Anatomy of computer accounting frauds

A. Seetharaman, M. Senthilvelmurugan and Rajan Periyanayagam
Faculty of Management, Multimedia University, Malaysia

Keywords *Fraud, Corruption, Financial reporting, Whistleblowing, Internal control, Corporate governance*

Abstract *This paper introduces fraud as asset misappropriations (85 per cent of cases), corruption and fraudulent statements. Symptoms include accounting anomalies, lack of internal control environment, lifestyle and behaviour. The most effective tools for fraud detection are internal audit review, specific investigation by management, and whistle-blowing. The paper details the fraud investigation process and the role of auditors as fraud examiners. The correlation of fraud perpetrators' personality with the size of losses is examined. Personality is analysed into age, gender, position, educational background and collusion. A strong system of internal control is most effective in fraud prevention. Fraud prevention procedures, targeted goals and improvements to system weaknesses feature in the paper. Fraud impacts on accounting transactions in accounts receivable, receipts and disbursements, accounts payable, inventories and fixed assets, and financial reporting. The monetary impact resulting from fraud is analysed by the type of victim and the amount of loss. Internal control and good employment practices prevent fraud and mitigate loss.*

Introduction

Accounting fraud involves an intentional action, leading to a misstatement in the financial statements. Webster's New Dictionary defines fraud as "intentional deception to cause a person to give up property or some lawful right". Federal Bureau of Investigation agent delineated fraud best as "the fraudulent conversion and obtaining of money or property by false pretences: included are larcenies by bailed and bad checks, except forgeries and counterfeiting" (Farrell and Franco, 1999).

Most frauds involved an employee or manager of the victims' organisation (Commercial Angles' Newsletter, 2001a, b, c). An analysis of the characteristics of perpetrators showed that the fraud influencing factors include age, gender, position, education background and existence of motive for collusion. The growth of digital/computer technology procreates fraud and generates additional risks of swindling and illicit activities in the future. The Internet can be used in crimes ranging from simple extortion to the most complicated, transnational effort. A dissection of fraud involving the Internet revealed three major categories: securities fraud, fraud in electronic commerce and fraud from Internet companies.

Fraud causes tremendous loss to the business world and creates morale problems in the workplace. When we are stripped of our money by fraudulent means, the consequences can be devastating. Fraud losses are serious problems to organisations that need to be managed, controlled and monitored. Technology, the criminal and law enforcement are continuously leapfrogging each other, as the race continues to build better tools, commit bigger crimes and develop more effective law enforcement. Fraud detection is an examination of the facts to identify the indicators of fraud. Reviewing and improving the internal control system is the primary defence against fraud and abuse. This study showed that a strong system of internal control is the most effective

Managerial Auditing Journal
Vol. 19 No. 8, 2004
pp. 1055-1072

0268-6902
DOI 10.1108/02686900410557953

way of fraud prevention. Hence, the aim of this effort is to raise the level of security awareness for organisations in order to plan and facilitate a concerted effort to battle fraud, as prevention is better than cure.

Research problem

Computer accounting fraud, error and abuse are problems that affect practically every organisation across many dimensions. There are many types of fraud involving different levels of management. This posed many research problems:

- it is difficult to estimate in financial terms the losses to business caused by fraud as most of the time, frauds are unreported or under reported;
- there is no single straightforward test for fraud investigations to show in every case that a fraud had been committed; and
- complex procedures to detect Computer accounting fraud and error. Although we can detect fraud, we cannot avoid fraud totally as it can be committed in many ways.

Objectives of the research

The objectives of the research are:

- to determine types of transactions most vulnerable to Computer accounting fraud, error and abuse;
- to profile fraud offenders and examine the characteristics of the employees who commit Computer accounting fraud, error and abuse;
- to assess the impacts of fraud to accounting transactions and organisation as a whole; and
- to detail and assess the detection and prevention controls.

Scope of the study

Fraud is a big subject. There are various types of fraud that are prevalent to various functions in an organisation. The scope of research focused on computer fraud and abuse that involves breaches of physical, personnel, communications and operations securities. The research included analysis of the modes of computer fraud and abuse, the characteristics of perpetrators and the risks faced by the organisations. The research covered the development and evaluation of strategies to prevent or detect fraud.

Survey of literature

Commercial Angles' Newsletter (2001a) introduced the various types of Computer accounting fraud. It classified groups that can perpetrate fraud: third parties, a company's employees, the company's management, suppliers and customers. In most cases, fraud was not reported because of the risk of embarrassment and reduction in the level of confidence in customers or shareholders. As a result, it was difficult to measure the losses to business caused by fraud. And of the reported frauds, a majority of the worst kind were usually committed by a company's own employees or management. Only a brief discussion took place on the ways fraud took place and the

motives of the perpetrators. The newsletter did not mention the impacts of fraud on an organisation and how fraud can be prevented.

Commercial Angles' Newsletter (2001b) examined the indicators to determine whether a fraud had taken or is taking place. There was no single test to show in every case that a fraud had been committed. Some of the more sophisticated frauds, such as short-term share price manipulation were incredibly difficult to unravel. Conversely, less sophisticated frauds frequently involved only an employee or a manager of the defrauded company. Sample questions for scanning of each method of perpetrating to the suspected fraud were distributed to the surveyed companies to allow the companies to evolve a fraud detection plan with clear objectives. The paper stressed that effective fraud detection required management to be sufficiently knowledgeable about the mechanics of the business and at the same time, be constantly aware of the need to be vigilant against fraud. The limitation of the paper is that the analysis of response to the queries was not made. It failed to provide information on specific tools or techniques to detect computer fraud and abuse.

