https://doi.org/10.48009/1_iis_2011_206-212

Issues in Information Systems

Volume XII, No. 1, pp. 206-212, 2011

AN ANALYSIS OF COMPUTER FRAUD: SCHEMES, DETECTION, AND OUTCOMES

Sandra Welch, University of Texas at San Antonio, sandra.welch@utsa.edu
Tom Madison, St. Mary's University, tmadison@stmarytx.edu
Orion J. Welch, St. Mary's University, owelch@stmarytx.edu

ABSTRACT

As more and more organizations' financial transaction systems are information system based, perpetrators of financial crimes must often circumvent accounting information system internal controls to commit their crimes. The ability of internal audit functions to audit information system internal control implementation and execution is receiving increased emphasis both in education and practice. This paper examines whether computer crime is more difficult to detect and investigate than traditional schemes. The study presents a detailed analysis of the ways the computer was used to assist the perpetrator in 72 cases. The study also examines differences between the computer fraud cases and 99 fraud cases without computer involvement. The fraud information was collected through the use of an electronic survey voluntarily completed by members of a professional accounting association in south Texas. The survey consisted of 73 questions that provided detailed information about the victim organization, perpetrators, fraud schemes, detection, investigation, and outcomes. The results of the study will be useful to accounting information systems professionals, fraud examiners, and auditors.

Keywords: Accounting Information Systems, Internal Controls, Computer Crime, Fraud Investigation, Forensic Accounting, Fraud Auditing.

THEORETICAL DEVELOPMENT

According to the Institute of Internal Auditors [16], an employee, outside individual, or a party representing another entity perpetrates a fraud against an organization for direct or indirect personal benefit. In general, the perpetrator conceals or misrepresents events or data, or makes false claims. Although no single study provides a comprehensive theory of fraud, many do offer at least some insight into the complexities of this important issue. Several facets of fraud in general may apply to fraud committed through use of the computer.

The Victim

Inappropriate signals from the organization's leadership may be perceived as condoning or even encouraging unethical behavior [5, 12, 21, 24]. Second, inadequate or missing formal deterrence mechanisms within the unit may exist [7, 9, 10, 12, 14, 21, 23, 24, 25, 28, 29]. These factors suggest that certain environments may be conducive to frauds.

The Perpetrator

Albrecht, Albrecht and Albrecht [1] state that 'every fraud perpetrator faces … perceived pressure,' and that while most involve a financial pressure to perform, 'beat the system,' or frustration can also provide motivation. Cressey [10] notes that a perpetrator must exhibit not only an inherent ethical weakness, but also must possess a structural knowledge of the fraud target for the successful commission of a fraud to result and that the perpetrator will also attempt to rationalize the fraudulent act. Personal characteristics of fraud perpetrators include age, sex, and position in the organization. Middle-aged [6, 32], married [28, 33] males [6, 11, 13, 28] have been linked with a propensity to commit fraud. In addition, the magnitude of the illegal advantage achieved has been found to be highly correlated with both the positions held by the perpetrators within the victim organizations [19, 34] and the specific level of responsibility involved [12, 18].

Fraud Opportunities and Duration, and Red Flags and Detection

Within accounting literature, inappropriate management attitudes (particularly toward internal controls) have frequently been linked to fraud and its detection [15, 31]. The Committee of Sponsoring Organizations of the Treadway Commission [8]states that management concerns for effective internal control must "permeate the organization", and that "support from the board of directors and senior management is needed to get the right focus, resources and attention" for enterprise risk management. Controllers responding to a survey agreed that ethically oriented behavior in an organization is a broad-based management responsibility and that as part of a management team, controllers themselves had to model such behavior [17]. On the basis of a comprehensive review of the literature, Hooks, Kaplan and Schultz [15] suggested that codes of conduct have little impact if not enforced. Thompson [30] noted that when top management displays "willful ignorance, [it] sends a powerful message that it will tolerate [wrongdoing]." Cressey [10] noted that frauds will occur in an organization when the perpetrator, who lacks the moral strength to resist temptation, is offered an opportunity to commit an offense. Entities that display lax attitudes toward controls offer such opportunities.

