MANAGERS' PERSPECTIVES ON EMPLOYEE INFORMATION TECHNOLOGY FRAUD ISSUES WITHIN COMPANIES/ORGANIZATIONS

Susan Behling, Western Illinois University, USA shaugen@uwec.edu
Kevin Floyd, Macon State College, Georgia, USA kevin.floyd@maconstate.edu
Terry Smith, Macon State College, Georgia, USA terry.smith1@maconstate.edu
Alex Koohang, Macon State College, Georgia, USA alex.koohang@maconstate.edu
Robert Behling, Arrowrock Technologies, behlingr@hotmail.com

ABSTRACT

Information Technology can be used to positively impact the development and growth of an organization, but also presents significant opportunities for fraud. In an effort to better understand these fraud issues a survey was conducted with members of the Association for Information Technology Professionals. The study found no sense of urgency to combat fraud, and from a list of 10 common fraud activities, no issue was described as critical by a majority of the respondents. Respondents also reported fraud policies are not clearly defined, fraud monitoring and detection tools are not effectively used, and fraud policies are not evenly enforced.

Keywords: IT Fraud, Organizational Fraud, Fraud Issues

INTRODUCTION

Fraud can be described as personal enrichment through deliberate misuse or misapplication of other's resources or assets. By its very nature fraud does not lend itself to being observed or measured, as almost all fraud involves attempted concealment [1]. A risk consulting company, Kroll, believes the current market downturn will provide new and increased fraud opportunities [11] leading to expanded company vulnerabilities. In an effort to better understand how managers view Information Technology (IT) fraud issues within their respective organizations, this study investigates managers' perspectives on employee IT fraud issues that have been described in the literature as important to both business and governmental operations. A survey was developed and administered to members of the Association for Information Technology Professionals (AITP), and the responses are tabulated and reported.

INFORMATION TECHNOLOGY FRAUD

Government and corporate organizations have become more dependent on information technology resources as a means of increasing employee and client access to programs and services, and in turn, generating higher revenues. While information technology systems can be beneficial tools that positively affect the development and growth of the organization, the widespread use of technology in the organization has increased the opportunities for the occurrence of computer-related criminal acts like fraud [4, 10, 3]. Increasing information accessibility heightens vulnerability and the potential for misuse of confidential data [7], and every organization faces some risk of fraud from within [17]. The typical organization loses at least 5% to 7% of their annual revenue to fraud, which is estimated to be as much as $994 billion [19, 1]. In 2003, at least $50 billion was lost to health care fraud, causing fraud management (the prevention, detection and prosecution of fraud) to come to the forefront as the nation moves towards a Nationwide Health Information Network [16]. In a 2007 report, the Federal Bureau of Investigation reported that mortgage fraud continues to be an escalating problem in the U.S., placing financial institutions at risk, and having an adverse impact on the stock markets [6]. Truer words were never spoken, and we are seeing the results today.

While employee dishonesty and fraud are clearly not new issues for business and other organizations, the increasing use of information technology and the ensuing opportunities for system penetration and manipulation can create a breeding ground for employee dishonesty [15]. Lineberry [12] suggests that to foster a culture that is information security aware, organizations need to train employees and understand their attitudes regarding sensitive information and security controls. It is important that managers recognize the opportunity for employee fraud within their organizations, factors that motivate employees to engage in fraudulent activities, and how to combat such fraudulent activities. When information systems fail, the impacts are far reaching

and can result in physical harm to humans, loss of financial resources, wasted time, and destroyed reputations [9].

Employee related fraud is a widespread problem for both government and corporate organizations. Wells [18] explained that a common element associated with most occupational fraud offenders, from the CEO to the rank-and-file employee, is that they are typically always first-time offenders. According to Todd [15], data from the Association of Certified Fraud Examiners (ACFE) showed that occupational fraud and abuse accounts for $600 billion in company losses per year in the United States. Their updated report shows it may be as much as one trillion dollars in 2008 [1].

