique.
c. The store is unaware of the short shipments because the receiving report accompanying the merchandise to the sales areas shows that everything was received.
d. Accounts Payable paid vendors for the total quantity shown on the receiving report.
e. Based on the receiving department supervisor's instructions, quantities on the receiving reports were not counted by sales personnel.

Required

Classify each of the five situations as a fraudulent act, a fraud symptom, an internal control weakness, or an event unrelated to the investigation. Justify your answers.
(CIA Examination, adapted)

5.2. A client heard through its hot line that John, the purchases journal clerk, periodically enters fictitious acquisitions. After John creates a fictitious purchase, he notifies Alice, the accounts payable ledger clerk, so she can enter them in her ledger. When the payables are processed, the payment is mailed to the nonexistent supplier's address, a post office box rented by John. John deposits the check in an account he opened in the nonexistent supplier's name.

Required

a. Define *fraud*, *fraud deterrence*, *fraud detection*, and *fraud investigation*.
b. List four personal (as opposed to organizational) fraud symptoms, or red flags, that indicate the possibility of fraud. Do not confine your answer to this example.
c. List two procedures you could follow to uncover John's fraudulent behavior.
(CIA Examination, adapted)

5.3. The computer frauds that are publicly revealed represent only the tip of the iceberg. Although many people perceive that the major threat to computer security is external, the more dangerous threats come from insiders. Management must recognize these problems and develop and enforce security programs to deal with the many types of computer fraud.

Required

Explain how each of the following six types of fraud is committed. Using the format provided, identify a different method of protection for each, and describe how it works.
(CMA Examination, adapted)

Type of Fraud	Explanation	Identification and Description of Protection Methods
a. Input manipulation		
b. Program alteration		
c. File alteration		
d. Data theft		
e. Sabotage		
f. Theft of computer time		

5.4. Environmental, institutional, or individual pressures and opportune situations, which are present to some degree in all companies, motivate individuals and companies to engage in fraudulent financial reporting. Fraud prevention and detection require that pressures and opportunities be identified and evaluated in terms of the risks they pose to a company.

Required

a. Identify two company pressures that would increase the likelihood of fraudulent financial reporting.
b. Identify three corporate opportunities that make fraud easier to commit and detection less likely.
c. For each of the following, identify the external environmental factors that should be considered in assessing the risk of fraudulent financial reporting:
   - The company's industry
   - The company's business environment
   - The company's legal and regulatory environment
d. What can top management do to reduce the possibility of fraudulent financial reporting? *(CMA Examination, adapted)*

5.5. For each of the following independent cases of employee fraud, recommend how to prevent similar problems in the future.

a. Abnormal inventory shrinkage in the audiovisual department at a retail chain store led internal auditors to conduct an in-depth audit of the department. They learned that one customer frequently bought large numbers of small electronic components from a certain cashier. The auditors discovered that they had colluded to steal electronic components by not recording the sale of items the customer took from the store.
b. During an unannounced audit, auditors discovered a payroll fraud when they, instead of department supervisors, distributed paychecks. When the auditors investigated an unclaimed paycheck, they discovered that the employee quit four months previously after arguing with the supervisor. The supervisor continued to turn in a time card for the employee and pocketed his check.
c. Auditors discovered an accounts payable clerk who made copies of supporting documents and used them to support duplicate supplier payments. The clerk deposited the duplicate checks in a bank account she had opened using a name similar to that of the supplier. *(CMA Examination, adapted)*

5.6. An auditor found that Rent-A-Wreck management does not always comply with its stated policy that sealed bids be used to sell obsolete cars. Records indicated that several vehicles with recent major repairs were sold at negotiated prices. Management vigorously assured the auditor that performing limited repairs and negotiating with knowledgeable buyers resulted in better sales prices than the sealed-bid procedures. Further investigation revealed that the vehicles were sold to employees at prices well below market value. Three managers and five other employees pleaded guilty to criminal charges and made restitution.

Required

a. List the fraud symptoms that should have aroused the auditor's suspicion.
b. What audit procedures would show that fraud had in fact occurred? *(CIA Examination, adapted)*

5.7. A bank auditor met with the senior operations manager to discuss a customer's complaint that an auto loan payment was not credited on time. The customer said the payment was made on May 5, its due date, at a teller's window using a check drawn on an account in the bank. On May 10, when the customer called for a loan pay-off balance so he could sell the car, he learned that the payment had not been credited to the loan. On May 12, the customer went to the bank to inquire about the payment and meet with the manager. The manager said the payment had been made on May 11. The customer was satisfied because no late charge would have been assessed until May 15. The manager asked whether the auditor was comfortable with this situation.

