# CHAPTER 5

**COMPUTER FRAUD**

**SUGGESTED ANSWERS TO 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?**

The statement is ironic because employees represent both the greatest control strength and the greatest control weakness. Honest, skilled employees are the most effective fraud deterrent. However, when fraud occurs, it often involves an employee in a position of trust. As many as 90% of computer frauds are insider jobs by employees.

Employers can do the following to maintain the integrity of their employees. (NOTE: Answers are introduced in this chapter and covered in more depth in Chapter 7)

* Human Resource Policies. Implement human resource policies for hiring, compensating, evaluating, counseling, promoting, and discharging employees that send messages about the required level of ethical behavior and integrity
* Hiring and Firing Practices: Effective hiring and firing practices include:
  + Screen potential employees using a thorough background checks and written tests that evaluate integrity.
  + Remove fired employees from all sensitive jobs and deny them access to the computer system to avoid sabotage.
* Managing Disgruntled Employees: Some employees who commit a fraud are disgruntled and they are seeking revenge or "justice" for some wrong that they perceive has been done to them. Companies should have procedures for identifying these individuals and helping them resolve their feelings or removing them from jobs that allow them access to the system. One way to avoid disgruntled employees is to provide grievance channels that allow employees to talk to someone outside the normal chain of command about their grievances.
* Culture. Create an organizational culture that stresses integrity and commitment to both ethical values and competence
* Management Style. Adopt an organizational structure, management philosophy, operating style, and appetite for risk that minimizes the likelihood of fraud
* Employee Training: Employees should be trained in appropriate behavior, which is reinforced by the corporate culture. Employees should be taught fraud awareness, security measures, ethical considerations, and punishment for unethical behavior.

**5.2** **You are the president of a multinational company where 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?**

In a kiting scheme, 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.</para></listitem>

Kiting can be detected by analyzing all interbank transfers. Since the scheme requires constant transferring of funds, the number of interbank transfers will usually increase significantly. This increase is a red flag that should alert the auditors to begin an investigation.

When the employee confesses, the company should immediately investigate the fraud and determine the actual losses. Employees often "underconfess" the amount they have taken. When the investigation is complete, the company should determine what controls could be added to the system to deter similar frauds and to detect them if they do occur.

Employers should consider the following issues before pressing charges:

* How will prosecuting the case impact the future success of the business?
* What effect will adverse publicity have upon the company's well being? Can the publicity increase the incidence of fraud by exposing company weaknesses?
* What social responsibility does the company have to press charges?
* Does the evidence ensure a conviction?
* If charges are not made, what message does that send to other employees?
* Will not exposing the crime subject the company to civil liabilities?

**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?**

The old saying "where there is a will, there is a way" applies to committing fraud and to breaking into a computer system. It is possible to institute sufficient controls in a system so that it is very difficult to perpetrate the fraud or break into the computer system, but most experts would agree that it just isn't possible to design a system that is 100% secure from every threat. There is bound to be someone who will think of a way of breaking into the system that designers did not anticipate and did not control against.

If there were a way to make a foolproof system, it would be highly likely that it would be too cost prohibitive to employ.

Though internal controls can't eliminate all system threats, controls can:

* Reduce threats caused by employee negligence or error. Such threats are often more financially devastating than intentional acts.
* Significantly reduce the opportunities, and therefore the likelihood, that someone can break into the system or commit a fraud.

**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.**

This problem has no clear answer. By strict definition, the actions of Logisticon in halting the software represented trespassing and an invasion of privacy. Some states recognize trespassing as a breach of the peace, thereby making Logisticon's actions illegal.

However, according to contract law, a secured party can repossess collateral if the contract has been violated and repossession can occur without a breach of the peace.

The value of this discussion question is not in disseminating a “right answer” but in encouraging students to examine both sides of an issue with no clear answer. In most classes, some students will feel strongly about each side and many will sit on the fence and not know.

**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.**

**<para>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?**

Answers will vary. Students should consider the following conflicting concepts:

*Software licensing encourages the development of new ideas by protecting the efforts of businesses seeking to develop new software products that will provide them with a profit and/or a competitive advantage in the marketplace.* This point is supported by the following ideas:

* The prospect of a financial reward is the primary incentive for companies to expend the time and money to develop new technologies.
* If businesses were unable to protect their investment by licensing the software to others, it would be much more difficult for them to receive a reward for their efforts in the research and development of computer software.
* Economic systems without such incentives are much more likely to fail in developing new products to meet consumer needs.

*The only way to foster new ideas is to make information and software available to all people.* The most creative ideas are developed when individuals are free to use all available resources (such as software and information).

Many security experts and systems consultants view proper ethical teaching as an important solution to most security problems. However, no single approach is a complete solution to the problem of computer fraud and abuse. Proper ethical teachings can reduce but not eliminate the incidents of fraud.

