Management and Political Sciences Review
Volume: 1 Issue: 1 Year: 2019 pp: 81-92

Impact Of Accounting Information Systems (Ais) On Fraud Detection

Arş. Gör. Güneş TOPÇU[1]

ABSTRACT

This paper examines whether fraudulent activities in financial statements have decreased with the use of computerized accounting information systems (CAIS) and what can be done by accounting information systems (AIS) to decrease fraud in financial statements. Studies show that using computerized accounting information systems do not decrease fraud each time because top management instead of lower level employees is the one who commits crimes. Although enterprise resource planning systems (ERP) provide controls such as segregation of duties, they may not be sufficient to detect fraud. Instead, data mining techniques such as neural networks, decision trees and Bayesian Belief Networks may be used.

Keywords: Internal control, fraud, computerized accounting information systems, ERP

JEL Classification: M40, M41

Muhasebe Bilgi Sistemlerinin Hile Tespit Etmedeki Rolü

ÖZET

Bu çalışma, finansal tablolardaki hileli faaliyetlerin bilgisayarlı muhasebe bilgi sistemlerinin kullanılmasıyla azalıp azalmadığını ve finansal tablolardaki hilelerin azaltılması için neler yapılması gerektiğini incelemektedir. Yapılan çalışmalar, bilgisayarlı muhasebe bilgi sistemlerinin hileyi her defasında azaltmadığını göstermektedir; çünkü, suçları işleyenler her zaman alt kademedeki çalışanlar değil yönetim kademesindeki çalışanlar da olabilmektedir. Kurumsal kaynak planlaması sistemleri görev ayrılığı gibi kontrolleri sağlamasına ragmen, hileyi tespit etmede yeterli olmayabilirler. Bunun yerine, sinir ağları, karar ağaçları ve Bayes inanç ağları kullanılabilir.

[1] Çanakkale Onsekiz Mart Üniversitesi, Siyasal Bilgiler Fakültesi, İşletme Bölümü, gunestopcu@comu.edu.tr

Anahtar Kelimeler: İç denetim, hile, bilgisayarlı muhasebe bilgi sistemleri, ERP

JEL Sınıflandırması: M40, M41

1 . INTRODUCTION

Business firms are concerned with fraud since it directly affects profit. Fraud costs millions of dollars to business firms (Best et al., 2009). According to The Coalition Against Insurance Fraud estimates, at least $80 billion fraudulent claims are made in U.S. annually.

Fraud is defined as 'the theft, concealment, and conversion to personal gain of another's money, physical assets, or information' (Turner & Weickgenannt, 2013). For example, an employee that changes cash records in the system to conceal his cash theft from the company is a fraud (Turner & Weickgenannt, 2013). Not only money and physical assets but also information stealing is in fraud context. For example, stealing valuable information about customers of a company and sharing this information with others is a type of fraud. In every firm, errors may occur which are done unintentionally. What differentiates fraud from error is that it is an intentional act such as sabotage, computer fraud or embezzlement.

In the literature, there is a concept named "fraud triangle" which stems from Donald Cressey's hypothesis (Cressey, 1973: 30). Fraud triangle has three legs: pressure, opportunity and rationalization. In order an individual to commit fraud, three of these factors should be simultaneously present. Pressure is the first factor that inspirits the crime. Perpetrator may have some financial problems that he cannot solve through legitimate means. For example, a family member may have a fatal illness whose treatment requires a lot of money, he may not pay his bills or he may want to create smooth earnings to gain investment confidence. All of these factors create pressure on the individual and he begins to consider committing a fraudulent activity such as stealing cash or falsifying financial statements. The second leg is opportunity. Opportunity is the ability to commit fraud. Penetrator can disguise the crime through abusing the trust he creates during his employment in the company. He perceives risk of being caught low so that he commits crime. In the rationalization part, penetrator tries to justify his crime. He believes that he is innocent and circumstances lead him to commit such a crime. Therefore, he convinces himself in a way that makes his act acceptable.