The auditor located the customer's paid check and found that it had cleared on May 5. The auditor traced the item back through the computer records and found that the teller had processed the check as being cashed. The auditor traced the payment through the entry records of May 11 and found that the payment had been made with cash instead of a check.

Required

What type of embezzlement scheme is this, and how does it work?

(CIA Examination, adapted)

5.8. Jamison Cardstock did not spend much time or money on internal controls for its cash transactions. The following information reflects Jamison's cash position as of June 30:

- The accounting records show a cash balance of $18,901.62, including undeposited cash receipts.
- A $100 bank statement credit was not recorded in the company's accounting records.
- The bank statement balance was $15,550.
- There were six outstanding checks:

Check Number	Amount
62	$116.25
183	$150.00
284	$253.25
8621	$190.71
8623	$206.80
8632	$145.28

The company cashier embezzled all undeposited cash receipts in excess of the $3,794.41 listed on the following bank reconciliation:

Balance per books, June 30			$18,901.62
Add: Outstanding Checks:			
No. 8621	$190.71		
No. 8623	$206.80		
No. 8632	$145.28	442.79	
			$19,344.41
Subtract: Undeposited Receipts			3,794.41
Balance per bank, June 30			$15,550.00
Subtract: Unrecorded Credit			100.00
True Cash, June 30			$15,450.00

Required

a. Prepare a schedule showing how much the cashier embezzled.
b. Describe how the cashier attempted to hide the theft. *(AICPA, adapted)*

5.9. An accountant with the Atlanta Olympic Games was charged with embezzling over $60,000 to purchase a Mercedes-Benz and to invest in a certificate of deposit. Police alleged that he created fictitious invoices from two companies that had contracts with the Olympic Committee: International Protection Consulting and Languages Services. He then wrote checks to pay the fictitious invoices and deposited them into a bank account he had opened under the name of one of the companies. When he was apprehended, he cooperated with

Case 5-1 David L. Miller: Portrait of a White-Collar Criminal

There is an old saying: Crime doesn't pay. However, for David Miller crime paid for two Mercedes-Benz sedans; a lavish suburban home; a condominium at Myrtle Beach; expensive suits; tailored and monogrammed shirts; diamond, sapphire, ruby, and emerald rings for his wife; and a new car for his father-in-law. Though Miller confessed to embezzling funds from six different employers over a 20-year period, he has never been prosecuted or incarcerated—in large part because his employers never turned him in.

Miller was fired from his first employer for stealing $200. After an assortment of odd jobs, he worked as an accountant for a local baker. Miller was caught embezzling funds and paid back the $1,000 he stole. Again, law enforcement was not notified, and he was quietly dismissed.

Several months after Miller started work at Wheeling Bronze, his third victim, the president discovered a $30,000 cash shortfall and several missing returned checks. An extensive search found the canceled checks, with forged signatures, in an outdoor sand pile. Miller confessed to the scheme and was given the choice of repaying the stolen funds or being prosecuted. When Miller's parents mortgaged their home and repaid the stolen money, he escaped prosecution.

Miller's fourth victim was Robinson Pipe Cleaning. When Miller was caught embezzling funds, he again avoided prosecution by promising to repay the $20,000 he stole.

Miller's fifth victim was Crest Industries, where he worked as accountant. He was an ideal employee—dedicated and hard working, doing outstanding work. He was quickly promoted to office manager and soon purchased a new home, car, and wardrobe. Two years later, Crest auditors discovered that $31,000 was missing. Miller had written several checks to himself, recorded them as payments to suppliers, and intercepted and altered the monthly bank statements. With the stolen money, he financed his lifestyle and repaid Wheeling Bronze and Robinson Pipe Cleaning. Once again, Miller tearfully confessed, claiming he had never embezzled funds previously. Miller showed so much remorse that Crest hired a lawyer for him. He promised to repay the stolen money, gave Crest a lien on his house, and was quietly dismissed. Because Crest management did not want to harm Miller's wife and three children, Crest never pressed charges.