Apostolou (2000c) provided background information for enhanced understanding of occupational fraud and abuse. The responsibilities of auditors and fraud examiners were also highlighted. She explained the fundamentals of fraud, which consist of the typical schemes, legal elements of fraud, detection and prevention techniques. By referring to the statistical finding in "2002 Report to the Nation on Occupational Fraud and Abuse", she noted that the fraud and abuse cost US organisations an estimated $400 billion losses annually. The author further categorised fraud into fraudulent financial reporting (management fraud) and misappropriation of assets (employee fraud). Examples were quoted from the professional standards, and risk factors of management fraud were analysed into:

- management's characteristics and influence over its control environment;
- industry conditions; and
- operating characteristics and financial stability.

She failed to make comparisons of the functions and the responsibilities of auditors and fraud examiners. The paper did not mention the role of management to prevent and detect occupational fraud and abuse.

McNamee (1999) introduced risk assessment as a tool to help to detect and deal with fraud in operations of organisations. He emphasised that managers had to take responsibilities to locate fraud. Risk assessment could also be used as a decision-making tool to assist managers sort through a number of possibilities and single out those with the greatest payoff. Furthermore, managers could use this technique to identify and prioritise the most likely business processes where potential fraud could occur. McNamee further analysed the three elements of risk assessment. First, risk identification to determine the high-risk areas and its sources. Second, risk measurement to determine the consequences of the risk and likelihood of its occurrence. Last, risk prioritisation is to determine the appropriate resources to manage the risk. This paper only focused on one particular tool to detect fraud and did not suggest any alternative. It failed to give examples to illustrate the application of the tool to investigate fraud.

Riahi-Belkaoui and Picur (2000) stated that organisations today were more susceptible to fraud in the accounting environment than ever before. Fraud had caused

massive losses to firms, individuals and society. They presented a general framework that was useful to identify conditions that were most conducive to fraud in the accounting environment. The framework was based on models and theories from criminology including conflict and consensus approaches, the ecological theory, cultural transmission theory and anomie theory. These theories offered alternative explanations for corporate fraud, white-collar crime, fraudulent financial reporting and audit failures. The authors failed to provide the steps on how to use the framework to categorise the fraud perpetrated in the accounting world. The paper also failed to mention the detective and preventive procedures that can be implemented.

To Commercial Angles' Newsletter (2001c), the best way of preventing fraud was to understand why it happened. Fraudsters generally identify an opportunity for exploiting a weakness in the control procedures and then assess whether their potential rewards would outweigh the penalties should they be caught. In addition, the paper introduced the two-stage processes of fraud prevention. First, an organisation must ensure that opportunities for fraud were minimised: fraud prevention. Second, organisation should ensure that potential fraudsters believe they will be caught: fraud deterrence. Introduction and enforcement of new controls would reduce the opportunities for perpetrators. A regular control was most effective and normally required little management time or effort. It also emphasised the importance of having strong management and a healthy corporate culture to detect and consequently deter fraud. The limitation of this paper is that it did not specify the detailed control procedures for two-step processes of fraud prevention. It failed to explain the financial effects and risk of computer fraud if prevention and deterrence procedures were not in place.

Bowe and Jobome (2001) discussed the designation of a managerial framework to control the operational risk, and focus on unauthorised trading fraud. A sample of 37 cases was taken for examination from financial institutions in eight countries over the period 1984-1999. The sample results indicated that internal controls were the primary defence against severe fraud losses and showed that the regulatory penalties imposed on senior supervisory management, in addition to the fraudster, were crucial in ensuring efficient mitigation of fraud loss. Losses from unauthorised trading fraud can be identified with breakdown of controls and constraints designed to mitigate losses from operational risk. The limitation of the paper is that only one type of fraud was analysed, as there may be other types of fraudulent activities in the financial services industry. The survey also failed to identify the motives of fraud and other preventive measures to combat fraud.

Apostolou (2000a) introduced fraud examinations as a non-recurring activity that was conducted when existence of a fraud in an organisation was established. The main objective of the paper was to outline the differences between a fraud examination and a traditional audit. Fraud examination methodology was presented in the context of important legal considerations. It was a methodology of resolving fraud allegations from inception to disposition. Fraud examination involved obtaining evidence and taking statements, writing reports, and testifying to findings. The author stated that to conduct a fraud examination, the persons required skills to properly detect and investigate an allegation of fraud and also knowledge of the legal elements and which law to apply. The limitation is that she failed to fulfil her objective to elaborate how the

traditional audit is different from the fraud examinations. In addition, it focused only on fraud examination and did not describe other preventive measures.

Vanasco (1998) emphasised that fraudulent financial statements were a great concern to the corporate world and the accounting profession. In particular, the author examined the roles of professional associations, governmental agencies and international accounting and auditing bodies in promulgating standards to deter and detect fraud in the US and a few other countries. Vanasco also examined the impact of management and employee fraud on various business sectors, government bodies and non-profit entities. He discussed the roles of management, the board of directors, the audit committees, auditors, and fraud examiners as well as their liabilities in fraud prevention and investigation. The author explained the ideal control environment to prevent fraud and also focused on the techniques and preventive procedures in the investigative and reporting process. In addition, the writer elaborated on white-collar crimes constituting employee fraud, embezzlement, kiting, larceny, lapping and pilferage. Vanasco also noted several accounts in the financial statements that are vulnerable to fraud. The limitation of the paper is that it did not focus on the impact of fraud on accounting transactions and financial statements. It failed to measure the effect of fraud to victims in monetary terms and the psychological impact on the morale of the employees.

Colbert and Alderman (1995) introduced the approaches adopted by auditors in deriving an audit strategy. The two approaches were procedures-driven approach and the risk-driven approach. Procedures-driven approach did not make full consideration of the risk present. In this approach, the auditor determined the specific audit procedures to be performed without considering the objective of the related risk. Whereas, risk-driven approach was the approach that was planned after the full and specific consideration of the risk. This approach involved assessing, during planning period, the various risks in each area. Generally, risk-driven approach was more effective and efficient than the procedures-driven approach because risk-driven approach focused on the internal auditor's effort areas with relatively more risk. The limitation of the paper is that it did not address the risk factors of an engagement on the procedures-driven approach. The authors failed to discuss in detail how the risk-driven approach helps detection of fraud.

