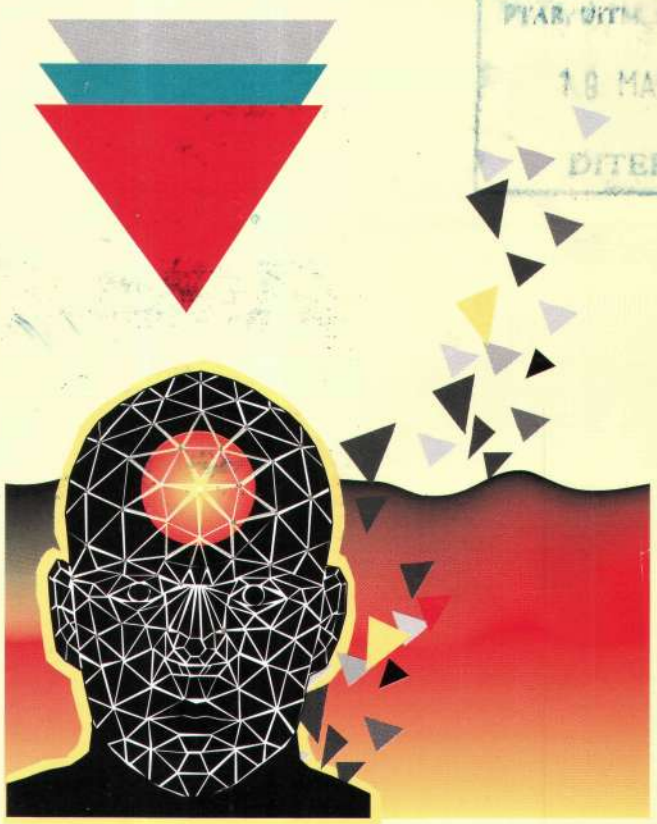
JILID 1 BIL. 1 OKTOBER 1997

Teknologi Maklumat & Sains Kuantitatif



Jurnal Fakulti Teknologi Maklumat dan Sains Kuantitatif
(Journal of the Faculty of Information Technology and Quantitative Sciences)

INFORMATION SYSTEMS AUDITING AND COMPUTER FRAUD

by
Yap May Lin

ABSTRACT

"EDP auditing is defined as the process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, achieves organizational goals effectively, and consumes resources efficiently." [Weber, 1988].

The issue of computer fraud has been given a considerable amount of space in most books devoted to the subject of EDP or Information Systems (IS) auditing. Studies have shown that the monetary amounts misappropriated in the average fraud involving EDP or IS substantially exceed the corresponding monetary amounts in the average fraud situation that does not involve automated services. Hence, the subsequent establishment or expansion of existing IS audit departments by management primarily as a defense against material fraud.

The purpose of this paper is to focus on two issues. One, the occurrence of computer fraud in the IT environment, and secondly, IS auditing as a deterrent to discourage the commission of fraud.

Yap May Lin is at Lecturer in MARA Institute of Technology, Shah Alam

INTRODUCTION

In many IT-advanced countries, computer fraud is already the most important form of crime, and incidentally is just about the most difficult to combat. The difficulty herein lies simply on the fact that computer fraud requires a higher type of intelligence and is essentially a white-collar crime. The EDP auditor (or IS auditor, as is commonly known today) can anticipate an ever-increasing role in combating computer fraud. The reasons for this may be attributed to the changing social and management attitudes, increasing materialism, and the expanded use and increasing sophistication of information technology in business environments [Mullen, 1990; Gallegos, et. al., 1987].

COMPUTER FRAUDS

Computer frauds typically involve considerable monetary amounts. One-time fraud and ongoing fraud are two major categories of large monetary frauds [Alexander, 1996; Pfleeger, 1989; Gallegos, et. al., 1987]. They are generally committed for quick dishonest profit or profit afer a duration of time, at the expense of the victim. A third category known as challenge-the-system fraud may not be committed for profit but may cost companies considerable losses not only in monetary but intangible resources as well [Alexander, 1996; Amoroso, 1994; Gallegos, et. al. 1987].

A one-time fraud involves one transaction for a great amount of money. IS services often handle large transactions and therefore are susceptible to such one-time frauds. These frauds are relatively unsophisticated and often take advantage of poor access controls or placing undue trust in a particular person in a manner that eliminates manual checks and balances. Indeed, most offences are committed by people who have achieved positions of trust and who then abuse these positions. Fortunately, in such instances, unless internal controls are non-existent, the fraud is generally detected shortly after it has been committed. The big problem is to detect fraud soon enough to facilitate the necessary recovery efforts. After such an occurrence, management will generally promote the installation of many additional controls to prevent a recurrence.