Barnard [4] suggested that top management is responsible for encouraging cooperation in achieving a moral purpose through moral behavior. A strong corporate awareness of the danger of fraud should encourage support of tight internal accounting controls and create a greater sensitivity to the risk factors commonly associated with the commitment of fraud. Additionally, these dynamics should discourage unethical activity and encourage the reporting of such illicit activities when they do occur. In contrast, organizations that display less awareness to the danger of fraud will provide inadequate support for internal controls. Such an environment might allow, or even encourage, unethical activity by some and discourage the reporting of suspicious activities by others. In sum, positive or strong ethical attitudes modeled by management encourage employee conscientiousness, while lax attitudes cause reduced employee conscientiousness. The Sarbanes-Oxley Act [26] established legal responsibility of corporate governance management for internal controls, and the resultant Statements on Auditing Standards 109 in 2006 and 115 in 2008 provided rules regarding this for the external auditor. (These Statements on Auditing Standards were subsequently used as the source for the Public Company Accounting Oversight Board professional standards 314 and 325, respectively [23, 25].) The integrity of an organization's internal control structure, coupled with the effectiveness of the audits (both internal and external) conducted on the organization and its programs, can have a significant impact on the likelihood that irregularities will commence, and if they do occur, that they will be detected on a timely basis [14]. Specifically, open channels of communication [14, 15] proper internal controls [18, 20] and a pool of sensitive personnel [12, 22] create important aids to detection. The importance of internal controls as a fraud deterrent was further emphasized following the corporate failures of the early 2000's, when the Sarbanes-Oxley Act [26] required that management must assess and make representation about the strength of its internal controls and external auditors must separately attest regarding the soundness of the internal control structure of the auditee.

Seetharaman , Senthilvelmurugan, and Periyananayagam [27] examined asset misappropriation frauds involving the use of computers. The scope of their research focused on computer fraud and abuse that involves breaches of physical, personnel, communications, and operations securities. They noted that given the pervasive use of computer technologies in organizations, computers would increasingly be used to commit fraud. They noted that data and information in computerized systems were less secure than those in manual systems. They recommended that, to contain computer fraud, organizations should strive to implement a broad range of interventions, including limiting access to building, rooms or computer systems. They also noted that to investigate frauds involving computers, investigators must have knowledge not only of transactions but also of systems.

The Controller's Report [2], a professional publication, cited the contribution of a corporate computer security lapse to a multimillion dollar fraud as a significant element of an SEC finding. Controllers were urged s to enlist IT managers in their efforts to combat fraud. This step was considered critical, since IT managers often view themselves as builders of computer systems, not as stewards of how the systems are used. Controllers were also advised to encourage IT managers to contact them, particularly if they work at far off subsidiaries, when there were irregularities that suggest someone was "cooking the books." Symptoms identified included constant rerunning of monthly accounting reports, suggesting that someone was playing with the numbers; non-systems people involved in the nitty-gritty aspects of report generation; and overridden access controls.

Outcome of the Fraud Investigation

Shapiro [29] notes that when a perpetrator can mask illicit behavior, the fraud examination may be both very time-consuming and only partially successful. In many fraud examinations, investigators may need to link several seemingly unrelated situations in order to confirm the existence of fraud. The discrete nature of transactions, coupled with the power commanded by a given perpetrator, may allow the perpetrator to hinder or, in some instances, even block any investigations that do take place.

Bainbridge [3] discussed the Fraud Act of 2006, a revision of English law that recognized the changing landscape given the pervasiveness of computers and the creativity of their users. The Act improved the ability to prosecute frauds involving the use of computers. The need in English law to prove deception was removed with regard to frauds involving computers. In addition, the law included unauthorized access and unauthorized modification of computer material as offences. Fraud, whether or not involving the use of a computer, is intended to gain a direct or indirect advantage through deception. This paper examines aspects of frauds involving the use of computers to provide practical insights.

METHOD

The study presents a detailed analysis of the ways the computer was used as a tool to commit or cover up a fraud. The study also examines differences between 72 computer fraud cases and 99 fraud cases without computer involvement. The fraud information was collected by an electronic survey distributed to the membership of a professional accounting society in south Texas. The lengthy survey consisted of 73 questions that provided detailed information on the victim organization, perpetrators, fraud schemes, detection, investigation, and outcomes. Some of the questions related to schemes had multiple components. Survey requests were sent to approximately 2,000 professional accountants in the summer of 2010. In order to successfully complete the survey, the accountants had to have significant detailed knowledge of a fraud committed in an organization. A total of 171 complete fraud case reports meeting the criteria were received. A number of partial responses were also received but did not have the sufficient scheme related information to be included in the results. The usable response rate was approximately 8%. This response rate percentage might be misleading because the number of accountants surveyed that had detailed knowledge of a fraud case would be a subset of those receiving the survey request. Eighty-eight percent of the reported fraud cases occurred or were on-going during the last ten years. The remainder of the cases occurred during the 1990's. A copy of the survey is available upon request.