Employee fraud can occur in organizations of any size regardless of the company's level of sophistication. The results of a study cited by Wells [18] revealed that in a sample of 12,000 employees, nearly 90% engaged in "work place deviance". The study also showed that the more dissatisfied the employee, the more likely he or she was to engage in criminal activities. Employee fraud does not occur in isolation. It is a combination of motive and opportunity. In a 2006 study conducted by the San Francisco-based Computer Security Institute, it was reported that nearly two-thirds of the 616 security professionals surveyed said that insiders account for some portion of the financial losses their organizations experience because of security breaches. In addition, thirty-nine percent of respondents attribute more than 20 percent of their organizations' financial losses to malicious insider incidents [8]. Eric Shaw, a psychologist and former CIA intelligence officer, explained that insider threats against the IT infrastructure can be among the most costly and damaging to a company's reputation. These threats are among the most feared by both government and corporate information technology security professionals [as cited in 8].

Conlin [2] reported that employees are more likely to engage in malicious activities during bad economic times. Given the current economic down turn, a recent Deloitte survey reported that two thirds of executives expect insider crime to rise in the next two years. Smith [14] used the Anomie Theory to explain employee motivation to engage in fraud related activities. The Anomie Theory states that employees with low levels of job security, power, and income have high aspirations to engage in illegal activities within the company [13]. Wells [18] further attributed insider crime to employees and executives who feel unfairly treated and seek retribution by engaging in acts of occupation fraud and abuse.

While technology systems are the primary target of insider fraud, they are often viewed by organizations as a first line of defense for controlling criminal acts by insiders. Recent advancements in fraud detection software such as the installation of fingerprinting scanners to tie activities to specific individuals, and the use of accounts payable software that can check for questionable activities, are helping companies fight theft [2]. The use of encryption technologies is needed to hide sensitive data. The technology must have the ability to immediately disable the network, system, and data access for employees that are terminated [8].

Conversely, Wells [18] explained that internal technology controls are not always enough to prevent fraud because controls are designed to provide reasonable, not absolute assurance that something bad will not happen. Furthermore, there are few controls that cannot be overridden by people with sufficient motivation.

Responding to threats of employee fraud can be a complex issue. While technology has been developed to help curtail incidents of employee fraud, employees are often able to use other technologies to circumvent the preventative measures. Kesar [10] attributed this to the fact that employees are usually more familiar with the organization's technology and they are often aware of the 'flaws' in the system, including the control of the resources associated with the system. This places employees in a better position than outsiders to engage in fraudulent activities. Employee related fraud schemes become more common and sophisticated as technology improves. Based on a recent survey, employee fraud in the financial services industry is a widespread problem that is largely attributed to advances in technology. Employees who have access to these information systems are often the ones with the tendency to steal [5]. Kesar [10] stated that the advancements in information technology in the work place have created unprecedented opportunities for the occurrence of computer fraud, particularly those committed by employees themselves. Todd [15] noted that in this age of information technology, more employees will engage in fraud related activities with the use of technology. Given the motivation and proper environment, even the best internal controls can be circumvented by employees.

The management of technology-related fraud by employees is a complex issue that will continue to be a vital element facing both public and private

organizations. To address these issues management must recognize the prevalence of employee-related fraud and understand employee motivations that lead to deviant behavior within the organization. Ultimately, the role of detecting and managing employee fraud is the responsibility of everyone in the organization.

METHODOLOGY

Survey Instrument

A ten-item, four-point Likert scale survey was developed to collect IT managers' perceptions on employee fraud issues. The first issue, unintentional acts, does not fall under the fraud definition, as fraud is the intent to deceive. However, it was included because it continues to be a significant management issue that falls into the same general area as the other nine fraud issues. The scale's descriptors were placed into four groups: "Critical", "Important", "Somewhat Important", and "Not Important". The items represented various employee fraud issues that have been described as important to both business and governmental operations. The issues are as follows:

1. UNINTENTIONAL ACTS. (Employee carelessness and accidents causing system disruption or error.)
2. OVERSIGHT. (Lack of management supervision to ensure employees follow policies and procedures.)
3. SABOTAGE. (Willful act to intentionally manipulate the financial systems.)
4. UNAUTHORIZED RESOURCE UTILIZATION. (Use of computer and technology resources for non-business or personal purposes.)
5. INSUFFICIENT INTERNAL CONTROLS. (Your organization lacks adequate or effective internal controls to detect, deter, and prevent employee fraud.)
6. ENFORCEMENT OF INTERNAL CONTROLS. (Management in your organization has lax enforcement procedures.)
7. EMPLOYEE TRUST. (Management does not adequately monitor employees.)
8. ATTENTION TO DETAILS. (Management does not pay adequate attention to activities that could lead to employee fraud.)
9. LIMITED STAFF. (Your organization has inadequate staff to detect and deter employee fraud.)
10. EMPLOYEE FRAUD IS A LOW PRIORITY. (Management does not see employee fraud as a major management concern.)

The respondents were also asked to describe what they saw as the three greatest challenges to effectively protect against employee fraud.

Survey Procedure and Subjects

Permission to administer the survey to 2000 IT managers was sought and granted from the Association for Information Technology Professionals (AITP). Founded in 1951, AITP is "the leading worldwide society of information technology business professionals and the community of knowledge". AITP "delivers relevant technology and leadership education, research and information on current business and technology issues, and forums for networking and collaboration." (See http://www.aitp.org/)

The survey was directly administered to the subjects by AITP. The subjects were assured that their participation in the study was voluntary. All subjects were 18 years or older. They were guaranteed anonymity with regard to the publication of the results. Sixty-five IT managers responded to the survey. Of the 65 responses, 17 were eliminated because of incomplete or missing data. The final total responses yielded 48 subjects.

Data Analysis

The collected data was analyzed through comparing frequency distribution of responses with the aim of categorizing the patterns of responses in each group - "Critical", "Important", "Somewhat Important", and "Not Important".

STUDY RESULTS

Demographics

Tables 1 through 5 show the demographics of the subjects. The subjects were from companies/organizations that included the major activities such as manufacturing, banking/financial services, insurance, computer software/services, health care/medical, retail, government/military, and services. The subjects were from small, medium, and large companies. These companies were regional, national, and global with limited to sophisticated information technology abilities. Their technology-based business activities included a combination of e-commerce (vendor to vendor), e-business (vendor to consumer), organizational web site, virtual private network, and outsourcing of technology development and/or support. The demographics are presented in tables 1 through 5:

	Total	**48**

Table 1: Major Activity of company/organization

	%	Count
Manufacturing	16.7	8
Banking/Financial Services	8.3	4
Insurance	12.5	6
Computer Software/Services	25.0	12
Health Care/Medical	8.3	4
Retail	4.2	2
Government/Military	12.5	6
Services	12.5	6
Total		**48**

Table 2: Number of employees in company/organization

	%	Count
1- 50	31.3	15
51- 500	14.6	7
501- 2,000	10.4	5
2001- 10,000	29.2	14
Over 10,000	14.6	7
Total		**48**

Table 3: Company/organization representation

	%	Count
Regional	47.9	23
National	22.9	11
Global	29.2	14
Total		**48**

Table 4: Rating of Information Technology at your organization

	%	Count
Sophisticated	66.7	32
Functional	29.2	14
Limited	4.2	2

Table 5: Technology based business activities found in your company/organization

Answer Options	%	Count
E-Commerce (vendor to vendor)	62.5	30
E-Business (vendor to consumer)	81.3	39
Organizational web site	83.3	40
Virtual private network	87.5	42
Outsourcing of technology development and/or support	58.3	28

Response Frequency Analysis of IT Fraud Issues

The impact to an organization that experiences employee fraud can be devastating. To better understand the challenges organizations face in detecting and managing employee fraud, this study targets individuals who are responsible for information security in various types and sizes of organizations. In the final analysis, 48 subjects responded to a survey on employee fraud issues. The subjects were asked to evaluate ten employee fraud issues from the perspective of their company or organization, ranking each issue as *critical*, *important*, *somewhat important*, or *not important*. The results of the survey are presented in Table 6.