Though no security system is impenetrable, system security measures can significantly reduce the opportunity for damages from both intentional and unintentional threats by employees. Controls can also make the cost (in time and resources) greater than the benefit to the potential perpetrator.

Ultimately, the reduction in security measures will increase opportunities for fraud. If the perpetrator has sufficient motive and is able to rationalize his dishonest acts, increased opportunity will probably lead to an increase in computer crimes.

**SUGGESTED ANSWERS TO THE PROBLEMS**

**5.1** **You were asked to investigate extremely high, unexplained merchandise shortages at a department store chain. Classify each of the five situations as a fraudulent act, an indicator of fraud, or an event unrelated to the investigation. Justify your answers.** Adapted from the CIA Examination

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.**

This is an indication of possible fraud. This conflict of interest is a fraud symptom that alerts auditors to the possibility of fraud. The receiving department supervisor’s ownership of the boutique may also be in conflict with the organization's code of ethics and conduct.

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.**

This is a fraudulent act because there is a theft accompanied by:

1. A *false statement, representation, or disclosure* (signing the receiving report)
2. A *material fact*</emphasis>, (the signature on the receiving report causes the company to act; that is, to pay the vendor)</para></listitem>
3. An *intent to deceive* (The supervisory deceives the company so that it will pay for the goods he steals)
4. A *justifiable reliance* (The store relies on the misrepresentation to pay the vendor)
5. An< *injury or loss* (The supervisor steals goods the store pays for)

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.**

This is a weakness in internal control. Sales personnel should count the goods received and match their counts to the accompanying receiving report. Failure to do so allows the theft to go undetected.

d. **Accounts Payable paid vendors for the total quantity shown on the receiving report.**

Proper internal control says that Accounts Payable should match the vendor’s invoice to both the purchase order and the receiving report. Because this matching would not detect the theft, some may argue that this is a weakness in internal control. However, the weakness lies in the sales department not counting (independently verifying) the receiving department count. (see parts c and e)

Therefore, accounts payable paying the vendor the total amount due is not a fraud or an indicator of fraud or an internal control weakness. It has no bearing on the investigation.

e. **Based on the receiving department supervisor’s instructions, quantities on the receiving reports were not counted by sales personnel.**

This is the same internal control weakness described in part c. The receiving department supervisor gave those instructions to facilitate his or her fraud

In addition, sales personnel’s following the receiving department supervisor’s instructions is another internal control weakness. The receiving department supervisor should not have control over or manage sales personnel. There should be a clear-cut segregation of duties between sales and receiving.

The receiving department supervisor having control over or supervising sales personnel is also a fraud symptom that should alert auditors to the possibility of fraud.

**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.** Adapted from the CIA Examination.

1. **Define fraud, fraud deterrence, fraud detection, and fraud investigation.**

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*</emphasis>, which is something that induces a person to act</para></listitem>
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

Fraud can be perpetrated for the benefit of or to the detriment of the organization and by persons outside as well as inside the organization.

Fraud deterrence is the actions taken to discourage the perpetration of fraud.

Fraud detection is using any and all means, including fraud symptoms (also called red flags of fraud) to determine whether fraud is taking place

Fraud investigation is performing the procedures needed to determine the nature and amount of a fraud that has occurred.

1. **List four personal (as opposed to organizational) fraud symptoms, or red-flags, that indicate the possibility of fraud.</para></listitem> Do not confine your answer to this example.**

* High personal debts or significant financial or investment losses.
* Expensive lifestyle; living beyond your means.
* Extensive gambling, alcohol, or drug problems.
* Significant personal or family problems.
* Rewriting records, under the guise of neatness.
* Refusing to leave custody of records during the day.
* Extensive overtime.
* Skipping vacations.
* Questionable background and references.
* Feeling that pay is not commensurate with responsibilities.
* Strong desire to beat the system.
* Regular borrowing from fellow employees.
* Personal checks returned for insufficient funds.
* Collectors and creditors appearing at the place of business.
* Placing unauthorized IOUs in petty cash funds.
* Inclination toward covering up inefficiencies or "plugging" figures.
* Pronounced criticism of others.
* Association with questionable characters.
* Annoyance with reasonable questions; replying to questions with unreasonable answers.
* Unusually large bank balance.
* Bragging about exploits.
* Carrying unusually large amounts of cash.

1. **List two procedures you could follow to uncover John’s fraudulent behavior.**

1. Inspecting the documentation supporting the release of a check to a vendor. There would be no receiving report. There might be a fake PO (not clear from the problem if John documents the fake purchase or if it is just oral).

2. Tracing all payments back to the supporting documentation. The receiving department would have no record of the receipt of the goods. The purchasing department would have no record of having ordered the materials or of having such materials requested.