Miller's sixth victim was Rustcraft Broadcasting Company. When Rustcraft was acquired by Associated Communications, Miller moved to Pittsburgh to become Associated's new controller. Miller immediately began dipping into Associated's accounts. Over a six-year period, Miller embezzled $1.36 million, $450,000 of that after he was promoted to CFO. Miller circumvented the need for two signatures on checks by asking executives leaving on vacation to sign several checks "just in case" the company needed to disburse funds while he was gone. Miller used the checks to siphon funds to his personal account. To cover the theft, Miller removed the canceled check from the bank reconciliation and destroyed it. The stolen amount was charged to a unit's expense account to balance the company's books.

While working at Associated, Miller bought a new house, new cars, a vacation home, and an extravagant wardrobe. He was generous with tips and gifts. His $130,000 salary could not have supported this lifestyle, yet no one at Associated questioned the source of his conspicuous consumption. Miller's lifestyle came crashing down while he was on vacation and the bank called to inquire about a check written to Miller. Miller confessed and, as part of his out-of-court settlement, Associated received most of Miller's personal property.

Miller cannot explain why he was never prosecuted. His insistence that he was going to pay his victims back usually satisfied his employers and got him off the hook. He believes these agreements actually contributed to his subsequent thefts; one rationalization for stealing from a new employer was to pay back the former one. Miller believes his theft problem is an illness, like alcoholism or compulsive gambling, that is driven by a subconscious need to be admired and liked by others. He thought that by spending money, others would like him. Ironically, he was universally well liked and admired at each job, for reasons that had nothing to do with money. In fact, one Associated coworker was so surprised by the thefts that he said it was like finding out that your brother was an ax murderer. Miller claims he is not a bad person; he never intended to hurt anyone, but once he got started, he could not stop.

After leaving Associated, Miller was hired by a former colleague, underwent therapy, and now believes he has resolved his problem with compulsive embezzlement.

1. How does Miller fit the profile of the average fraud perpetrator? How does he differ? How did these characteristics make him difficult to detect?
2. Explain the three elements of the opportunity triangle (commit, conceal, convert), and discuss how Miller accomplished each when embezzling funds from Associated Communications. What specific concealment techniques did Miller use?
3. What pressures motivated Miller to embezzle? How did Miller rationalize his actions?
4. Miller had a framed T-shirt in his office that said, "He who dies with the most toys wins." What does this tell you about Miller? What lifestyle red flags could have tipped off the company to the possibility of fraud?
5. Why do companies hesitate to prosecute white-collar criminals? What are the consequences of not prosecuting? How could law enforcement officials encourage more prosecution?
6. What could the victimized companies have done to prevent Miller's embezzlement?

Source: Based on Bryan Burrough, "David L. Miller Stole from His Employer and Isn't in Prison," *The Wall Street Journal* (September 19, 1986): 1.

police to the extent of telling them of the bogus bank account and the purchase of the Mercedes-Benz and the CD. The accountant was a recent honors graduate from a respected university who, supervisors stated, was a very trusted and loyal employee.

a. How does the accountant fit the profile of a fraudster? How does he not fit the profile?
b. What fraud scheme did he use to perpetrate his fraud?
c. What controls could have prevented his fraud?
d. What controls could have detected his fraud?

5.10. Lexsteel, a manufacturer of steel furniture, has facilities throughout the United States. Problems with the accounts payable system have prompted Lexsteel's external auditor to recommend a detailed study to determine the company's exposure to fraud and to identify ways to improve internal control. Lexsteel's controller assigned the study to Dolores Smith. She interviewed Accounts Payable employees and created the flowchart of the current system shown in Figure 5-3.

Lexsteel's purchasing, production control, accounts payable, and cash disbursements functions are centralized at corporate headquarters. The company mainframe at corporate headquarters is linked to the computers at each branch location by leased telephone lines.

The mainframe generates production orders and the bills of material needed for the production runs. From the bills of material, purchase orders for raw materials are generated and e-mailed to vendors. Each purchase order tells the vendor which manufacturing plant to ship the materials to. When the raw materials arrive, the manufacturing plants produce the items on the production orders received from corporate headquarters.