Colbert (2000) illustrated how the International Federation of Accountants and the American Institute of Certified Public Accountants provided guidance to auditors for detecting misstatements in the financial statements that were caused by errors and fraud. Misstatements may be the result of error or fraudulent activities. The author made the comparison of International Standard for error and fraud to the two US audit Standards and disclosed several similarities and few differences particularly on reassuring to auditors serving client offering cross-border securities. The major provisions in the standards provided guidance related to the definitions of error and fraud, the categories of risk, the process of assessing risk, and recommended audit procedures performed to locate and report errors, were alike. She further concluded that the remarkable consistency between the Standards implied that, comparable work was being performed no matter which guidance the auditor was utilising. The limitation is that the paper only provides guidance from the point of view of the auditors; and did not provide a platform for fraud prevention procedures that could be carried out by management. Despite the differences noted in comparing the standards,

no recommendation for improvement or amendment to standards was made to the less well development standards.

Farrell and Franco (1999) conducted a survey objectively to determine the variation in the opinion of those working for the former "Big Six" and other accounting firms. The survey was based on questionnaires mailed to approximately 1,700 accounting firms in New York, New Jersey and Connecticut areas, and approximately 300 questionnaires to the former "Big Six" accounting firms in the United States. The respondents were mainly managers and partners with only 10 per cent response rate. They concluded from the survey that all organisations were victimised by high product costs and low corporate profits. Normally everyone gets shock and disbelief when fraud was detected within an organisation. They also stress the motives and specific characteristics of the offenders and the importance of prevention or detection strategies against business fraud. The auditor played an important role in prevention and detection of business fraud. The limitation of this paper is that the samples of the survey were only limited to certain areas of the United States. Moreover, the response rate may be too low to represent the whole population. The generality of the empirical findings are therefore dubious.

Report to the Nation on Occupational Fraud and Abuse (2002) stated that occupational fraud and abuse was a prevalent problem that had affected practically every organisation, regardless of size, location, or industry. The Association of Certified Fraud Examiners (ACFE) defined the term "occupation fraud" as " the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organisation's resources or assets". The report was based on responses of questionnaires mailed to approximately 10,000 certified fraud examiners (CFE), with 971 fraud cases that were applicable to the survey. The CFEs typically fell into two broad groups: investigators and auditors. They were employed mainly in three sectors: government, business and public accounting. The report covered six categories: the cost of fraud, the methodologies, detection and prevention of fraud, the perpetrators and the victims, and the legal outcomes of fraud cases. The limitation of this survey is that it only focused briefly on the aspect of detection and prevention of fraud. There were no guidelines on the application of preventive procedures for a business organisation. In addition, the respondents of the survey were mainly based on the US business environment.

The 2001 Global e.fraud survey stated that many experts believed that fraud related crimes had been greatly assisted by the introduction of the Internet and e-commerce, hence resulting in e.fraud growth. No country or company was immune to the depredations of the fraudster. KPMG surveyed the world's largest companies in 12 countries on electronic fraud and security issues. This survey was based on questionnaires mailed to more than 14,000 CEOs, CIO, and other senior executives of the companies, for which only an average response rate of 9 per cent was achieved. This survey included awareness of e.fraud and e-commerce security risks and threats, e.fraud and security breaches, prevention and detection of e.fraud and security breaches, and consumer perceptions about e-commerce security. The limitation of the survey is that the scope of research was only on the largest companies in 12 countries, as the opportunities for fraud are greater in smaller companies. The impact of fraud to the companies and the economy is also absent in this survey.

Apostolou (2000b) discussed the procedures of conducting an Internet fraud investigation in a four-part series paper. In part one, she presented the terminology essential to developing expertise in fraud investigative techniques and an overview of civil and criminal law proceedings. Asset misappropriation, as introduced in part two was a serious problem that it can lead to material misstatement in the financial statements. Identifying the various asset misappropriation schemes was part of the fraud investigation. The third part covered the methods of making illegal payments in the disbursement process. Part four discussed the fraud investigation procedures. Fraud investigation consists of obtaining information to prove or disprove an allegation. The investigator should choose the procedures that provide maximum evidence for the minimum cost and risk. The fraud investigative techniques discussed are less applicable to the management as she had illustrated them from the viewpoint of the legal authority. In addition, the author failed to mention the fraud prevention procedures.

Baker (1999) analysed three matters with significant potential for misleading and fraudulent practices and the issue of fraud on the Internet. The three are:

- securities fraud on the Internet, especially activities that violated US security laws like stock price manipulation and non-existent investments;
- fraud in electronic commerce with regard to misused information and non-existent products; and
- fraud arising from the rapid growth of Internet companies that lacked traditional management and internal controls.

The author also gave suggestions on how these abuses may be combated. The paper did not discuss the risk and impact of Internet fraud to an organisation and the economy as a whole. It did not highlight the role of management and auditors in the prevention and detection of Internet fraud.

Smith (1999) noted that now-a-days, digital technologies played an important role in the daily activities of the public. Benefits can be derived from digital technologies as the governments can deliver services electronically to everyone. Russell stressed how the developments of delivering services electronically by governments led to improper use and how the growing use of computer technologies by government agencies created additional risks of illegal and fraudulent conduct. This paper focused on two areas: the nature and the extent of the problem, and the preventive and control strategies. Several solutions to the problems were given, many of which also made use of computers. The author did not mention from the micro point of view about the other victims as fraud may happen anytime, anywhere and to any organisations. The paper also failed to give explanation on the cost and risky effects of a defrauding government towards the confidence of the people.