Ongoing fraud is the second category of large monetary computer fraud and it involves the consistent, systematic misappropriation of funds, products or services. Here perpetrators take advantage of the consistency of processing being performed by a dumb machine. This type of fraud may go undetected for years depending on the patience and greed of the perpetrator. These frauds are often relatively sophisticated and perpetuated by someone who is an expert or who has an in-depth knowledge in overall company operations in the given area. Often the perpetrator is a user of the

system and not a member of the IS department. Access to the relevant systems, or parts of systems, may either be authorized by a gullible employer or engineered by the would-be perpetrator. The perpetrator must believe that there is a reasonable chance of concealing either the existence of the fraud itself, or their own identity. The most effective way of preventing fraud of this type is by employing such application control measures as automated reasonableness tests, limit tests and exception reporting on the detailed level. Many of these frauds require adjustments of transaction entries to periodically cover any traces of the misappropriation. Special emphasis should, thus, be placed on the review of transactions adjustment and correction, and the trail of authorizations of such reviews.

The third type of fraud unique to IT is that inspired by the technical challenge of the system and its organization. Challenge-the-system fraud is often not committed for profit. It is, however, committed to gain recognition for the perpetrator's innovative abilities of hacking or gaining illegal access into a sophisticated information system. Regardless of intent, this type of fraud can prove extremely costly in direct losses, damage to the company's reputation and by encouraging other would-be hackers to meet the challenge. Perpetrators are usually highly skilled technicians working for the company or outsiders (most commonly, high school and college students) with the ability to tap into the organization's computer system through available local area networks (LAN) and wide area networks (WAN) networks [Alexander, 1996; Stallings, 1995; Pfleeger, 1989; Cooper, 1988].Sometimes perpetrators start out with the intent of committing mischief by the intellectual challenge of beating the system, or simply having fun and then identify an opportunity to benefit financially as well. The most effective protection against this type of fraud is to establish comprehensive backup and recovery procedures and not install any system which cannot be reasonably secured.

IS AUDITING AS A DETERRENT TO FRAUD

It is important to increase the level of awareness among organizations on the need for computer security. Organizations should make computer security its prime responsibility. Taking precautions to secure one's computer environment is a necessary first step to defend one's system against fraudulent activities. The presence of an effective *IS* audit function is a significant part of the overall internal control structure of an organization [Mullen, 1990; Watne & Turney, 1990; Chambers & Court, 1988; Weber, 1988].The most effective way for the *IS* auditor to be a fraud deterrent is to be highly visible. Visibility may be achieved in some of the following ways:

- Conducting a considerable number of interviews and observations involving users and IS personnel, making them aware of the auditor's presence.

- Conducting security audits (or surprise audits) and avoiding the establishment of a consistent and routine audit schedule.

- Conducting audits of new and existing production processing operations throughout the year.

- Identifying control deficiencies and promoting their timely correction through written and oral communication.

- Making extensive use of computer-aided audit techniques throughout the year.

In addition to maintaining visibility, the *IS* auditor can effectively deter fraud by expanding the scope of his or her reviews to all potential areas of concern such as personnel hiring practices, purchasing practices and the disposal of equipment and billing for services rendered. Many auditors who perform application reviews fail to venture into user areas to establish that user controls and supervisory controls are operating as intended. In all these instances, the scope of *IS* audit can serve as an effective deterrent against fraud.

In addition to the above mentioned functions, the IS auditor should play an active advisory role in the strategic planning of information systems. The *IS* auditor should participate in such advisory functions as a step towards building information systems that are more reliable and secure. However, the independence of the auditor during the course of the *IS* development process must be stressed [ISACA, 1994]. The auditor's involvement in an *IS* development process should strictly be at an advisory level (e.g., recommending control enhancements), he or she should not be actively involved in the decision-makings of an information system's design and implementation processes as this would impair the auditor's ability to perform an independent evaluation of the system after its implementation. Hence, although the auditor's expertise could be tapped, with the end-result of proper IS controls being incorporated into the building of the system [Mullen, 1990; Watne & Turney, 1990; Weber, 1988], the manner and appearance of the auditor should be independent so as not to compromise his or her audit review of the system upon completion.

There is a need for *IS* auditors to catch up and keep pace with fast-moving information technology in order to maintain a technical competency necessary in the performance of their work [ISACA, 1994]. Moreover, further audit education would be essential as a fraud deterrence. Obtaining information about new security devices and techniques being developed and evaluate their applicability to the IT environment. Establishing contact with other *IS* auditors in similar processing environments and jointly develop means of detecting and correcting improprieties. Studying all new hardware, software, database management and telecommunication systems being implemented to learn all about their inherent controls and vulnerabilities.

CONTROL MEASURES FOR FRAUD IDENTIFICATION

While the mere presence of an IS audit function can be considered a general deterrent to fraud, there are many things that the auditor can do to improve chances of identifying frauds should they occur. When a fraud has been discovered the auditor can focus attention on very specific tasks that must be performed. However, some control measures the IS auditor can employ to identify frauds in advance are as follows:

- Establish close working relationships with management, legal counsel, external EDP auditors, and others to ensure that the internal IS auditors are made aware of any suspicious situations.