RESULTS AND DISCUSSION

The perpetrators were able to use the computer systems of the organization in the following schemes to assist in or conceal their frauds. The respondents were asked to check all that apply when responding to this question, so multiple schemes could have occurred on an individual case. The following table presents, in descending order, the number and percentage of cases where computer misuse occurred, when that scheme was checked.

Table 1. IS Fraud Schemes

Scheme	**#**	**%**
Fictitious entry	38	53
Unauthorized transfer	29	40
Fictitious reimbursement	24	33
Fictitious invoice	18	25
Fraudulent account	13	18
Unauthorized internal access	12	17
Modification of database	08	11
Inflated invoice	07	10
Unauthorized external access	03	04
Unauthorized downloads o	02	03

As described in Table 1, the four most commonly used schemes directly relate to methods of fraudulently accessing and obtaining cash. In many of the cases, the perpetrators used multiple schemes to commit their crimes. These frequently include schemes involving creation of fictitious entries of various types and unauthorized transfers of funds. Violations of internal and external access were not as frequent as might be expected. The crimes were committed by people who had access to the systems and were able to exploit internal control weaknesses in the transaction control systems. Which weaknesses were most exploited are identified in the following table.

Table 2. Internal Control Weakness

Weakness	**Mean (1 to 7 scale)**
Separation of duties	5.89
Proper authorization	5.70
Periodic checks and balances	5.69
Lax attitudes	5.22
Asset safeguards	5.13
Required documentation	4.94
Competent personnel	3.52

Table 2 indicates the degree to which a weakness in internal control was exploited to commit the crime. The higher the rating the more significantly the weakness was viewed by the respondent as a contributing factor to the fraud. T-tests results on the sample means that were performed to examine if reported differences in the means were significant. This would help internal auditors prioritize their fraud prevention measures and AIS controls. At the .05 level, lack of separation of duties was significantly higher than asset safe guards, required documentation and lack of competent personnel weaknesses. Weaknesses in proper authorization and failure to perform periodic checks and balances were more significant contributing factors than missing required documentation and lack of competent personnel. Finally, lax attitudes towards rules and policies by management/employees, lack of asset safeguards, and required documentation were significantly more important than lack of competent personnel. The fact that lack of competent personnel was significantly lower in respect to all other internal controls may indicate that it may become a a significant factor only if other internal weaknesses exist. Pearson correlations were run to test for correlations between the weaknesses in the IS fraud cases. There was significant correlation at the .05 level between all the variables. This indicates that in IS fraud cases it is likely that multiple control weaknesses will exist to enable the commission of the fraud. In the reported cases, the lack of authorization procedures and missing required documentation were almost always paired together. This is particularly noteworthy since the highest percentage of schemes used in the computer-enabled cases was related to fictitious entries. The study also examined the differences between cases where the computer was used to commit or enable the crime versus those that did not involve the information systems of the organization.

Table 3 – Demographics of Victim Organization and Perpetrators

Victim Characteristics	**IS**	**Non IS**	**Sig.**
# Employees (Median)	150	150	
Publicly traded (%)	22	17	ns
Internal audit (%)	29	35	ns
External audit (%)	60	65	ns
Loss amount (Median)	$250K	$80K	.01
Loss amount (Average)	$1.82M	$.56M	.06
Perpetrator Characteristics	**IS**	**Non IS**	**Sig.**
Male (%)	45	51	ns
Age (Avg.)	41	41	ns
Married (%)	62	78	ns
Education			
High School (%)	41	37	ns
College (%)	44	51	ns
Graduate school (%)	16	12	ns
Collusion (%)	28	27	ns

Table 3 shows information systems frauds were larger and on the whole, committed in organizations with less audit pressure. The demographics of the perpetrators and the likelihood of collusion in the commission of the fraud was similar for both IS and non IS implemented frauds. The only surprise in relation to the literature on fraud was related to gender. This study found that the primary perpetrator was equally likely to be male or female.