Haugen and Selin (1999) claimed that computer crime and fraud were more perilous to organisations today. This paper presented the statistics about the growth of fraud, and causes of fraud in the workplace. Furthermore, they elaborated on the common computer frauds, techniques used to commit fraud, the computer-based controls, as well as on how business assets can be protected. They stated that none of the organisations in the world could be 100 per cent free of risk, and assessing an organisation's risk to fraud was not easy. However, the risk could be mitigated by implementing a proper internal control system with good employment practices. The

limitation of the paper is that the computer-based control that was suggested for prevention of fraud is costly and not user friendly, as it requires a specialist for its construction and maintenance. The author also failed to assess the effectiveness of the controls to an organisation.

Dhillon (1999) claimed that computer related fraud caused a lot of losses in organisations and it could be avoided if a more serious approach about the prevention and deterrence procedures was taken. Business and organisations were trying to cope with the intricacy and mystique that surrounds computer system. He further stated that it seems that less security was applied to the data or information held in computer systems than held in manual systems. Typically, only IT department were concerned about computer security, but the other professionals did not give adequate attention to it. The author emphasised that more proactive security administration was needed to avoid losses caused by computer fraud. Fraud by insiders was a major problem, as it was difficult to prevent especially when blended with legitimate transactions. On the other hand, by having appropriate legislative controls and stricter criminal penalties, fraud could be prevented to a certain extent. The author failed to provide information on types of fraud that could occur and the impact of fraud on the organisation. He failed to suggest the types of security system that are suitable for implementation in different organisations with different needs and requirements.

Rusch (2001) discussed the rapid rising tide of Internet fraud in electronic commerce. Fraud grew in conjunction with the expansion of legitimate Internet use. The author quoted the report of International Chamber of Commerce's Commercial Crime Services Division that Internet fraud in 2000 was "rising dramatically", more than twice as much as in 1999. The emerging data suggested that the problem of Internet fraud was becoming global in scope and impact, as criminals could plan and execute fraudulent schemes from anywhere in the world and victims might be located anywhere in the world. The paper illustrated that the criminal statutes that apply to other types of white collar crime – conspiracy, mail and wire fraud, credit card fraud, securities fraud, money laundering, and identity theft – were equally applicable to various forms of Internet fraud. In addition, a variety of existing sentencing guidelines also enabled federal prosecutors to seek higher sentences in appropriate cases of Internet fraud. The limitation of the paper is that it did not provide the solutions to Internet fraud. The authors failed to discuss the Internet fraud breaches by insiders, as insider fraud is more serious.

Research methodology

Information for research in Computer accounting fraud was gathered from different sources of secondary data. Most data were collected through Internet search engines like Google and Altavista. The online papers were downloaded from the Internet Web sites such as Emerald, Newsletter, Business Week and Managerial Auditing Journal. Fraud Survey Reports were published by the ACFE while E-fraud Survey Reports was obtained from KPMG Forensic & Litigation Services. Some data were obtained from reference books.

From the secondary data collected, the research framework is developed on the anatomy of Computer accounting frauds as shown in Figure 1.

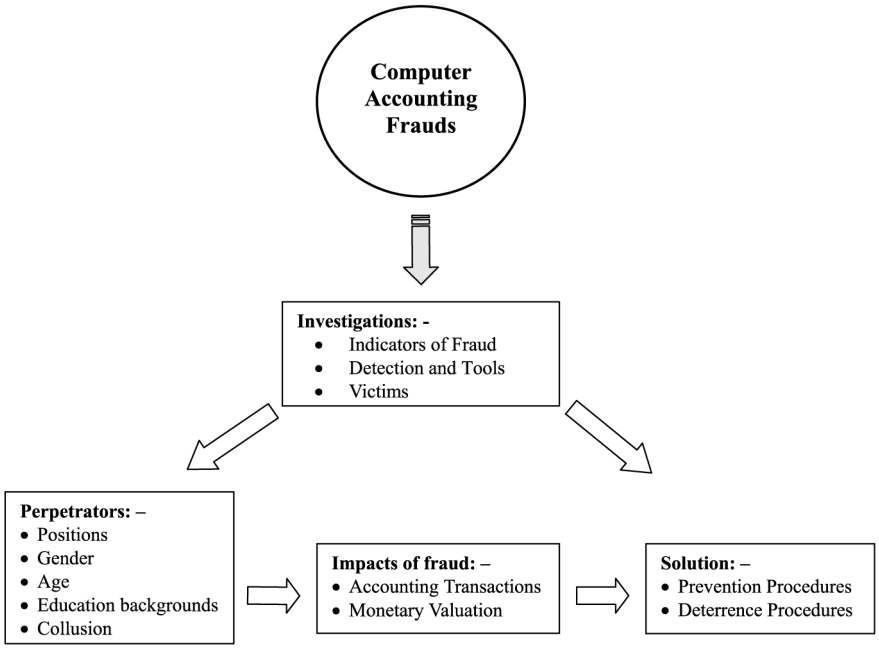

Figure 1.
Research framework on anatomy of computer accounting frauds

Discussion, analysis and finding

Fraud is a common issue for business. Computer fraud is defined as "any fraudulent behaviour connected with computerisation by which someone intends to gain a dishonest advantage" (Vanasco, 1998).

Fraud is easily committed, but is difficult to prevent and detect. ACFE classified fraud into three major categories: asset misappropriations, corruption and fraudulent statements.

- Assets misappropriation includes the misuse or theft of assets in an organisation (for example inventory fraud, payroll fraud and computer fraud).
- Corruption is the act that people wrongly use their power in the business transaction in order to procure some benefits for themselves or others (for example, conflicts of interest and related-party transactions).
- Fraudulent statements are the falsification of financial statements of an organisation (for example, unrecorded liabilities).

Assets misappropriation is the main reason of fraud, with more than 85 per cent of total fraud under this category. The assets that are targeted by perpetrator commonly are cash.

Indicators of fraud

While professional internal auditors may not be the insurers against fraud, their responsibility for due professional care requires an increasingly high level of alertness

to the indicators of fraud (Vanasco, 1998). An organisation should take up a proactive approach to reduce costs related to fraud. Fraud prevention programs should be emphasised and not reaction to fraud already committed.