- Schedule periodic reviews, including security audits (or surprise audits), for all significant financial applications.

- Ensure that there is a rotation of personnel functions in user and IS areas so that individuals do not have undue control over systems.

- Periodically take inventory of assets to ensure that they are protected against misappropriation.

- Ensure that passwords and security codes are revised on a timely basis, and especially when key IS personnel leave the organization.

- Establish procedures by which employees can anonymously report any suspicious situations to the internal IS auditors for follow-up.

- Ensure that when improprieties are discovered they are properly investigated and appropriate corrective action is taken.

- Ensure that effective termination procedures are employed to prevent improprieties by terminated employees.

- Ensure that adequate controls are being incorporated and that all control procedures are consistently and effectively being employed.

- Ensure that appropriate access controls are utilized to limit access to information systems on a need-to-know basis.

- Utilize exception reporting techniques to identify unusual transactions for subsequent audit follow-up.

THE *IS* AUDITOR AND A COMPUTER FRAUD SITUATION

At some point in the career of an IS auditor, he or she will possibly encounter a fraud situation despite countless deterrents. He or she may discover it during the normal course of auditing, or when asked by management to investigate a suspected fraud or when asked to gather supporting evidence to determine the extent of a particular fraud and prosecute the perpetrators.

Regardless of the original means of detection, once a fraud situation surfaces, the IS auditor should develop a coordinated workplan for dealing with it [Gallegos, et. al., 1987]. The participants during the planning process should include appropriate members of management, the director of information systems, the corporate legal counsel and the *IS* auditor. Each should be assigned specific tasks to perform. The *IS* auditor must carefully extend the scope of his or her investigation to ensure that the entire fraud is uncovered and appropriate measures are taken to prevent its recurrence.

From a technical perspective, the techniques of controls testing and evidence collection posed for dealing with the audit environment are equally effective when dealing with fraud investigations. The fraud situation presents a more focused objective and narrower perspective than the typical audit situation. However, from a management perspective, an *IS* auditor must often deal with highly volatile issues under extreme time pressures while constantly under management's close scrutiny. Sometimes, discretion may be required should management choose not to publicize the suspected fraud. The decision to prosecute, reward or chastise the perpetrators may not be made until the investigation is completed. Under all conditions, the *IS* auditor should keep a daily log of all activities related to the investigations and document all evidence and findings in detail [ISACA, 1994].

The role of the auditor in fraud proceedings should essentially be that of an investigator working for upper management and applying technical training and proficiency as an auditor [ISACA, 1994]. It is inappropriate for the auditor to negotiate with the perpetrator or other personnel, discuss proceedings with other company personnel or outsiders or decide the course of action that the company should pursue in the situation. The auditor is bound, however, to recommend that management consider seeking legal aid if evidence indicates computer fraud.

CONCLUSION

The number of cases of computer fraud has increased, substantially so with Internet, and the methods are getting more sophisticated [Alexander, 1996; Stallings, 1995]. The *IS* auditor must develop an effective procedure for dealing with fraud. Aside from serving as an effective deterrent and possessing the technical expertise to prevent fraudulent activities, the auditor plays a vital role in the investigation of frauds when they do occur. Significantly, it is elemental that the auditor enlist the aid of management or outside expertise, since it is most important to deal with the situation expeditiously once a fraud is suspected. In retrospect, the message herein lies in that despite the continuing efforts of *IS* auditors and computer security experts, there still exists a need for greater awareness of computer fraud prevention procedures and an innate desire to keep our information systems safe and secure.

REFERENCES

Alexander, M. (1996). *The Underground Guide To Computer Security.* Addison-Wesley Publishing Company.

Amoroso, E. (1994). *Fundamentals Of Computer Security Technology.* Prentice-Hall International Editions.

Chambers, A.D. and Court, J. M. (1988). *Computer Auditing.* Pitman.

Cooper, A.J. (1988). *Computer And Communications Security.* Macmillan.

Gallegos, F., et.al. (1987). *Audit And Control Of Information Systems.* South-Western Publishing Company.

Information Systems Audit & Control Foundation (ISACA) (1994). *General Standards For Information Systems Auditing & Statements On Information Systems Auditing Standards.* ISACA.

Mullen, J.B. (1990). *The Practitioner's Guide To EDP Auditing.* NYIF Corp.

Pfleeger, C.P. (1989). *Security In Computing.* Prentice-Hall International Editions.

Porter, T. and Perry, W.E. (1984). EDP: *Controls and Auditing.* Kent Publishing Company.

Schwitzer, J.A. (1987). Computer *Business And Security: The New Role For Security.* Butterworth Press.

Stallings, W. (1995). *Network And Internetwork Security: Principles & Practice.* Prentice-Hall International Editions.

Watne, D.A. and Turney, P.B.B. (1990). *Auditing EDP Systems.* Prentice-Hall International Editions.

Weber, R. (1988). EDP Auditing: *Conceptual Foundations And Practice.* McGraw-Hill International Editions.