**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.**

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

| Type of Fraud | Explanation | Identification and Description of Protection Methods |
| --- | --- | --- |
| Input manipulation | This requires the least amount of technical skill and little knowledge of how the computers operate.  Input data are improperly altered or revised without authorization. For example, payroll time sheets can be altered to pay overtime or an extra salary. | Documentation and Authorization   * Data input format authorized and properly documented. * Control over blank documents. * Comprehensive editing * Control source of data   Programmed Terminal/User protection   * Programs that only accept inputs from certain designated users, locations, terminals, and/or times of the day. |
| Program alteration | Program alteration requires programming skills and knowledge of the program.  Program coding is revised for fraudulent purposes. For example:   * Ignore certain transactions such as overdrafts against the programmers' account * Grant excessive discounts to specified customers | Programmers should not be allowed to make changes to actual production source programs and data files.  Segregation of Duties   * Programmers should not have access to production programs or data files.   Periodic Comparisons   * Internal Audit or an independent group should periodically process actual data, and compare the output with output from normal operations. Differences indicate unauthorized program changes. * Periodic comparisons of on-line programs to off-line backup copies to detect changes. * Independent file librarian function who controls custody/access to programs |

|  |  |  |
| --- | --- | --- |
| File alteration | Defrauder revises specific data or manipulates data files. For example:   * Using program instructions to fraudulently change an employee’s pay rate in the payroll master file * Transferring balances among dormant accounts to conceal improper withdrawals of funds. | Restrict Access to Equipment/Files   * Restrict access to computer center. * Programmers and analysts should not have direct access to production data files. * Have a librarian maintain production data files in a library. * Restrict computer operator access to applications documentation, except where needed to perform their duties, to minimize their ability to modify programs and data files. |
| Data theft | Smuggling out data on:   * Hard copies of reports/files. * Magnetic devices in briefcases, employees' pockets, etc.   Tap or intercept data transmitted by data communication lines | Electronic sensitization of all library materials to detect unauthorized removals.  Encrypt sensitive data transmissions. |
| Sabotage | Physical destruction of hardware or software. | Terminated employees immediately denied access to all computer equipment and information to prevent them from destroying or altering equipment or files.  Maintain backup files at secure off-site locations. |
| Theft of Computer Time | Unauthorized use of a company's computer for personal or outside business activities. This can result in the computer being fully utilized and lead to unnecessary computer capacity upgrades. | Assigning blocks of time to processing jobs and using the operating system to block out the user once the allocated time is exhausted. Any additional time would require special authorization. |

**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.** Adapted from the CMA Examination.

1. **Identify two company pressures that would increase the likelihood of fraudulent financial reporting.**

* Sudden decreases in revenue or market share
* Financial pressure from bonus plans that depend on short-term economic performance
* Intense pressure to meet/exceed earnings expectations or improve reported performance
* Significant cash flow problems; unusual difficulty collecting receivables or paying payables
* <entry valign="top"><para>Heavy losses, high or undiversified risk, high dependence on debt, or unduly restrictive debt covenants</para></entry></row>
* Heavy dependence on new or unproven product lines
* Severe inventory obsolescence or excessive inventory buildup
* Highly unfavorable economic conditions (inflation, recession)
* Litigation, especially management vs. shareholders
* Impending business failure or bankruptcy
* Problems with regulatory agencies
* Unusual spikes in interest rates
* Poor or deteriorating financial position

1. **Identify three corporate opportunities that make fraud easier to commit and detection less likely.**

* Weak or nonexistent internal controls
* Failure to enforce/monitor internal controls
* Management not involved in control system or overriding controls
* Unusual or complex transactions such as the consolidation of two companies
* Accounting estimates requiring significant subjective judgment by management
* Managerial carelessness, inattention to details
* Dominant and unchallenged management
* Ineffective oversight by board of directors
* Nonexistent or ineffective internal auditing staff
* Insufficient separation of authorization, custody, and record-keeping duties
* Inadequate supervision or too much trust in key employees
* Unclear lines of authority
* Lack of proper authorization procedures
* No independent checks on performance or infrequent third-party reviews
* Inadequate documents and records
* Inadequate system for safeguarding assets
* No physical or logical security system
* No audit trails

The list show here can be augmented by the items in Table 5-4 listed in the Other Factors column.

1. **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**

* + Specific industry trends such as overall demand for the industry's products, economic events affecting the industry, and whether the industry is expanding or declining.
  + Whether the industry is currently in a state of transition affecting management's ability to control company operations.

**• The company’s business environment**

* + The continued viability of the company's products in the marketplace.
  + Sensitivity of the company's operations and profits to economic and political factors.

**• The company’s legal and regulatory environment**

* The status of the company's business licenses or agreements, especially in light of the company's record of compliance with regulatory requirements.
* The existence of significant litigation.