The symptoms of fraud are often obvious to anyone who cares to look. These indicators may arise as a result of control established by management, tests conducted by auditors and other sources both within and outside the organisation. Among some indications are:

- accounting anomalies, which include embezzlement, understatement of liabilities, overstatement of expenses, missing documents, alterations to documents, excessive voids or credits and duplicate payments;
- internal control symptoms, which include lack of control environment, lack of physical safeguards, lack of segregation of duties, lack of proper documents and records and inadequate accounting system;
- analytical symptoms, which include transactions that occur at odd times and places with amounts that are too large or too small;
- lifestyle symptoms, which show the employees' living lifestyles are far beyond what they can afford considering the employees' financial needs, greed or pressures;
- behavioural symptoms, which come from the employees' odd and recognisable behaviour patterns; unusual irritability and suspiciousness; and
- tips and complaints from other employees that something is wrong.

Fraud detection

Further investigation if the indicators are present may lead to fraud detection. Fraud detection is an examination of the facts to identify the indicators of fraud sufficient to warrant recommending an investigation. In facts, there is no single test that a fraud has been committed. Most frauds involved an employee or manager of the victims' organisation (Commercial Angles' Newsletter, 2001a, b, c).

The most effective tools for fraud detection are internal audit review, specific investigation by management, employee notification and accidental discovery. Whistle-blowing is considered as another way of detection. Whistle-blower is the employee who reports unethical and illegal practices in the place of work. Whistle-blower needs to be protected and cherished by their employers (Vinten, 1994). Those who have an occasion in blowing the whistle are sometimes bitter about the results of having done so. Employee must be given an easy opportunity for whistle-blowing and must assure that it is okay to come forward (Vanasco, 1998).

In making the ordinary examination, an independent auditor is aware of the possibility that fraud may exist. Financial statements may be overstated as the result of defalcation and similar irregularities, or deliberate misrepresentation by management, or both. However, the ordinary examination in accordance with the auditing standards is directed to the expression of an opinion in financial statements and is not primarily or specifically designed to detect fraud. It cannot be relied upon to disclose the misstatement or omission, although their discovery may be fruitful at times.

The five-step approach suggested by Vanasco (1998) for fraud detection in an audit is as follows:

(1) know fraud exposure in specific terms;
(2) know exposure specific symptoms of fraud;
(3) be alert for fraud symptoms;
(4) incorporate into routine audit program steps that are likely to reveal fraud symptoms; and
(5) follow through on all observed symptoms.

Fraud investigation

Investigation consists of performing extended procedures necessary to determine whether fraud, as suggested by the indicators, has occurred. It includes gathering sufficient evidential matter about the specific details of a discovered fraud. All computer fraud investigations need to start with a plan for gathering and handling the evidence. Internal auditors, lawyers, investigators, security personnel, and other specialists from inside or outside the organisations are the parties that usually conduct or participate in fraud investigations. The investigator must be familiar with good systems administration practices and possess extensive background of skills and knowledge relevant to computer security and various concepts at work in the areas under investigation (Wright, 2000).

When fraud has been detected, an organisation's main concern is to identify the source of fraud and to determine whether it is an internal or an external problem. According to the IIA Standards (SIAS No. 3), the roles of internal auditing in the investigation of fraud include:

- assessing the probable level and extent of the complexity of fraud within the organization;
- assessing the qualifications and the skills of the internal auditors and the specialists available to participate in the investigation to ensure that it is conducted by individuals having the appropriate type and level of technical expertise to effectively carry out the investigation;
- being cognisant of the rights of alleged perpetrators and personnel within the scope of the investigation and the reputation of the organization itself;
- designing procedures to follow in attempting to identify the perpetrators, extent of fraud, techniques used, and cause of fraud; and
- coordinating activities with management personnel, legal counsel, and other specialists as appropriate throughout the course of the investigation.

When a fraud investigation reveals irregularities, which may have an adverse impact on the financial position and results of operations, the internal auditors should inform the appropriate management and the audit committee. A suspect should not be confronted until supporting evidence has been gathered. Confrontation should be done by persons who specialize in investigating criminal activity, not by internal auditors.

Investigating a case may involve covert operations, surveillance, informants, dumpster diving and sources of information (Apostolou, 2000c).

- Covert (undercover) operations may be used to prove the allegation of fraud. The court deems the undercover operations, as an acceptable method of acquiring

information, provided there is sufficient probable cause that a crime has been committed.

- Surveillance is the secretive and continuous observance of a suspect's activities and is frequently used in developing evidence. It may be used to obtain probable cause for search warrants, develop investigative leads, identify co-conspirators, gather intelligence, and locate persons or objects.
- Informants are persons who have specific knowledge of a criminal activity. Informants can be extremely useful in fraud investigations regardless of their personal motivation for supplying information.
- Dumpster diving is used when the investigator finds it necessary to sift a suspect's trash to obtain evidence and leads. Important documents and information concerning illegal activity may be found in garbage. The courts have upheld that investigators may sift through trash without a search warrant, provided that the trash has left a suspect's possession. After it has left the suspect's possession, there is no longer the reasonable expectation of privacy, and thus it is a fair game.
- A large variety of information sources are available to the investigator to assist in the investigation of a case. Information can be "in-house" or public and might be used for locate individuals or verify their identity or research assets or financial positions or document lifestyles and background information.

Perpetrators

Who are the fraud perpetrators? Fraud perpetrators are the persons those commit fraud. What is the correlation of a perpetrator's personality with the size of losses in an organisation? We further examine the personality into age, gender, positions education background and the factor of collusion.

First, with age, the 2002 survey from the ACFE showed that the older the perpetrator, more costly their schemes become. The losses for older employees were 27 times higher than losses caused by the younger age employees. The reason being, older employees hold more senior positions with greater access to assets. Commonly, in an organisation, the majority of higher positions (managerial and above) are held by males. Findings in the survey report revealed that most fraud cases were committed by males. The losses committed by males were three times more than females, i.e. males committed more than 75 per cent of all fraud. Generally, those in higher positions in an organisation tend to have higher levels of education. The ACFE report showed that those with college degree caused about 3.5 times higher losses than those with only high school diplomas. As the perpetrator's education level increased, the losses are also increased. Losses caused by age, gender and education background appeared to be correlated to the employee's position in the organisation. Position effects were the strongest indicator of the size of the losses in most of the fraud cases.