The manufacturing plant checks the goods received for quality, counts them, reconciles the count to the packing slip, and e-mails the receiving data to Accounts Payable. If raw material deliveries fall behind production, each branch manager can send emergency purchase orders directly to vendors. Emergency order data and verification of materials received are e-mailed to Accounts Payable. Since the company employs a computerized perpetual inventory system, periodic physical counts of raw materials are not performed.

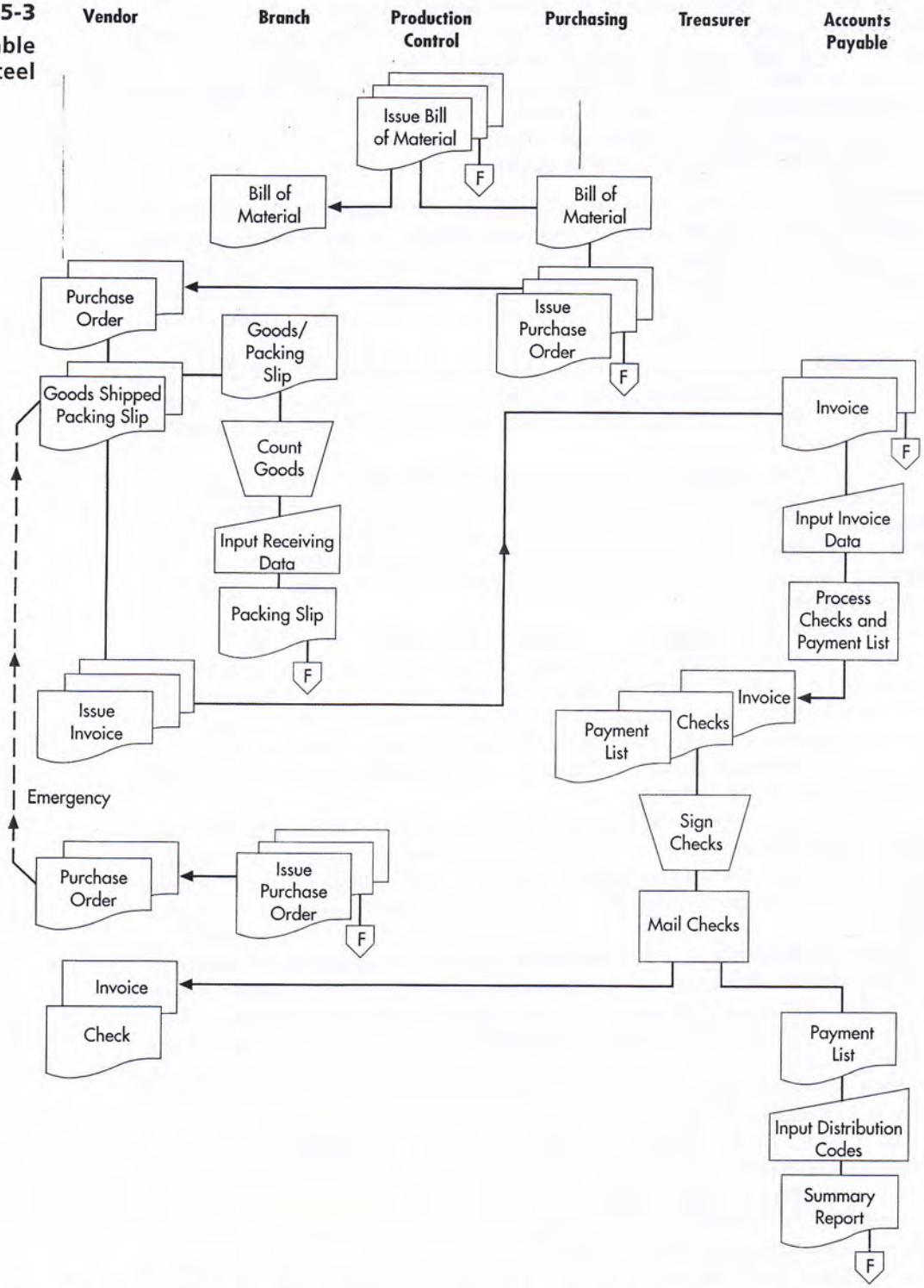
Vendor invoices are e-mailed to headquarters and entered by Accounts Payable when received. This often occurs before the branch offices transmit the receiving data. Payments are due 10 days after the company receives the invoices. Using information on the invoice, Data Entry calculates the final day the invoice can be paid, and it is entered as the payment due date.