Table 4. Duration and Schemes

	IS	Non IS	Sig.
Duration (years)	3.05	2.07	ns
Scheme characteristics (1-7 scale)			
Common	3.65	4.03	ns
Complex	3.00	1.80	.00
Continual	5.57	4.73	.03
Easy to detect	4.23	4.93	.04

Table 4 indicates how the respondents viewed four separate scheme characteristics. The higher the rating the more common the scheme, the more complicated the scheme, the more repetitive the scheme, and the easier it was to detect. The differences between scheme characteristics in IS fraud cases and non IS cases were analyzed using t-tests and also reported in Table 4. The results supported that IS related schemes were significantly more complex in nature (.00), were more continuously repeated (.03), and more difficult to detect (.04). The dimension of rare versus common was not significant (.31). While the average duration of the IS frauds was longer, the difference was not significant.

Table 5. Investigation and Outcome

Investigation by (%)	IS	Non IS
CFE	5	4
Internal audit	22	13
External audit	22	9
Security	5	2
Outside agency	50	36
Termination	83	67
Civil prosecution	10	11
Criminal prosecution	36	24
Settled	32	21
Pending	14	8

Table 5 illustrates that internal and/or external auditors were more likely to be involved in investigation of the computer related frauds. This was true even though the victim organizations involving the non computer aided frauds had slightly higher percentages of having internal and external auditors (see Table 3). Additionally, the percentages of cases in which outside agencies were used in the investigations were higher in the computer cases. This might be related to the fact the IS enabled frauds resulted in larger losses, which would trigger the use of law enforcement involvement. The number of cases prosecuted or pending for the IS related cases was 50% versus 32% for the non IS cases. Also, terminations were higher in the IS related cases. This may be related to the lower median and average loss amounts involved in the non IS cases and the fact more of the non computer frauds were handled within management channels without involving audit departments and outside agencies.

SUMMARY AND CONCLUSIONS

Primary schemes used to commit the information system assisted frauds involved various types of fictitious entries. The primary internal control weaknesses exploited included lack of separation of duties, lack of proper authorization, and lack of periodic checks and balances. Single control weaknesses were seldom the problem. The respondents in the study frequently identified multiple internal control weaknesses as contributing factors. Contrary to previous studies, women were equally involved as perpetrators as men. Also collusion was equally present in the information systems and non information systems frauds. The study found that information systems frauds involved more complicated schemes, were more difficult to detect, were more likely to involve repetitive transactions, and

perhaps as a result, incurred significantly higher losses. Information systems frauds were also more likely to require auditors and outside expert involvement in the investigation.

From an accounting information systems perspective, this study suggests that technology based control systems that focus primarily on access controls may be insufficient. A combination of management controls and oversight together with technology controls and oversight together with technology safeguards may be more effective in making fictitious entries more difficult. Additionally, audit software with business intelligence components that identify anomalies in transactions might be useful. Finally, while the Sarbanes-Oxley Act, specifically targets financial statement frauds, its suggestion of using specialized audits to detect weaknesses in internal controls systems might be appropriate for misappropriation frauds as well.