Collusion is an illegal collaboration activity that is very difficult to prevent and detect, especially when collusion is between managers and employees. This is because the managers are naturally counted upon as a key part of the organisation's control structure. They are entrusted to identify and detect fraud through their oversight functions. When managers participate in fraud along with their employees, this serves

to disrupt a major component of internal control and creates a much higher level of insecurity for the organisation.

Fraud prevention

The value of internal control is apparent in both preventing and detecting fraud as prevention is better than cure. A weak internal control creates opportunities for fraud and about half of all frauds occur in the financial area (Vanasco, 1998). Internal control system has four broad objectives, those are to safeguard assets of the firm; to ensure the accuracy and reliability of accounting records and information; to promote efficiency in the firm's operation; and to measure compliance with management's prescribed policies and procedures (Haugen and Selin, 1999). The effectiveness of internal control depends largely on management integrity.

The cost of a fraud is not only a monetary loss, but it vitiates the organisation's atmosphere, creates mistrust and calls for harsh measures that could have been avoided. Reviewing and improving internal control are often thought of as the primary defence against fraud and abuse. A strong system of internal control is the most effective method of fraud prevention. Prevention of fraud starts with identification of the weakness in the current systems of an organisation. Next, the organisation must improve those systems with new or better controls. The introduction and enforcement of controls will reduce the opportunities for fraud. The control warns potential fraudsters that management is actively monitoring the business and that in turn deters fraud (Commercial Angles' Newsletter, 2001a, b, c). As a result, an organisation, which seeks to contain computer fraud, should strive to implement a broad range of interventions, be it technical, formal or informal. Technical interventions are controls implemented to limit access to building, rooms or computer systems. Formal interventions involve horizontal expansion of the hierarchy of organisation to have a flatter pyramid. Education, training and awareness programmes are some measures implemented in the informal interventions. Controls have dysfunctional effects because isolated solutions have been provided for specific problems. These "solutions" tend to ignore other existing controls and their contexts. Thus, individual controls in each of the three categories, though being important, must complement each other. This necessitates an over-arching policy, which determines the nature of controls being implemented, and therefore provides a comprehensive security to the organisation (Dhillon, 1999).

Fraud prevention procedures should have three realistic and measurable goals:

(1) reduce losses resulting from fraud;

(2) deter fraud through proactive policies; and

(3) increase the likelihood of early fraud detection.

Fraud control policies should provide guidelines on ways to reduce the risk of fraud. For example, a comprehensive security program assists in the prevention and detection of computer fraud from all sources. The use of various layers of properly implemented protection mechanisms will have the synergistic effect of increasing and enhancing a security program. Currently, many experts considered the "onion" model of security as the best and safest approach to manage the risks dealing with computer fraud (KPMG, 2001).

Employees have the highest possibilities to be fraudsters. Thus, the main factor which fraud can be contained lies in ensuring that trustworthy and reliable staffs are

employed, particularly in positions of responsibility (Vanasco, 1998). Employee has the ability to make use of confidential information or facilities to commit fraud or collude with an outsider to perpetrate a crime. Performing background checks, to a certain extent, would help to prevent fraud. The level of background checks performed should be commensurate with the level of risk associated with the position (KPMG, 2001).

Fraud deterrent

The deterrent effects of criminal prosecution and punishment represent the final means of preventing fraud. In addition to conventional judicial punishments such as imprisonment and fines, deterrence can also be achieved through professional disciplinary sanctions, civil action, injunctive orders and confiscation of an offender's assets.

Technology would also help to deter fraud. "Logic bombs" is a strategy that is developed to prevent software piracy and is installed into programs. When activated through an act of unauthorised copying, the malicious code destroys the copied data and is even able to damage other software or hardware being used by the offender. Employees who cause such damage would, presumably, be personally liable for replacement costs and any consequential loss (Smith, 1999).

Impact on accounting transactions

In accounting environment, there are many types of fraud transactions (Vanasco, 1998). First is the fraud in the accounts receivable and sales. Accounts receivable is quite vulnerable to asset misappropriation schemes. The most common fraud schemes affecting accounts receivable are lapping, fictitious receivables and improper posting of credits. Sales and marketing fraud may be the fraudulent actions to generate fabricated commissions, or sales representatives who swindle customers for the benefit of the company or themselves. Financial statements may be misrepresented by the exaggerated accounts receivable and sales end of the year.

Cash receipts and disbursements are also subject to fraud transaction. There are three typical cash fraud schemes that may be encountered in these transactions; they are skimming, larceny and fraudulent disbursements. If the duties for cash receipts and cash application are performed by the same person, this may results in fraudulent misappropriation of cash. Internal control enforcement is to ensure that the segregation of duties for cash receipts, cash application, and cash report functions to avoid any risk of fraud.

Inventory schemes and fixed asset fraud schemes are under asset misappropriation schemes. Inventory frauds involve appropriating inventories and supplies for personal use, stealing inventory, theft of scrap and charging embezzlements to inventory. When a fraud is expected in the organisation's inventory and fixed asset, auditors need to examine what assets are held and how those assets can be taken. Some fixed assets that are easily removed from the premises are especially prone to employee theft. Whereas, unauthorised personal use of fixed assets by employees can develop into a fraud or abuse situation if the management does not address the subject via improved controls. In addition to the improper usage of the asset itself, the loss of productive time might be more costly than the use of the asset.