Once a week, invoices due the following week are printed in chronological entry order on a payment listing, and the corresponding checks are drawn. The checks and payment listing are sent to the treasurer's office for signature and mailing to the payee. The check number is printed by the computer, displayed on the check and the payment listing, and validated as the checks are signed. After the checks are mailed, the payment listing is returned to Accounts Payable for filing. When there is insufficient cash to pay all the invoices, the treasurer retains certain checks and the payment listing until all checks can be paid. When the remaining checks are mailed, the listing is then returned to Accounts Payable. Often, weekly check mailings include a few checks from the previous week, but rarely are there more than two weekly listings involved.

When Accounts Payable receives the payment listing from the treasurer's office, the expenses are distributed, coded, and posted to the appropriate cost center accounts. Accounts Payable processes weekly summary performance reports for each cost center and branch location.

1. Discuss three ways Lexsteel is exposed to fraud, and recommend improvements to correct these weaknesses.
2. Describe three ways in which management information could be distorted, and recommend improvements to correct these weaknesses.
3. Identify and explain three strengths in Lexsteel's procedures. *(CMA Examination, adapted)*

FIGURE 5-3
Accounts Payable Procedures at Lexsteel



5.11. The Association of Certified Fraud Examiners periodically prepares an article called "What Is Your Fraud IQ?" It consists of 10 or more multiple choice questions dealing with various aspects of fraud. The answers, as well as an explanation of each answer, are provided at the end of the article. Visit the *Journal of Accountancy* site (http://www.journalofaccountancy.com) and search for the articles. Read and answer the questions in three of these articles, and then check your answers.

5.12. Explore the Anti-Fraud and Forensic Accounting portion of the AICPA Web site (www.aicpa.org/InterestAreas/ForensicAndValuation/Resources/ForensicAcctg/Pages/default.aspx), and write a two-page report on the three most interesting things you found on the site.

Case 5-1 David L. Miller: Portrait of a White-Collar Criminal

There is an old saying: Crime doesn't pay. However, for David Miller crime paid for two Mercedes-Benz sedans; a lavish suburban home; a condominium at Myrtle Beach; expensive suits; tailored and monogrammed shirts; diamond, sapphire, ruby, and emerald rings for his wife; and a new car for his father-in-law. Though Miller confessed to embezzling funds from six different employers over a 20-year period, he has never been prosecuted or incarcerated—in large part because his employers never turned him in.

Miller was fired from his first employer for stealing $200. After an assortment of odd jobs, he worked as an accountant for a local baker. Miller was caught embezzling funds and paid back the $1,000 he stole. Again, law enforcement was not notified, and he was quietly dismissed.

Several months after Miller started work at Wheeling Bronze, his third victim, the president discovered a $30,000 cash shortfall and several missing returned checks. An extensive search found the canceled checks, with forged signatures, in an outdoor sand pile. Miller confessed to the scheme and was given the choice of repaying the stolen funds or being prosecuted. When Miller's parents mortgaged their home and repaid the stolen money, he escaped prosecution.

Miller's fourth victim was Robinson Pipe Cleaning. When Miller was caught embezzling funds, he again avoided prosecution by promising to repay the $20,000 he stole.

Miller's fifth victim was Crest Industries, where he worked as accountant. He was an ideal employee—dedicated and hard working, doing outstanding work. He was quickly promoted to office manager and soon purchased a new home, car, and wardrobe. Two years later, Crest auditors discovered that $31,000 was missing. Miller had written several checks to himself, recorded them as payments to suppliers, and intercepted and altered the monthly bank statements. With the stolen money, he financed his lifestyle and repaid Wheeling Bronze and Robinson Pipe Cleaning. Once again, Miller tearfully confessed, claiming he had never embezzled funds previously. Miller showed so much remorse that Crest hired a lawyer for him. He promised to repay the stolen money, gave Crest a lien on his house, and was quietly dismissed. Because Crest management did not want to harm Miller's wife and three children, Crest never pressed charges.