Companies may prevent fraudulent activities through CAIS. Basically, CAIS help companies to increase productivity and eliminate data redundancy. Computer software namely ERP systems such as SAP, Oracle and Peoplesoft are used by companies to ease data management and for controlling purposes. ERP systems, a subset of accounting information systems (AIS), are a set of software applications

that are designed to integrate the processes and functions within a company (Daoud & Triki, 2013: 13). With the help of those systems, occurrence

of fictitious and inaccurate transactions are minimized (Sharma, 2004), data is updated and efficiency increases. Another benefit of ERP is its support in the prevention of fraud. Auditors continuously monitor those systems to prevent fraudulent financial reporting. Besides, auditors use not only ERP systems but also computer assisted auditing techniques (CAATs) such as ACL and IDEA to prevent fraud (Fong, 2004). These computer assisted auditing techniques provide auditors to sort and summarize data, select sample, and make calculations from large datasets in ERP systems in a more accurate way (Fong, 2004). However, whether using computerized systems decreased or increased fraud is a question in mind. According to KPMG 1998 Fraud Survey, while average loss from false financial statements was $765,000 in the 1994 survey, it increased to $1,239,000 in the 1998 survey (Cullinan & Sutton, 2006). Studies show that using computerized accounting information systems do not decrease fraud each time because top management instead of lower level employees is the one who commit crimes. Besides, since focus shifts from segregation of duties[2] to greater access, greater risks of fraud occur (Hunton et al., 2001). The aim of this paper is to review whether fraud in financial statements decreased with the computerized accounting information systems and what can be done by AIS to decrease fraud.

This paper is composed of four sections. Section 2 reviews the literature. It basically gives information about computer fraud cases, its comparison with manual fraud cases, ERP's importance in detecting fraud, financial statement frauds and employee types that involve in fraudulent activities. Section 3 mentions whether ERP is enough to reduce fraud, and new auditing procedures based on information systems that decrease fraud. Section 4 concludes the paper.

2 . FRAUDULENT ACTIVITIES AND AIS

When compared with traditional manual systems, computerized systems have many benefits. For example, they reduce human error associated with manual controls, save time for businesses and allows for easy data access. On the other hand, they have disadvantages as well. Welch et al. (2011) investigated whether computer crime is more easily detected than traditional fraud and how computers are used as a tool to cover up a crime. They conducted a survey, which consists of 73 questions mainly covering information on the victim organization, perpetrators, fraud schemes, detection, investigation, and outcomes. 72 computer

[2] Segregation of duties means giving different users distinct but interrelated tasks, so that a failure of one user in the system can be detected by another. For example, users who create master records should not post transactions.

fraud cases and 99 non-computer fraud cases were analyzed. Sample is composed of 2,000 professional accountants and the survey was sent in 2010 summer. Results of the survey show that fictitious entry has the highest rank with 53 % amongst the other IS fraud schemes. The other IS fraud schemes ranked in a descending order were unauthorized transfer, fictitious reimbursement, fictitious invoice, fraudulent account, unauthorized internal access, modification of database, inflated invoice, unauthorized external access and unauthorized downloads, respectively. Welsch et al. (2011) state that the first four schemes are related with fraudently accessing and obtaining cash. The crimes were conducted by perpetrators who have access to internal control systems. Weaknesses in internal control systems were exploited by these perpetrators. Main weaknesses in the internal control systems were separation of duties, proper authorization, periodic checks and balances, lax attitudes, asset safeguards, required documentation and competent personnel. They found that computerized systems frauds contain more complicated schemes and lead to more damages compared with manual systems. They also investigated demographic characteristics of perpetrators such as gender, age, marital status and education level. Contrary to other studies, they found that women are equally likely to commit crime as men. As a suggestion, they proposed that fictitious entries be detected not only primarily focusing on access controls but also on management controls, technology controls and technology safeguards. Also, they suggested using audit software with business intelligence components.