1. **What can top management do to reduce the possibility of fraudulent financial reporting?**

* Set the proper tone to establish a corporate environment contributing to the integrity of the financial reporting process.
* Identify and understand the factors that can lead to fraudulent financial reporting.
* Assess the risk of fraudulent financial reporting that these factors can cause within the company.
* Design and implement internal controls that provide reasonable assurance that fraudulent financial reporting is prevented, such as establishing an Internal Audit Department that reports to the Audit Committee of the Board of Directors.
* Enforce the internal controls

NOTE: Most fraudulent financial reporting fraud is perpetrated by top management, often by overriding internal controls. While some of the above controls in part d are more likely to prevent misappropriation of assets, they can still be useful for preventing or deterring fraudulent financial reporting.

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

* 1. **Due to abnormal inventory shrinkage in the audiovisual department at a retail chain store, internal auditors conducted an in-depth audit of the department. They learned that a 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.**

While collusion is difficult to prevent, the store could improve its control system by:

* Implementing job rotation so that the same employees are not always performing the same duties.
* Separating the payment for expensive items from the pickup of these items at a separate location.
* Videotaping the cashiers and periodically reviewing the tapes looking for fraud and collusion. More specifically, they could determine whether or not a sale was rung up.
* Tagging each item with an electronic tag that can only be deactivated by scanning it into a cash register. This may cost more (and be more hassle) than it is worth.

b. **During an unannounced audit, auditors discovered a payroll fraud when they distributed paychecks instead of department supervisors. 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.**

The payroll fraud could be prevented with better internal controls, including:

* Separation of duties. A supervisor with the authority to approve time cards should not be allowed to distribute paychecks. An individual with no other payroll-related duties should distribute checks.
* Periodic floor checks for employees on the payroll.
* Electronically depositing paychecks in employee accounts, thereby eliminating their physical distribution.

1. **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 the supplier’s.</para></listitem></orderedlist><source>**

The accounts payable fraud could be prevented with better internal controls, including:

* Implement and enforce a policy that prohibits the payment of invoices based on copies of supporting documents.
* Require all vendors to submit a numbered electronic invoice. The computer could match the invoice to the supporting documents, automatically looking for duplicate invoices or duplicate supporting documents.
* Make all payments to the vendor’s bank account using electronic funds transfers (EFT).
* Require specific authorization if a situation arises where payment on the basis of copies of supporting documents is necessary.

**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.** Adapted from the CIA Examination

a. **List the fraud symptoms that should have aroused the auditor’s suspicion.**

* Failure to follow the established policy of requiring sealed bids to dispose of vehicles being salvaged.
* Management's vigorous justification for departing from established policy.
* Repairing vehicles before they were sold for salvage.

b. **What audit procedures would show that fraud had in fact occurred.**

* Review thoroughly the sales documentation that identifies the people who bought the vehicles at negotiated prices, including comparing the buyers to a list of company employees.
* Determine whether the company received fair value when the vehicles were sold. This could be accomplished by one or more of the following:
  + Compare the sales price to "blue book" prices or to proceeds of sales of comparable vehicles made based on sealed bids
  + Locate the actual vehicles and have their values appraised.
* Review maintenance records for salvaged vehicles looking for recent charges that indicate the vehicle might have been fixed before it was sold..

**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.**

**What type of embezzlement scheme does this appear to be, and how does that scheme operate?** Adapted from the CIA Examination

The circumstances are symptomatic of lapping, which is a common form of embezzlement by lower-level employees in positions that handle cash receipts.

In a lapping scheme, the perpetrator steals cash, such as a payment on accounts receivable by customer A. Funds received at a later date from customer B are used to pay off customer A's balance. Even later, funds from customer C are used to pay off B, and so forth. Since the time between the theft of cash and the subsequent recording of a payment is usually short the theft can be effectively hidden. However, the cover-up must continue indefinitely unless the money is replaced, since the theft would be uncovered if the scheme is stopped.

**5.8** AICPA adapted

**a. Prepare a schedule showing how much the cashier embezzled.**

Balance per Books, November 30 18,901.62

Add: Outstanding Checks

Number Amount

* 1. 116.25

183 150.00

284 253.25

1. 190.71
2. 206.80

8632 145.28

1,062.29

Add Bank credit 100.00

Total additions to balance per books 1,162.29

Subtract: Deposits in transit (3,794.41)

Balance per bank 16,269.50

Balance per bank (according to the bank) 15,550.00

Amount of theft 719.50

1. **Describe how the cashier attempted to hide the theft.**

The cashier used several methods to attempt to hide the theft:

1. The cashier did not include 3 outstanding checks in the reconciliation:
   * + No. 62 – 116.25
     + No. 183 – 150.00
     + No. 284 – 253.25

519.50

1. Error in totaling (footing) the outstanding checks. The total of the checks listed on the reconciliation is actually 542.79 not 442.79.
2. Deducting instead of adding the bank credit (100) after the balance per bank is calculated.
3. The total is 719.50 (519.50 + 100 + 100)

**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 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.**

1. **How does the accountant fit the profile of a fraudster?**

The accountant fit the fraud profile in that he was

* Young
* Possessed knowledge, experience, and skills
* A dedicated, loyal and trusted employee
* An honest, valued, and respected members of the community.</para>

**How does he not fit the profile?**

He invested a portion of his ill-gotten gains instead of spending it like the typical fraudster.