Miller's sixth victim was Rustcraft Broadcasting Company. When Rustcraft was acquired by Associated Communications, Miller moved to Pittsburgh to become Associated's new controller. Miller immediately began dipping into Associated's accounts. Over a six-year period, Miller embezzled $1.36 million, $450,000 of that after he was promoted to CFO. Miller circumvented the need for two signatures on checks by asking executives leaving on vacation to sign several checks "just in case" the company needed to disburse funds while he was gone. Miller used the checks to siphon funds to his personal account. To cover the theft, Miller removed the canceled check from the bank reconciliation and destroyed it. The stolen amount was charged to a unit's expense account to balance the company's books.

While working at Associated, Miller bought a new house, new cars, a vacation home, and an extravagant wardrobe. He was generous with tips and gifts. His $130,000 salary could not have supported this lifestyle, yet no one at Associated questioned the source of his conspicuous consumption. Miller's lifestyle came crashing down while he was on vacation and the bank called to inquire about a check written to Miller. Miller confessed and, as part of his out-of-court settlement, Associated received most of Miller's personal property.

Miller cannot explain why he was never prosecuted. His insistence that he was going to pay his victims back usually satisfied his employers and got him off the hook. He believes these agreements actually contributed to his subsequent thefts; one rationalization for stealing from a new employer was to pay back the former one. Miller believes his theft problem is an illness, like alcoholism or compulsive gambling, that is driven by a subconscious need to be admired and liked by others. He thought that by spending money, others would like him. Ironically, he was universally well liked and admired at each job, for reasons that had nothing to do with money. In fact, one Associated coworker was so surprised by the thefts that he said it was like finding out that your brother was an ax murderer. Miller claims he is not a bad person; he never intended to hurt anyone, but once he got started, he could not stop.

After leaving Associated, Miller was hired by a former colleague, underwent therapy, and now believes he has resolved his problem with compulsive embezzlement.

1. How does Miller fit the profile of the average fraud perpetrator? How does he differ? How did these characteristics make him difficult to detect?
2. Explain the three elements of the opportunity triangle (commit, conceal, convert), and discuss how Miller accomplished each when embezzling funds from Associated Communications. What specific concealment techniques did Miller use?
3. What pressures motivated Miller to embezzle? How did Miller rationalize his actions?
4. Miller had a framed T-shirt in his office that said, "He who dies with the most toys wins." What does this tell you about Miller? What lifestyle red flags could have tipped off the company to the possibility of fraud?
5. Why do companies hesitate to prosecute white-collar criminals? What are the consequences of not prosecuting? How could law enforcement officials encourage more prosecution?
6. What could the victimized companies have done to prevent Miller's embezzlement?

Source: Based on Bryan Burrough, "David L. Miller Stole from His Employer and Isn't in Prison," *The Wall Street Journal* (September 19, 1986): 1.

Case 5-2 Heirloom Photo Plans

Heirloom Photos sells a $900 photography plan to rural customers using a commissioned sales force. Rather than pay the price up front, most customers pay $250 down and make 36 monthly payments of $25 each. The $900 plan includes the following:

1. A coupon book good for one free sitting every 6 months for the next 5 years (10 sittings) at any Heirloom-approved photo studio. The customer receives one free 11-by-14-inch black-and-white print. Additional photos or color upgrades can be purchased at the photographer's retail prices.
2. To preserve the 11-by-14-inch photos, the family name is embossed in 24-carat gold on a leather-bound photo album.

The embossed leather album, with a retail value of $300, costs Heirloom $75. Each sitting and free 11-by-14-inch print, with a retail value of $150, costs Heirloom only $50 because photographers are given exclusive rights to all Heirloom customers in a geographic region and have the opportunity to offer customers upgrades to color and/or more pictures.

The commissioned sales staff is paid on the 10th of each month, based upon the prior month's sales. The commission rates are as follows:

Number of plans sold	Commission	Quantity bonus
Fewer than 100	$100 per plan	
101 to 200	$125 per plan	On sale of plan #101, $2,500 is paid to cover the extra $25 on the first 100 sales
More than 200	$150 per plan	On sale of plan #201, $5,000 is paid to cover the extra $25 on the first 200 sales

Over 70% of all agents sell at least 101 plans per year; 40% sell over 200. There is a strong sales surge before year-end as customers purchase plans to give as holiday gifts. About 67% of all agents reach their highest incentive level in late November or December. Heirloom treats the sales staff and the photographers as independent contractors and does not withhold any income or payroll taxes on amounts paid to them.