If a company has effective AIS, it can avoid fraud. One of the ways of decreasing fraud in financial statements is using ERP systems. ERP systems prevent fraud by providing controls such as segregation of duties and continuous monitoring. To give an example, sales representative may decrease price of the product more than required to sell it or to increase their relations with customers. Since all transactions are recorded and monitored in ERP systems, it is difficult to hide those transactions. Client First Business Solutions states three ways that ERP systems can prevent fraudulent activities: (1) audit tracking, (2) alerts, and (3) access restrictions. Audit tracking allows managers to monitor who accessed the system when and the usage of those documents through security audit logs. These logs record the events such as failed and successful logins, transaction entries, changes in transactions, and changes in master records (Best et al., 2009). The system gives user id, time, date, etc. For example, unauthorized payment of invoices can be prevented by this way. Alerts allow people to be notified when a data change in the system occurs if certain fields are set up in the system. For example, when clients' information such as names, addresses, and banking details change, the system sends alerts. Access restrictions do not allow penetrators to conduct operations they are not authorized to. Even if people have authorization

to do something, say, approval of the CFO is needed for all requests. Authorized personnel should have physical and remote access to system resources.

Since ERP systems integrate information coming from all departments, it will be more difficult for penetrators to commit crime and disguise their transactions. Sometimes, owners take strategic decisions for the company and they do not want to share those decisions with managers or with other owners, which will be learned if an ERP system is implemented in the company. Or, subdivisions may show resistance to implementation since they are afraid of losing their monopoly power in the company.

Fraud is done mainly by two groups: top management and lower level employees. Cullinan & Sutton (2006) state that fraud is seen as a lower level employee act. However, SEC's Accounting and Auditing Enforcement Releases (AAERs) show that financial statement fraud is mostly done by CEO or equivalent level employees. They state that, therefore, low-cost systems are built to detect lower level employee frauds, and frauds created by top management are lower to detect because of lack of control systems for top managers. According to Cullinan & Sutton's study (2006), during the period 1998 to 1999, they found 72 fraud cases, which shows an increase in the number of frauds when compared with the statistics of AAERs, which found 204 fraud cases over the period 1987 to 1997. Among 72 cases, 70.8% of frauds were committed by CEO, president or equivalent, 19.4% was done by other management, and 7% was done by division management which shows over 90% of cases were committed by senior management. It is also stated in the article that professional standards in the US say "...management is responsible for the prevention and detection of fraud" (AU 316.02) which gives authorization to the management. This leads to ignorance of fraud committed by top management.

SAS 82 in AICPA 1997 reports mainly two types of financial statements fraud: (1) misappropriation of assets, and (2) fraudulent financial reporting. The first one includes theft of assets and can easily be detected by internal control systems, but the second type is most likely to be conducted by top management and cannot be easily detected by the systems.

Literature shows that one of the reasons for fraudulent financial statements is to show continuous growth. Managers in firms which could not reach constant growth choose fraudulent actions to maintain their existing trends (Kirkos et al., 2007); Stice et. al., 1991). The article gives an example of a fraud case made in the Cendant Corporation: In order to show outsiders constant growth, manager overstated annual revenues by more than $300 million. An internal auditor in that company says: "We never thought [senior management of Cendant] were the type

that would do [that] sort of thing" (MacDonald, 1998). In Cendant case, internal control system could not detect fraud since it occurred outside the system.

Another reason for managers to prepare fraudulent financial statements may be high debt ratios (Persons, 1995). Managers are stewards and they protect the rights of owners. However, when there is high level of debt, they misrepresent financial statements to meet debt covenants and they disguise high level of risk. Bayraktar (2007) claims that managers involve in fraudulent accounting activities such as recording fictitious transactions and preparing inaccurate financial statements either (1) to show companies' financial health better than what it is now or (2) vice versa, i.e., to show it worse than what it is right now. If the firm is small, its aim is to show loss in income statement to decrease taxable income. If the firm is bigger, then its aim shifts to show itself as a profitable firm to the third parties such as to common shareholders.