Accounts payable or purchases is a financial reporting fraud. Lack of control in accounts payable may cause fraudulent financial statements. If no verification was

made on the existence of vendors, a person in charge may defraud by means of cheques written to non-existent vendors and diverted to his own bank accounts. Verification of vendors is necessary and stopping the practice of hand delivery of cheques will help mitigate the risk as well.

Payroll fraud is a situation where an employee causes an organisation to issue a payment by making false claims for compensation. This fraud took place by setting phantom employees; failing to delete employees who have been terminated and submitting excessive overtime. This kind of fraud may arise when lack of implementation in the internal control system.

Related-party transactions played a large role in several well-publicised fraud cases. In carrying out all phases of the audit, the auditor should be alert to any clues regarding the existence of related parties and for transactions involving them. Related-party transactions are frequently used as conduits for transferring assets out as in the Continental Vending Machine fraud case. To muddy the audit trails, loan proceeds are transferred back and forward between the companies (Vanasco, 1998). In July 1975, the AICPA issued SAS No. 6, Related Party Transactions and provided the following definition: related parties exist when another entity has the ability to significantly influence the management or operating policies of the transacting parties or when another entity has an ownership interest in one of the transacting parties and the ability to significantly influence the other, to the extent that one or more of the transacting parties might be prevented from fully pursuing its own separate interests. Accounting fraud may happen when liabilities are unrecorded. This may happen when a company is trying to cover the real conditions from the shareholders or the public. Procedures of examining subsequent cash disbursements may help to detect the liabilities that existed at the year-end but are omitted from liabilities recorded in the client's financial statements.

Conflict of interest occurs when employees are both self-employed and work with an organisation. Frequently, they tend to sell their personal products to the organisation they work for. Normally, an organisation will not transact business with their employees so that the employees will not be placed in a situation where a conflict of interest exists between the employees' responsibilities to the employers and the employees' self-interest. Conflicts of interests can lead to fraud which are difficult to detect.

Monetary valuation

Problems resulted from fraud are staggering. Victims are the organisations that employ the fraud perpetrators and suffer losses from their crime. The ACFE's report categorised the victims into four sectors, which are publicly traded company, privately held company, government agency and not-for-profit organisation. The results showed that the largest losses came from the category of publicly traded company. This is due to the magnitude of financial assets involved in fraud in publicly traded companies is relatively higher than the other categories. In terms of fraud occurrence, privately held company is highest (31.9 per cent), followed by publicly traded company (30.0 per cent), government agency (24.7 per cent) and not-for-Profit organisation (13.4 per cent). The internal control environment for privately held company usually is less effective and sometimes not even in place, hence results in higher exposure to risk of fraud (Figure 2).

It is impossible to calculate the actual cost that is incurred by fraud because not all fraud is detected or reported. The CFEs projected the loss resulted from the fraud

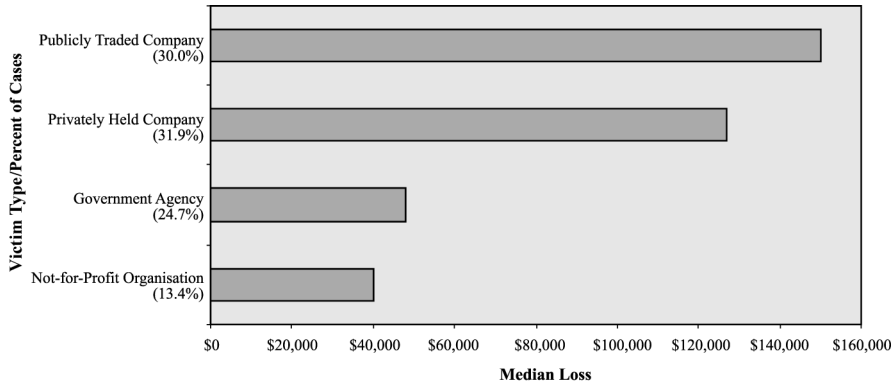

Figure 2.
Loss by organisation type

Source: 2002 Report to the Nation on Occupational Fraud and Abuse

and abuse at median cost of six per cent of revenues in 2002. A study conducted by AFE revealed that losses from fraud to US organisations amounted to $600 billion per year. Figure 3 shows the statistics collected in the surveys of CFE from 620 cases.

Limitations

The computer has incredible speed. It controls one millionth of a second. Human ingenuity has always an edge over all these developments. This research only touches on the surface of the Computer accounting fraud due to time constraint. There is much more to investigate and explore on this topic especially on the techniques of committing fraud in a computerised business environment. In addition, there are still many ways of conducting investigation, as the research done in the literature review topics is quite specific. Tools for preventing and deterring fraud are not discussed in details. The legal cases and proceedings in court involving fraud are not discussed. The benefits derived from safeguarding assets through good internal control system in an organisation are emphasised in the current study. An evaluation on the effectiveness of procedures and measures in preventing fraud can be a focus for further

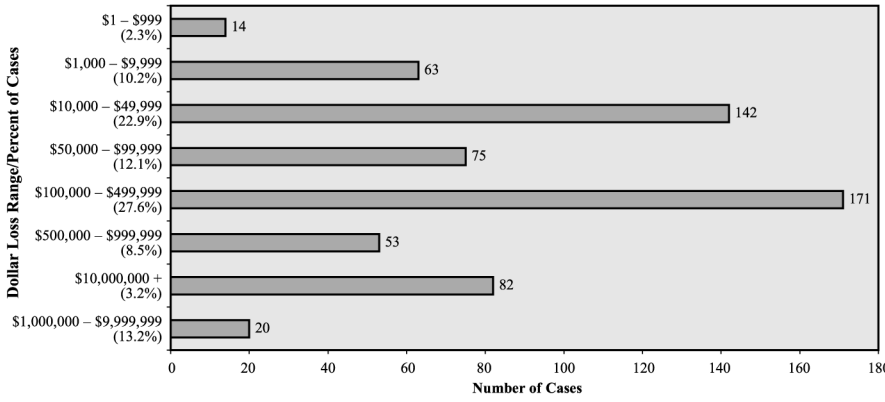

Figure 3.
Distribution of dollar losses number of cases

Source: 2002 Report to the Nation on Occupational Fraud and Abuse

research. With the introduction of virtual business transactions in the electronic era, the risk of fraud increases tremendously. Future research can concentrate on the preventive and detective techniques as there is not much survey evidence.