Salespeople send Heirloom's accounting department the order form, the total payment or the down payment, and the signed note for $650 if the customer finances the transaction. Often, the payment is a hand-written money order. Because many customers live in rural areas, the return address is often a Post Office box, and some customers do not have phones. Heirloom does not perform any credit checks of customers.

Heirloom makes the following entries at the time a new contract is recorded:

To record sale of the contract (assumes contract financed)		
Cash	250	
Note Receivable	650	
Sales of Photo Plans		900
To record expenses related to the sale		
Album Expense	65	
Embossing/shipping	10	
Sales Expense	130	
Album Inventory		65
Accounts Payable		10
Commissions Payable		130
(Sales expense is estimated using the average cost paid to salespersons in the prior year.)		
To record the liability for Photographer Sittings Expense		
Photographer Expense	500	
Accrued Liabilities		500

Because the entire cost of the photographer is accrued, the company points to the last entry to show how conservative its accounting is.

After waiting 10 days for the check or money order to clear, Heirloom embosses and ships the album, the photo coupon book, and a payment coupon book with 36 payments of $25. Customers mail a payment coupon and a check or money order to a three-person Receivables Department at headquarters. The Receivables employees open the envelopes, post the payments to the receivables records, and prepare the bank deposit.

The photo coupon book has 10 coupons for photographer sessions, each good for a specific 6-month period. If not used within the 6-month period, the coupon expires.

Each month, the credit manager sends letters and makes phone calls to collect on delinquent accounts. Between 35% and 40% of all customers eventually stop paying on their notes, usually either early in the contract (months 4 to 8) or at the 2-year point (months 22 to 26).

Notes are written off when they are 180 days delinquent. Heirloom's CFO and credit manager use their judgment to adjust the Allowance for Bad Debts monthly. They are confident they can accurately predict the Allowance balance needed at any time, which historically has been about 5% of outstanding receivables.

Agricultural product prices in the area where Heirloom sells its plans have been severely depressed for the second straight year.

Heirloom has been growing quickly and finds that it is continually running short of cash, partly because of the large salaries paid to the two equal owners and their wives. (The wives each receive $100,000 to serve as the treasurer and the secretary; very little, if any, time is required in these duties.) In addition, Heirloom spent large amounts of cash to buy its headquarters,

equipment and furnishings, and expensive automobiles for the two owners, their wives, and the four vice presidents.

Heirloom needs to borrow from a local bank for corporate short-term operating purposes. It is willing to pledge unpaid contracts as collateral for a loan. A local bank president is willing to lend Heirloom up to 70% of the value of notes receivable that are not more than 60 days overdue. Heirloom must also provide, by the fifth day of each month, a note receivable aging list for the preceding month and a calculation showing the maximum amount Heirloom may borrow under the agreement.

1. **Figure 5-4** shows the employees and external parties that deal with Heirloom. Explain how Heirloom could defraud the bank and how each internal and external party, except the bank, could defraud Heirloom.
2. What risk factor, unusual item, or abnormality would alert you to each fraud?
3. What control weaknesses make each fraud possible?
4. Recommend one or more controls to prevent or detect each means of committing fraud.