In another study, Beneish (2007) found that companies which involve in fraudulent activities are newly founded, have low-stock performance, their growth depends on debt, and have deteriorating financial ratios such as decreasing asset quality and gross margin. Sutton & Kuhn (2006) gave example of WorldCom Company as a fraud act. WorldCom management manipulated expenditure to revenue (E/R) ratio at 42% during fraud years, which is lower than it should have been to meet analyst expectations. They also manipulated financial information such as revenue growth, cost reduction and profit, which led to a fraud amount of $11 billion. How they manipulated financial statements can be classified under 4 headings: (1) operating expenses were categorized as capital expenditure, (2) the value of MCI assets was reclassified as goodwill, (3) future expenses were put under write-downs of acquired assets, and (4) bad debt reserve calculations were manipulated. To solve these problems, they propose that continuous monitoring be needed and it is provided by ERP systems, specifically with SAP R/3 in that paper. The paper describes the function of SAP as so: "SAP general ledger contains all accounting information for regulatory financial reporting in two tables, GLPCT and GLPCA. The continuous assurance application, as described herein, accesses the SAP instance via RFC to extract the table data directly from the SAP database into the auditor's continuous assurance system's relational database for analysis." In another paper, SAP R/3 was mentioned as the current market leader and its segregation of duties was emphasized (Little & Best, 2003). Basically, SAP R/3 assigns profiles that supply authorizations to users which restrict entry into the system.

Therefore, if companies build an effective and efficient AIS, it may detect even managers' fraudulent activities. Using ERP systems may be beneficial since it allows continuous monitoring of fraud risk. On the other hand, ERP systems may

create problems since companies do not manage their security processes effectively. For example, configurable controls may create problem since they are the user-defined settings. Detailed review of configurable controls complements ERP's role on fraud detection.

When we look at Turkey, the number of ERP systems built increased over time. Profitability of the companies have fallen because of decreasing inflation levels over time, which affect sale prices. Therefore, companies try to decrease cost levels. Since ERP systems create efficiency in the companies, their usage adds value in the company. Bayraktar (2007) summarized accounting frauds in Turkey over the years 1990 to 2007 because it was observed that the most of fraudulent accounts occurred between those years. He investigated different kinds of frauds such as accounting fraud, corruption, fictitious export, forgery of documents, and tax evasion. He found that the most common fraud types in Turkey are inappropriate loan usage, fictitious accounts, fraudulent activities by using foreign loans, off-record transactions, and unlawful acts on off-shore accounts. Among these, Bayraktar (2007) claims that the most common fraud type is document fraud such as understatement of sales, overstatement of costs and embezzlement. Fake invoices prepared by companies are given as example: auditors of income are assigned to investigate accounts of S Film Yapım Yönetim Corporation for the year 2003. Controllers prepared 16 pages of report consisting of 53 main points. In these reports, it is written that fake invoice amount is YTL 750,000.

He found that in banking sector, inappropriate use of loan, fictitious accounts and off-record transactions are the most common fraud types. In sectors except banking, the most common fraud types are off-record transactions and document fraud. Whether a firm is a production firm or not affects fraud types as well. For example, if the firm is a production firm, then cost of goods produced is shown as higher than its real value. In publicly traded firms, a common fraud type is misstatement of financial statements, e.g., overstatement of revenues to increase share value. As it is seen, implementation of ERP systems in Turkey may have a high importance since it prevents most of the fraudulent actions aforementioned. These activities are much more related with lower-level employees, which eases ERP systems to detect fraudulent activities.

3. IS ERP ENOUGH TO REDUCE FRAUD?

As Stanton (2012) states, ERP software becomes a necessity for the complex business environment. It helps continuous monitoring of the firm activities. Otherwise, some employees realize that errors are undetected and they continue their fraudulent actions.