1. **What fraud scheme did he use to perpetrate his fraud?**

The accountant prepared fake invoices from legitimate contractors, wrote checks to pay the invoices, and then deposited the checks into a bank account he had opened under the name of one of the companies

1. **What controls could have prevented his fraud?**

All the accountant had to do was create fictitious invoices, as he had custody of checks before and after they were signed and he had the authorization to approve payments and sign checks. The fraud could have been prevented by separating accounting duties

* + Restrict access (custody) to company checks and the check signing machine to someone that does not have recording or authorization responsibilities.
  + Do not permit the person that prepares the check to disburse the check (mail it to the recipient, etc)
  + Have someone familiar with the contractors authorize payments – someone who would have known that the goods and services were never ordered or performed. This should be someone other than the preparer of the check; that is, someone without custody or recording functions.
  + Require that someone other than the people with custody and authorization responsibilities record the payments.

1. **What controls could have detected his fraud?**
   * A bank reconciliation prepared by someone else. An Olympic Committee official should have reviewed bank statements and cancelled checks.
   * Periodic confirmations of invoices with vendors.
   * Analytical reviews designed to detect an abnormal increase in expenses

**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.** Adapted from the CMA Examination

1. **Discuss three ways Lexsteel is exposed to fraud and recommend improvements to correct these weaknesses.**

|  |  |
| --- | --- |
| **Weakness** | **Recommendation** |
| There are no controls over branch managers issuing emergency purchase orders. The branch manager can decide when an "emergency" exists and she is permitted to choose a vendor subjectively. This opens the door to fraud and errors. | A procedure for expediting emergency orders should be developed for the purchasing department that contains appropriate controls. |
| Invoices are paid without agreeing them to purchase orders and receiving reports. Making payments without this comparison could result in payments for goods that were not ordered or that were not received. | Require proper authorizations and verification documentation (agreement of invoices, purchase orders, and receiving report) prior to payment. |
| There is no supporting documentation attached to the checks when they are forwarded to the treasurer for payment. | Checks sent to the Treasurer for signature should be accompanied by all original supporting documents (invoice, purchase order and receiving report) so the Treasurer can verify that the payment is valid and appropriate. |
| The supporting documents are not canceled after payment, allowing the possibility of a second payment of the same invoice. | The invoices and other supporting documents should be canceled after the checks are signed. |

1. **Describe three ways management information could be distorted and recommend improvements to correct these weaknesses.**

|  |  |
| --- | --- |
| **Weakness** | **Recommendation** |
| 1. Cash balances are distorted when checks are drawn when due but are not mailed until sufficient cash is available. Cash management will also be affected by inaccurate due dates, lack of procedures for taking vendor discounts, and inaccurate information for EOQ calculations. | Checks should be drawn only when cash is available and mailed immediately. Procedures should be established for taking advantage of vendor discounts when appropriate. |
| 2. Accounts payable information is distorted by drawing checks and then holding them for future payment, by entering invoices without supporting documentation, and by inaccurate receiving documentation. | Invoices should not be entered into the system until matched with supporting documents, and receiving documents should be matched against original purchase orders. |
| 3. Inventory balances are likely to be misstated because of no physical counts. | Periodically count inventory and reconcile the counts to inventory records. |
| 4. Calculating due dates by hand and using the invoice date instead of the date the goods are received could lead to inaccurate due dates that could damage vendor relations. | The system should calculate due dates from the date goods are received, not based on the date they are invoiced. |
| The lack of control over emergency orders could distort inventory balances and cause duplicate purchases. | Implement appropriate controls to prevent duplicate purchases, such as immediate entry of emergency orders so the system has a record of them. |

1. **Identify and explain three strengths in Lexsteel’s procedures**

* The company has a centralized EDP system and database in place. This eliminates duplication of effort and data redundancy while improving data integrity, efficiency, productivity, and timely management information.
* Most purchase orders are issued by the centralized purchasing department from computerized production orders or bills of material. This limits overstocking of materials inventory and employs the specialized expertise in the purchasing function.
* The functions of purchasing, production control, accounts payable, and cash disbursements are centralized at the corporate headquarters. This improves management control and avoids a duplication of efforts. The separated departments help maintain internal control by the segregation of duties for authorization, payment, and coding.

**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.**

There should be 5 or 6 of these articles on the Journal of Accountancy web site. No solution is provided here as the solutions are at the end of each article. Most questions are thought provoking and the answers informative.