REFERENCES

1. Albrecht, W. S., Albrecht C., and Albrecht, C. C. (2008). Current trends in fraud and its detection. *Information Security Journal: A Global Perspective*, 17, 2-12.
2. Anonymous. (2000). Computer fraud. *The Controller's Report.* February. Retrieved from Accounting and Taxation Periodicals http://proquest.com.libweb.lib.utsa.edu/. Document ID: 50833458.
3. Bainbridge, D. (2007). Criminal law tackles computer fraud and misuse. *Computer Law & Security Report*, 23, 276-281.
4. Barnard, C. (1938). *The Functions of the Executive*. Cambridge, MA: Harvard University Press.
5. Coleman, J. (1987). Toward an integrated theory of white-collar crime. *American Journal of Sociology*, 93(2), 406-439.
6. Collins, J., and Schmidt, F. (1993). Personality, integrity, and white collar crime: A construct validity study. *Personnel Psychology*, 46(2), 295-311.
7. Committee of Sponsoring Organizations of the Treadway Commission (COSO). (1992). *Internal control—integrated framework*. Harborside, NJ: American Institute of Certified Public Accountants.
8. Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2011). *Embracing enterprise risk management: Practical approaches for getting started*. www.coso.org.
9. Cornish, D., and Clarke, R. (1987). Understanding crime displacement: An application of rational choice theory. *Criminology*, 25(4), 933-947.
10. Cressey, D. (1953). *Other People's Money*, NewYork: The Free Press.
11. Daly, K. (1989). Gender and varieties of white- collar crime. *Criminology*, 27(4), 769-793.
12. Guercio, J., Rice, E. and Sherman, M. (1988). Old fashioned fraud by employees is alive and well: Results of a survey of practicing CPAs. *The CPA Journal*, 58(9), 74-77.
13. Hollinger, R., and Clark, J. (1983). Deterrence in the workplace: Perceived certainty, perceived severity, and employee theft. *Social Forces*, 62(2), 398-418.
14. Holtfreter, K. (2005). Is occupational fraud "typical" white collar crime? A comparison of individual and organizational characteristics. *Journal of Criminal Justice*, 33, 353-365.
15. Hooks, K., Kaplan, S., and Schultz, J. (1994). Enhancing communication to assist in fraud prevention and detection. *Auditing: A Journal of Practice and Theory*, 13(2), 86-117.
16. Institute of Internal Auditors. (1985). Deterrents, detection, investigation, and reporting of fraud (*Statement on Internal Auditing Standards No. 3*), Sarasota, FL.
17. Irvine, B., and Lindsay, L. (1994). Corporate ethics and the controller. CMA Magazine, 23-26.
18. Loebbecke, J., Eining, M., and Willingham, J. (1989). Auditor's experience with material irregularities: Frequency, nature, and detectability. *Auditing: A Journal of Practice and Theory*, 9(1), 1-28.
19. Mann, K. (1992). White-collar crime and the poverty of the criminal law. *Law and Social Inquiry*, 17(2), 561-571.
20. Matsumura, E., and Tucker, R. (1992). Fraud detection: A theoretical foundation. *The Accounting Review*, 7(4), 753-782.
21. National Commission on Fraudulent Financial Reporting (NCFFR). (1987, October). *Report of the National Commission on Fraudulent Financial Reporting*. Washington, DC: Author.
22. Ponemon, L. (1994). Whistle-blowing as an internal control mechanism: Individual and organizational considerations. *Auditing. A Journal of Practice and Theory*, 13(2), 118-139.

23. Public Company Accounting Oversight Board (PCAOB). (2008). Understanding the entity and its environment and assessing the risks of material misstatements (*AU Section 314*). New York, NY.
24. Public Company Accounting Oversight Board (PCAOB). (2008). Consideration of fraud in a financial statement audit. (*AU Section 316*). New York, NY.
25. Public Company Accounting Oversight Board (PCAOB). (2008). Communications about control deficiencies in an audit of financial statements (*AU Section 325*). New York, NY.
26. Sarbanes-Oxley Act of 2002. (2002). http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/content-detail.html, July 30.
27. Seetharaman, A., Senthilvelmurugan, M., and Periyananayagam, R.. (2004). Anatomy of computer accounting frauds. *Managerial Accounting Journal*, 19 (8), 1075-1082.
28. Seidman, J. (1990). A case study of employee frauds. *The CPA Journal*, 60(l), 28-35.
29. Shapiro, S. (1990). Collaring the crime, not the criminal: Reconsidering the concept of white-collar crime. *American Sociological Review*, 55(3), 346-365.
30. Thompson, C. (1993) Fraud findings. *Internal Auditor*, 50(3): 64–65.
31. Vinten, G. (1992). The whistleblowing internal auditor: The ethical dilemma. *Internal Auditing*, 8(3), 26–33.
32. Weisburd, D., Waring, E., and Wheeler, S. (1990). Class, status, and the punishment of white-collar criminals. *Law and Social Inquiry*, 15(2), 223-243.
33. Weisburd, D., Wheeler, S., Waring, E., and Bode, N. (1991). *Crimes of the middle classes: White-collar offenders in the federal courts*. New Haven, CT: Yale University Press.
34. Wheeler, S., and Rothman, M. (1982). The organization as weapon in white-collar crime. *Michigan Law Review*, 80, 1403-1426.