Conclusions

The development of computer technologies in organisation has greatly enhanced the ability of people to defraud. The losses caused by fraud can only be estimated, as many cases go unreported or under reported. However, it has to be recognised that the fraud losses incurred can be enormous.

Futurist predicted that organised crime would take full advantage of the information superhighway. A prime target will be financial institutions. Computer-literate mob groups will re-route electronic-cash flow and steal valuable information kept by banks (Vanasco, 1998). The movement toward an increasingly computerised global economy likely will heighten exposure to fraud.

A concerted endeavour must be exercised by the management of the business and all employees of the business in order to battle fraud in businesses. Fraud is not a victimless crime (Farrell and Franco, 1999). Assessing the organisation's risk to fraud is made more difficult by today's modern business practices where transactions are processed remotely and electronically and operations are geographically separated from each other.

Preventing fraud consists of those actions taken to discourage the perpetration of fraud and limit the exposure if fraud does occur. Nobody can guarantee that fraud will not occur. Given its inherent limitations, even an effective internal control structure cannot provide more than reasonable assurance that fraud will be prevented. Nevertheless, by initiating adequate internal controls by management, good employment practices and training programs, organisations can take a proactive stance in warding off fraud and keep losses to minimum.

References

Apostolou, B. (2000a), "Conduct an internal fraud investigation", (Part 1-4), available at: http://accounting.smartpros.com/

Apostolou, B. (2000b), "Introduction to fraud examination", available at: www.smartpros.com/x20682.xml

Apostolou, B. (2000c), "Fundamentals of occupational fraud and abuse", available at: www.smartpros.com/x20634.xml

Baker, C.R. (1999), "An analysis of fraud on the Internet", *Internet Research: Electronic Networking Applications and Policy*, Vol. 9 No. 5, pp. 348-60.

Bowe, M. and Jobome, G. (2001), "Fraudulent activity in financial institutions and optimal incentive structures for managing operational risk", *Bank of Valletta Review*, No. 24.

Colbert, J.L. (2000), "International and US standard: error and fraud", *Managerial Auditing Journal*, Vol. 15 No. 3, pp. 97-107.

Colbert, J.L. and Alderman, C.W. (1995), "A risk-driven approach to the internal audit", *Managerial Auditing Journal*, Vol. 10 No. 2, pp. 38-44.

Commercial Angles' Newsletter (2001a), "Fraud prevention", May 2001, available at: www.commercialangles.com/articles/fraud_prevention.htm

Commercial Angles' Newsletter (2001b), "Fraud prevention", June 2001, available at: www.commercialangles.com/articles/fraud_detection.htm

Commercial Angles' Newsletter (2001c), "Fraud prevention", July 2001, available at: www.commercialangles.com/articles/fraud_control.htm

Dhillon, G. (1999), "Managing and controlling computer misuse", *Information Management & Computer Security*, Vol. 7 No. 4, pp. 171-5.

Farrell, B.R. and Franco, J.R. (1999), "The role of the auditor in the prevention and detection of business fraud: SAS No. 82", *Western Criminology Review*, Vol. 2 No. 1.

Haugen, S. and Selin, J.R. (1999), "Identifying and controlling computer crime and employee fraud", *Journal: Industrial Management & Data Systems*, Vol. 99 No. 8, pp. 340-4.

KPMG (2001), "2001 global e.fraud survey", available at: www.kpmg.ie/irm/efraud.pdf

McNamee, D. (1999), "Risk assessment and fraud", available at: www.mc2consulting.com/fraurisk.htm

Riahi-Belkaoui, A. and Picur, R.D. (2000), "Understanding fraud in the accounting environment", *Managerial Finance*, Vol. 26 No. 11, pp. 33-40.

Rusch, J. (2001), "The rising tide of Internet fraud", *United States Attorneys' Bulletin*, (Internet Fraud Cybercrime II), Vol. 49 No. 3, pp. 6-12.

Smith, R.G. (1999), "Defrauding governments in the twenty-first century", *Trends & Issues in Crime and Criminal Justice*, April, No. 111.

Vanasco, R.R. (1998), "Fraud auditing", *Managerial Auditing Journal*, Vol. 13 No. 1, pp. 4-71.

Vinten, G. (1994), *Whistleblowing – Subversion or Corporate Citizenship?*, St Martin's Press, New York, NY.

Wright, T.E. (2000), "An introduction to the field guide for investing computer crime", (Part1-Part 8), available at: http://online.securityfocus.com

Further reading

Association of Certified Fraud Examiners (ACFE) (1996), "Report to the nation on occupational fraud and abuse", available at: www.cfenet.com

Association of Certified Fraud Examiners (ACFE) (2002), "2002 report to the nation on occupational fraud and abuse", available at: www.cfenet.com

Briney, A. (2000), "Security focused", *Information Security*, pp. 40-68.

Ernst & Young (2002), "Global information security survey 2002", available at: www.ey.com/global

Lee, M. and Colbert, J.L. (1997), "Analytical procedures: management tools for monitoring control", *Management Decision*, Vol. 35 No. 9, pp. 682-8.

Morris, D.A. (2001), "Tracking a computer hacker", *United States Attorneys' Bulletin*, (Internet Fraud Cybercrime II), Vol. 49 No. 3, pp. 13-17.

Painter, C.M.E. (2001), "Tracing in Internet fraud cases: pairgain and NEI world web", *United States Attorneys' Bulletin*, (Internet Fraud Cybercrime II), Vol. 49 No. 3, pp. 18-21.

Power, R. (2002), "2002 CSI/FBI computer crime and security survey", *Computer Security Issues & Trends*, available at: www.gocsi.com/