**5.12 Explore the Anti-Fraud and Forensic Accounting portion of the AICPA Web site (http://www.aicpa.org/INTERESTAREAS/FORENSICANDVALUATION/RESOURCES/Pages/default.aspx), and write a two-page report on the three most interesting things you found on the site.**

Solutions will vary. The purpose of the problem is to expose the students to the website contents. The author grades the report on a pass/fail basis based on whether the student gave an honest effort in exploring the site and writing up the report.

**SUGGESTED ANSWERS TO THE CASES**

**5.1** **1. How does Miller fit the profile of the average fraud perpetrator?**

* Like many fraud perpetrators, David Miller was not much different than the general public in terms of education, values, religion, marriage, and psychological makeup.
* Like Miller, many white-collar criminals are regarded as ideal employees until they are caught. Like him, they are dedicated and work long hours.
* He was well respected, occupied a position of trust, and was viewed as an honest, upstanding citizen.
* Most fraud perpetrators spend all that they steal. Few invest it. Miller was no exception.

**How does he differ?**

* + - Miller was not disgruntled and unhappy, nor was he seeking to get even with his employer.
* Though David Miller was never convicted of fraud, he was involved in a number of schemes. In contrast, most fraud perpetrators are first time offenders.

**How did these characteristics make him difficult to detect?**

It is often difficult to detect fraud perpetrators because they possess few characteristics that distinguish them from the public. Most white-collar criminals are talented, intelligent, and well educated. Many are regarded as the ideal employee that occupies a position of trust, is dedicated, and works hard for the company. They are otherwise honest, upstanding citizens that have usually never committed any other criminal offense.

1. **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?**

There are three elements to the opportunity triangle:

1. The perpetrator must **commit** the fraud by stealing something of value, such as cash, or by intentionally reporting misleading financial information.

Miller was able to steal cash by undermining the internal controls that required two signatures on checks. He asked company officials to sign checks before they went on vacation "just in case" the company needed to disburse funds while they were gone.

1. To avoid detection, the perpetrator must **conceal** the crime. 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.</para>

To conceal the theft, Miller retrieved the canceled check from the bank reconciliation and destroyed it. The amount stolen was then charged to an expense account of one of the units to balance the company's books. Miller was able to work himself into a position of trust and influence. Because he occupied this position his actions were not questioned and he was able to subvert some of the internal controls intended to prevent the type of actions he was able to take.

1. The perpetrator must **convert** the stolen asset into some form usable by the perpetrator if the theft is of an asset other than cash. For example, stolen inventory and equipment must be sold or otherwise converted into cash. In financial statement fraud, the conversion is more indirect, such as in undeserved pay raises, promotions, more stock options, etc.

Miller was able to convert the check to cash by writing himself checks and depositing them in his personal account.

1. **What pressures motivated Miller to embezzle? How did Miller rationalize his actions?**

Motivation. After David Miller had undergone therapy, he believed his problem with compulsive embezzlement was an illness, just like alcoholism or compulsive gambling. He stated that the illness was driven by a subconscious need to be admired and liked by others. He thought that by spending all of that money others would like him. Ironically, he was universally well liked and admired at each job and it had nothing to do with money. In fact, one associate at Associated was so surprised at the news of the thefts that he said that it was like finding out that your brother was an ax murderer. Miller also claimed that he is not a bad person, that he never intended to hurt anyone, but once he got started he just could not stop.

Rationalization. The case does not specify what Miller's rationalizations were. He may, in fact, have had a number of different rationalizations. The case suggests that he "needed it" to pay back the money he stole from previous employers. He was always "just borrowing" the money and intended to pay it back. Miller may have also been convinced that he would never be prosecuted for his crimes. Many of the rationalizations listed in the text are also possibilities.

1. **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?**

Miller's life seemed to be centered on financial gain and the accumulation of material goods or, as the quote says, "toys." Such gain, he felt, would lead to prestige and recognition among his friends in the business community.

The wealth and extravagant spending in relation to Miller's salary was the primary red flag that most companies never questioned. Consider that on his $130,000 a year salary he was able to afford two Mercedes-Benz sedans; a lavish suburban house; 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.

1. **Why do companies hesitate to prosecute white-collar criminals?**

* Negative publicity. Companies are reluctant to prosecute fraud because of the financial damage that could result from negative publicity. A highly visible fraud is a public relations disaster. The company could lose a lot of business due to the adverse publicity.
* Exposes system weaknesses. Reporting and prosecuting fraud may reveal vulnerabilities in a company's system. This could attract even more acts of fraud.
* Concern for the perpetrator's family. If an employee is willing to make retribution, companies may not press charges to protect the employee’s family and reputation.
* Society is more concerned with "real" crime. Political considerations motivate enforcement officials to focus their resources on more violent and visible crimes such as rape, murder, and robbery. Some people see fraud as an internal problem and not as a serious crime that demands prosecution.
* Unclear definition of computer fraud. One reason computer fraud is not prosecuted more is that the definition of computer fraud is so vague. As a result, no one really knows how much it really costs and there isn't as much motivation to go after computer fraud cases.
* Prosecution difficulties. It is difficult, costly, and time consuming to investigate fraud. It is even harder to prove. As a result, it can be hard to prosecute fraud cases successfully and get convictions.
* Lack of expertise. Many law enforcement officers, lawyers, and judges lack the skills necessary to investigate, prosecute and evaluate fraud, especially computer fraud.
* Light sentences. When fraud cases are prosecuted and a conviction is obtained, the sentences received are sometimes very light. This discourages prosecution.