Surprisingly, no issue was determined to be *critical* by a majority of the respondents. Employee SABOTAGE was identified as *critical* by 23 or 47.9% of the respondents. This was followed by LIMITED STAFF (18 or 37.5% of the respondents) and INSUFFICIENT INTERNAL CONTROLS (17 respondents or 35.4%). Fraud, as the result of an UNINTENTIONAL ACT, was deemed *critical* by only 6 or 12.5 % of the respondents, the lowest of the ten issues. More than 50% of the respondents indicate that OVERSIGHT (64.6%), UNINTENTIAL ACTS (64.6%), and ENFORCEMENT OF INTERNAL CONTROLS (54.2%) are *important* but not *critical* issues.

As stated earlier, the role of detecting and managing employee fraud will be the responsibility of the organization. It is through the use of preventive

measures, monitoring, and detection, and enforcement of policies and procedures that companies and organizations can limit potential damage by employee sabotage or accidental acts. The respondents identified INSUFFICIENT INTERNAL CONTROLS (35.4%) and LIMITED STAFF (37.5%) as *critical* issues they face in preventing, monitoring, and detecting employee fraud. The lack of OVERSIGHT (64.6%) and ENFORCEMENT OF INTERNAL CONTROLS (54.2%) were identified as *important* to the enforcement of the companies or organizations preventive measures. Management has a responsibility to create a corporate culture that addresses employee fraud. The issue, EMPLOYEE FRAUD IS A LOW PRIORITY, ranked number four as both *critical* and *important*.

Table 6: Response Frequency of IT Fraud Issues

Answer Options	Critical	Important	Somewhat Important	Not Important
SABOTAGE	47.9% (23)	27.1% (13)	20.8% (10)	4.2% (2)
LIMITED STAFF	37.5% (18)	(37.5% (18)	20.8% (10)	4.2% (2)
INSUFFICIENT INTERNAL CONTROLS	35.4% (17)	41.7% (20)	20.8% (10)	2.1% (1)
EMPLOYEE FRAUD IS A LOW PRIORITY	27.1% (13)	39.6% (19)	27.1% (13)	6.3% (3)
ATTENTION TO DETAILS	25.0% (12)	47.9% (23)	25.0% (12)	2.1% (1)
OVERSIGHT	20.8% (10)	64.6% (31)	12.5% (6)	2.1% (1)
ENFORCEMENT OF INTERNAL CONTROLS	20.8% (10)	54.2% (26)	22.9% (11)	2.1% (1)
EMPLOYEE TRUST	18.8% (9)	43.8% (21)	31.3% (15)	6.3% (3)
UNAUTHORIZED RESOURCE UTILIZATION	18.8% (9)	33.3% (16)	37.5% (18)	10.4% (5)
UNINTENTIONAL ACTS	12.5% (6)	64.6% (31)	20.8% (10)	2.1% (1)

Analysis of Open Ended Questions

Respondents were asked to describe what they saw as the three greatest challenges to effectively protect against employee fraud. While wording and phrasing differed, responses could be grouped into three major challenges:

- Companies and organizations need to develop and communicate policies and procedures to address employee fraud. Comments from the respondents suggest that policies are not clearly defined, communicated, explained, nor enforced. To be specific, "management does not see employee fraud as a major management issue".

- Although many monitoring capabilities and fraud detection controls are in place, they are not effectively used because of limited staff, shrinking budgets, and time constraints. Additionally, companies or organizations do not like to be seen as a "Big Brother".

- Policies are not enforced. A lack of or uneven support from management results in the inconsistent application of punishments. When an act of fraud is detected and confirmed, punishments need to be "...enforced fairly but decisively".

DISCUSSION

Even with the continual fraud warning articles being published in the literature and popular press, the results of this survey did not find a sense of urgency among the responding managers to address fraud and information security issues. The objective of fraud is to deceive, and we suspect that in many organizations the objective has been successfully met by people perpetrating a variety of frauds. The message does not seem to be getting to management about the serious risks and the potential for substantial financial losses to organizations from fraud and information manipulation.