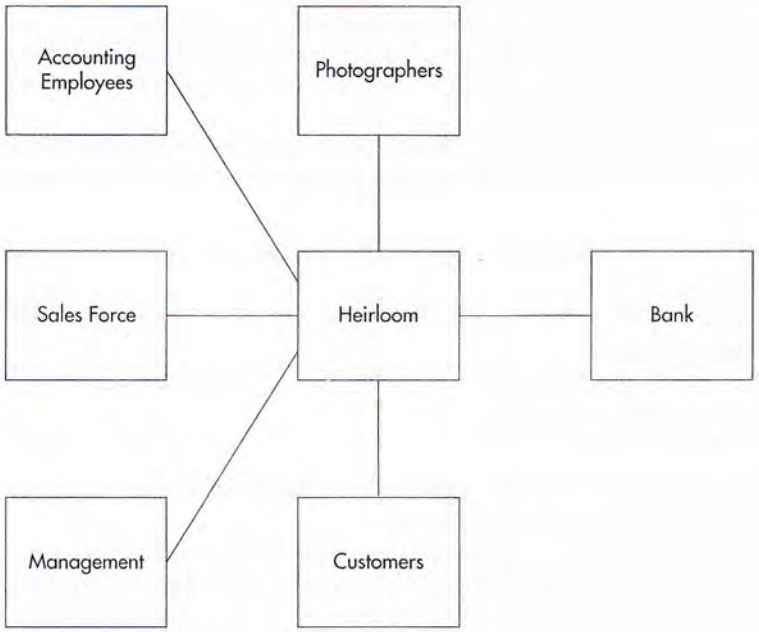


FIGURE 5-4
Internal and External Relationships at Heirloom Photos

AIS IN ACTION SOLUTIONS

Quiz Key

1. Which of the following is a fraud in which later payments on account are used to pay off earlier payments that were stolen?
   ▶ **a.** lapping (Correct.)
   b. kiting (Incorrect. In a kiting scheme, the perpetrator creates cash by transferring money between banks.)
   c. Ponzi scheme (Incorrect. In a Ponzi scheme, money from new investors is used to pay off earlier investors.)
   d. salami technique (Incorrect. The salami technique involves stealing tiny slices of money over a period of time.)
2. Which type of fraud is associated with 50% of all auditor lawsuits?
   a. kiting (Incorrect. Losses from kiting, a scheme involving bank transfers, are not large enough to be associated with 50% of auditor lawsuits.)

d. power outages (Incorrect. Massive power failures caused by defective software occasionally occur and leave hundreds of thousands of people and businesses without power, but this is not the main cause of computer security issues.)

7. Which of the following is NOT one of the responsibilities of auditors in detecting fraud according to SAS No. 99?
   a. Evaluate the results of their audit tests. (Incorrect. When an audit is completed, auditors must evaluate whether any identified misstatements indicate the presence of fraud. If they do, the auditor must determine the impact of this on the financial statements and the audit.)
   b. Incorporate a technology focus. (Incorrect. SAS No. 99 recognizes the impact technology has on fraud risks and provides commentary and examples specifically recognizing this impact. It also notes the opportunities the auditor has to use technology to design fraud-auditing procedures.)
   c. Discuss the risks of material fraudulent misstatements. (Incorrect.While planning the audit, team members should discuss among themselves how and where the company's financial statements might be susceptible to fraud.)
   ▶ **d.** Catch the perpetrators in the act of committing the fraud. (Correct. SAS No. 99 does not require auditors to witness the perpetrators committing fraud.)

8. Which of the following control procedures is most likely to deter lapping?
   a. encryption (Incorrect. Encryption is used to code data in transit so it cannot be read unless it is decoded. It does not stop employees from lapping accounts receivable payments.)
   b. continual update of the access control matrix (Incorrect. The access control matrix specifies what computer functions employees can perform and what data they can access with a computer. It does not stop employees from lapping accounts receivable payments.)
   c. background check on employees (Incorrect. A background check can help screen out dishonest job applicants, but it does not stop employees from lapping accounts receivable payments.)
   ▶ **d.** periodic rotation of duties (Correct. Lapping requires a constant and ongoing cover-up to hide the stolen funds. Rotating duties such that the perpetrator does not have access to the necessary accounting records will most likely result in the fraud's discovery.)

9. Which of the following is the most important, basic, and effective control to deter fraud?
   a. enforced vacations (Incorrect. Enforced vacations will prevent or deter some, but not all, fraud schemes.)
   b. logical access control (Incorrect. Logical access controls will prevent or deter some, but not all, fraud schemes.)
   ▶ **c.** segregation of duties (Correct. Segregating duties among different employees is the most effective control for the largest number of fraud schemes, because it makes it difficult for any single employee to both commit and conceal a fraud.)
   d. virus protection controls (Incorrect. Virus protection controls will help prevent some computer-related abuses, but they are unlikely to deter much fraud.)

10. Once fraud has occurred, which of the following will reduce fraud losses? (Select all correct answers.)
   ▶ **a.** insurance (Correct. The right insurance will pay for all or a portion of fraud losses.)
   ▶ **b.** regular backup of data and programs (Correct. Regular backup helps the injured party recover lost or damaged data and programs.)
   ▶ **c.** contingency plan (Correct. A contingency plan helps the injured party restart operations on a timely basis.)
   d. segregation of duties (Incorrect. Segregation of duties is an effective method of deterring fraud but does not help a company recover from fraud once it occurs.)