**What are the consequences of not prosecuting?**

When fraud is not prosecuted, it sends a message to employees and to the public that enforcing laws is not important to the company. A reputation for being "soft" on fraud may result in the companies becoming increasingly vulnerable to additional fraud.

Failure to report and prosecute a fraud also means that the perpetrator goes free and can repeat his or her actions at another company, as David Miller did. If the perpetrator does not have to pay the consequences of his actions, she is more likely to repeat them because she "got away with it" and was not punished.

**How could law enforcement officials encourage more prosecution?**

To encourage more fraud prosecution, law enforcement officials must take actions to solve each of the problems mentioned above. In addition, they must encourage more effective reporting of such crimes. The public should be educated to recognize and report fraud as a serious offense.

1. **What could the victimized companies have done to prevent Miller’s embezzlement?**

Not much is said in the case about how Miller committed many of the frauds. In each of the frauds, it is likely that the theft of cash could have been prevented by tighter controls over access to cash and blank checks and to the means of writing and signing checks. Some could have been prevented or at least detected by better control over monthly bank statements and their reconciliation.

In retrospect, Miller was given too much trust and authority and that led to a breakdown of internal controls. However, companies have to trust their top level employees, such as the CFO. Even though this trust is necessary, a greater separation of duties and more supervision of Miller's work would have made it more difficult for him to perpetrate the frauds.

In all but the first fraud, a more thorough background check of Miller may have revealed his past fraudulent activities and the company could have avoided the problems that arose after he was hired.

**5.2**

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.**

There are many ways to perpetrate fraud. Some of the more easily recognizable ways are the following:

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Ways to Commit Fraud | 1. Indication Something is Wrong | 1. Weaknesses Allowing Fraud | 1. Controls to Minimize Fraud |
| Receivables employees could  **1. Steal cash receipts by lapping**. Payments are made by sending in a coupon and a $25 payment. Any of the three receivables employees could pocket the payment, save the coupon, put a subsequent payment with the “saved” coupon, and run the payment through the system.  **2. Steal cash receipts and allow accounts to be written off.**  It is difficult to collect from some customers because they only have a PO Box address and do not have a phone. Receivables employees could steal cash receipts from these customers each month and allow the accounts to be written off. | Lag between customer payments and the posting of the payments.  If the appropriate controls are in place, customers listed on the pre-listing of cash would not match the names on the bank deposit or those credited for payment on the same day.  Increase in the number of accounts written off.  If the perpetrator did not get greedy, this might not be easily detected since 35-40% of accounts are defaulted on already. Even a slow steady increase in the number of defaulting-due-to-fraud customers might not be easily detected.  Customer complaints. | No separation of duties between cash receipts, posting receivables, and preparing bank deposit.  No independent checks on performance.  No monthly statements.  No work or family secondary addresses and phone numbers. | Separate custody of cash (opening cash receipts) from recording (posting payments to receivables records).  Have 2 people open all cash receipts and prepare a pre-listing of cash receipts.  Compare customer names on the pre-listing to customer names on the receivables posting and the bank deposits.  Send monthly statements.  Bank financing, credit card payments, or automatic withdrawals from checking or savings accounts.  Involve sales agent in tracking down customers that cannot be reached before writing them off. |
| Sales agents could  **3. Falsify sales to reach an incentive level.** Agents can book fictitious contracts, pay with a money order, send correspondence to a PO Box they control, and let the contract default with no more payments. An agent selling 81 contracts can break even by falsifying 20 sales. ($250 down - $125 commission = $2500 cost. $2500 bonus / $125 cost = 20 contracts)  An agent selling 151 contracts can break even on 50 sales.  **4. Defer yearend sales**  Sales that will not qualify for a new incentive level could be held and put in next year’s sales. | Abnormally large number of sales just before year end, combined with agent barely reaching an incentive level  Increase in the number of accounts written off, especially for agents barely reaching an incentive level.  Customer complaints. | Few and steep incentive levels that motivate unwanted behavior.  Inability to effectively follow -up on collections (addresses and phone numbers). See #2  Customer credit not checked.  Address and phone numbers not verified. | More graduated incentives that do not provide such strong incentives.  Base sales incentives on customer collections, not on original sales.  Analysis of December sales for sales agents who barely reach an incentive level, especially on last day or two of the year.  Analysis of default rates per sales agent for those who barely reach an incentive level, especially on last day or two of the year.  Check customer credit, addresses, and phone numbers. |
| Sales agents could  **5. Steal part of a customer’s payment.** An agent could send in $250 of a $900 sale and pocket the difference. The agent could then make payments for a while and let the contract lapse. Not a big risk as virtually all customers choose financing. | Decrease in the number of customers paying the $900, which will be hard to detect since, so few use that option.  Customer complaints.  Do most customers finance because agents are already doing this? | Photographers don’t verify if customers are current before a sitting, so $250 is as good as $900.  Customers don’t sign, initial photography plan order forms | Require photographers to verify that customers are current before each sitting.  Require customers to sign photography plan order forms and initial the amount paid and financing arrangements. |
| **6.** **Management can bleed the company or engage in non-arms-length transactions with owners.**  Both owners are paying their spouses exorbitant salaries and have extravagant expense accounts and perks.  Buildings, equipment, and furnishings could be purchased from/by the owners at inflated or deflated prices.  This is not fraud, as long as what occurs is reported properly for tax purposes and financial statement given to the bank properly disclose any needed items.  It is fraud if one owner authorizes payments, perks, or non-arms length transactions to himself or his family that the other partner is not aware of. | Company perpetually short of cash  Expense accounts and perks unusually high  Inflated salary expenses  Abnormally high prices for the assets purchased. | No apparent controls to prevent one owner from defrauding the other owner. | Require all payments, perks, or non-arms-length transactions to an owner to be approved by the other owner.  An external, independent audit.  Full disclosure of all payments, perks, or non-arms-length transactions to a qualified tax preparer to ensure full compliance with applicable tax laws. |
| **7. Customers can use photo coupons without completing their payments.** There are no controls to prevent customers who have stopped paying on their note from taking their coupon to their photographer for a sitting and getting their picture taken. | Increase in the number of sittings per current customer.  Coupons submitted for customers that have been written off.  Photographer complaints. | Photographers are not required to verify if customers are current before a sitting.  Customer given all their coupons at initial purchase. | Set up automatic withdrawals from checking accounts or automatic charges to credit cards.  Require photographers to verify that customers are current before each sitting.  Keep a list of customer payments; do not pay for customers that are no longer current.  Do credit checks on all potential customers. |
| **8. Photographers could send in unused coupons or fake coupons.** Photographers have exclusive rights to customers in their specified areas. They could encourage customers to leave the coupons at the photo studio so they are not lost or misplaced. If a customer did not come in during the 6-month period, the photographer could submit his unused coupon.  If the coupon book is not left for safekeeping, the photographer could scan a coupon, change the name to a customer who did not use their coupon, print it, and send it in. | Abnormally high rate of customers using their coupons  Coupons that do not look authentic.  Customer complaints. | Photographers given an exclusive area.  Customers not signing coupons or otherwise verifying they had a sitting.  Photographers could send in coupons for non-current customers as they are not required to verify if customers are current before a sitting. Nor does the company verify that submitted coupons are for a current customer. | Pre-number coupons.  Have a code on the coupon that the photographer has to call in to the company (or enter on a website) before authorization is granted to take the photo.  For each photographer, analyze what percent of customers use their coupons looking for abnormally high usage rates.  Require photographers to verify that customers are current before each sitting.  Do not pay for customers that are no longer current. |
| **9. Heirloom can defraud the bank by misstating the maximum amount Heirloom can borrow.**  Notes payable are in the borrowing base until they are 60 days overdue. To maximize that base, Heirloom could lap customer payments. They could take a monthly payment on a current account and apply it to an account that is just about to go 60 days overdue. The inflated list could be used to support a higher than justified loan. | Abnormally high number of customers 30-60 days overdue. | Bank does not verify data from Heirloom. | Analysis of the list, such as   * An increase in the number or percentage of accounts on the list submitted to the bank with no comparable increase in sales. * Comparison of monthly lists to see if the same names appear month after month. |
| **10. Heirloom can defraud the bank by misstating its financial statements in many ways.** For example:  - Understating its allowance and bad debt expense (not writing off uncollectible receivables and low-balling the bad debt expense).  - Creating fictitious sales and notes receivables.  - Intentionally under or over stating the sales commission estimates. | Unusual decrease in the allowance or bad debt amounts.  Sales increase without a comparable increase in receivables; inventory; cost of goods sold; and applicable expenses such as photographer and album expenses, embossing and shipping, and commissions.  Sales commissions out of line with those of the industry or past years. | There is no mention of an external audit by independent CPAs. | An external, independent audit.  Financial statement analysis, such as   * Analysis of bad debt to sales and allowance to sales ratios to see if they are below those of past years and those of comparable customers in the same industry. * Analysis of sales ratios, comparing sales to receivables; inventory; gross margin, cost of goods sold; and applicable expenses such as album and photographer expenses, embossing and shipping, and commissions. |