The management strategy of making all employees

aware of fraud risks, and having each and every employee be responsible for protecting the organization from fraud, does not seem to be filtering down to the operational levels. The results of this survey tell us that there is more that needs be done in combating fraud, in educating managers, and ultimately in protecting the financial and other resources of business and government.

A number of organizations such as Kroll [11] collect relevant fraud data as to industries, amounts, techniques and such. This information is useful, but if we are to accept the premise that the operational manager is ultimately the first line of defense in the prevention and detection of fraud, then manager's attitudes play a significant role in determining how effective they will be in combating fraud. This study points out that there is no sense of urgency in the surveyed population, which is modest in size. It would be useful to validate the survey results with a larger and/or more comprehensive study. We have shown that there is the need to pursue this issue further, and to gather and analyze more definitive data. Perhaps a different management population such as financial, manufacturing, or operations, would yield useful survey results. One thing is certain; fraud is not going away, especially in these difficult economic times.

REFERENCES

1. ACFE (2008). 2008 Report to the nation on occupational fraud & abuse, *Association of Certified Fraud Examiners*.
2. Conlin, M. (2009). Catching Corporate Crooks. *Business Week*, Retrieved February 23, 2009, from http://www.businessweek.com/print/magazine/content/09_07/b4119052687973.htm
3. CSI/FBI: Computer Crime and Security Survey. Retrieved February 23, 2009 from http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf
4. Ernst & Young: Global information security survey (2004). Retrieved February 22, 2009 from http://www2.eycom.ch/publications/items/saas_global_security_survey_2004/en.pdf
5. Esola, L. (2007). Employee fraud is key concern for financial institutions. *Business Insurance*, *41*(35), 11-12.
6. FBI (2008). 2007 Mortgage fraud report. Retrieved March 1, 2009 from http://www.fbi.gov/publications/fraud/mortgage_fraud07.htm
7. Fraud Investigators. (2007). Incident response and fraud investigation. The role of the information technology auditor, retrieved March 1, 2009 from http://www.fraudinvestigation.co.za/fraud_technology.htm
8. Greenemeier, L., & Gaudin, S. (2007). The threat from within – Insiders represent one of the biggest security risks because of their knowledge and access. To head them off, consider the psychology and technology behind the attacks. *Insurance & Technology*, *32*(2), 38-41.
9. Johnson, D. G. (1994). *Computer ethics*. Upper Saddle River, NJ: Prentice Hall.
10. Kesar, S. (2006). Legal issues alone are not enough to manage computer fraud committed by employees. *Journal of International Commercial Law and Technology*, *1*(1), 25-40.
11. Kroll (2009). Global fraud report, retrieved March 3, 2009 from http://www.kroll.com/fraud
12. Lineberry, S. (2007). The human element, the weakest link in information security, *Journal of Accountancy*, *204*(5), 44-49.
13. Riah-Belkaoui, A., & Picur, R. D. (2000). Understanding fraud in the accounting environment. *Managerial Finance*, *26*(11), 33-41.
14. Smith, A. D. (2005). Accountability in EDI systems to prevent employee fraud. *Information Systems Journal*, *22*(2), 30-38.
15. Todd, K. J. (2004). Using digital evidence to ferret out the dishonesty employee. *Employee Relations Law Journal*, *30*(2), 13-22.
16. US Department of Health and Human Services. (2005). Report on the use of health information technology to enhance and expand health care anti-fraud activities, retrieved March 1, 2009 from http://www.hhs.gov/healthit/documents/reportontheuse.pdf
17. Wells, J. T. & Gill, J. (2007). Assessing fraud risk, *Journal of Accountancy*, *204*(4), 63-65.
18. Wells, J. T. (2001). Why employees commit fraud. *Journal of Accountancy*, *191*(2), 89-91.
19. Wells, J. T. (2007). What is your fraud IQ?, *Journal of Accountancy*, *204*(6), 56-57.