On the other hand, standard auditing procedures may not be adequate to cope with financial statement frauds. Although ERP systems provide controls such as segregation of duties, they may not be sufficient to detect fraud. Instead, data mining techniques such as neural networks, decision trees and Bayesian Belief Networks may be used. These techniques can establish relationships among variables that seem to be unrelated and detect correlations that humans cannot identify. Moreover, they can analyze non-numerical data such as recordings of customer service calls and qualitative information in employee files (Fong, 2014). Fong (2014) summarized usage and applications of using three data mining techniques in audit i.e., decision trees, Bayesian Belief Networks, and neural networks, respectively and what could go wrong with those techniques when used in audit. For example, decision trees may be used to audit employee files. Work history of an employee may show any kind of disputes with management that motivate employee to involve in fraudulent acts to take revenge from management. The tree first looks out the first attribute: Odd hours the employee make transactions. As a second attribute, it looks out the employee's work history. If the second attribute is the final attribute, then the branch that predicts the employees that committed fraud among the subset of employees may give accurate results when compared with the real act. The problem with decision trees is that there may be outliers, which lead to a very large tree and additional branches at each node, which have insignificant parts. These insignificant parts do not have a role in the accuracy of the decision tree. The Bayesian Belief Networks (BBN) is based on calculating conditional probabilities. When an unknown sample is chosen, probability of fraud is calculated by using occurred frauds' probability in a previous sample. Technically, "it allows for the representation of dependencies among subsets of attributes". "A BBN is a directed acyclic graph, where each node represents an attribute and each arrow represents a probabilistic dependence" (Kirkos et al., 2007). According to Kirkos et al. (2007), BBN classified 90.3% of the validation sample for fraud detection accurately. It outperformed the other two models, i.e., neural networks and decision trees. Drawback of BBN is that validation of the model is costly and time consuming, and it is the most difficult one when compared with other data mining methods (Fong, 2014). Neural networks are inspired from the functions of human brain which uses a set of interconnected nodes and they are widely used in classification and sampling (Sharma & Panigrahi, 2012). Its advantages are: (1) it is adaptive, (2) it creates robust models, (3) classification process can be changed depending on new training weights, and (4) its analytical abilities grant dealing with inconsistent data (Sharma & Panigrahi, 2012; Fong, 2014). They can be used to predict the occurrence of fraud at the management level (Cerullo & Cerullo, 1999). Besides, it can be used to find correlations among accounts and

transactions (Fong, 2014). Drawback of neural networks is its overreliance on technology. Uğurlu & Sevim (2015) first reviewed financial statement frauds and then empirically analyzed fraud risk detection in banking sector in Turkey, which includes commercial and corporate customers of banks for the year 2007. Specifically, they analyzed the use of model in commercial bank loan assessments. The aim was to minimize fraudulent activities in financial statements that cause bad loans. As a method, they proposed artificial neural network (ANN). They found that their model accurately predicts fraud risk in financial statements with an accuracy ratio of 90%. Another study for Turkey related with ANN is conducted by Küçükkocaoğlu et al. (1997). They used a model depending on ANN that predicts fraudulent activities in financial statements of companies that are registered at İstanbul Stock Exchange (İMKB). They found that this model overperforms other models such as probit model. Accuracy ratio of ANN to predict companies that involve in fraudulent activities is 86.17%.

Islam et al. (2011) argue that ERP systems cannot detect multi-transaction fraud, which limits its internal control capability. They proposed a system named fraud scenarios, which are "a set of user activities that indicate the possible occurrence of fraud". These scenarios concentrate on high-level user transactions on financial data instead of computer system events and states. Scenarios do not confirm that a fraud has occurred. Instead, it gives a possibility of fraud that has to be investigated further. They use four fraud scenarios that put collusion into individual fraud scenarios. These are redirected payment, false invoice payment, misappropriation, and non-purchase payment. They also combine ERP system logs with phone logs, and e-mail logs to detect collusion. While ERP system logs give information about daily activities of users, the other logs give information about communications of the users.

4. CONCLUSION

This paper briefly reviews the literature on financial statements fraud, the role of ERP systems on fraud detection, type of employees that involve in fraudulent activities, and other types of information systems and decision models that are used to prevent fraud. ERP systems can prevent fraudulent activities through audit tracking, alerts, and access restrictions. Although technology based control systems, i.e. computerized systems are successful at preventing fraud, they do not always decrease it since computerized systems frauds contain more complicated schemes and lead to more damages compared with manual systems.

Although ERP systems provide controls such as segregation of duties and achieves continuous monitoring, they may be insufficient to detect fraud. Other information systems such as neural networks, decision trees, and Bayesian Belief Networks can be applied to detect and prevent fraud in financial statements. These techniques are superior at establishing relationships among variables when compared with humans.

Studies show that financial statement fraud is done mainly by top management to show company's performance better than its existing performance or vice versa. Another reason is to disguise high level of debt.

As a whole, it can be said that nobody can deny the benefits of computerized accounting information systems such as ERP at detecting fraud when compared with manual systems that exist in the past. However, it should be supported with management controls and audit software with business intelligence components as it is stated at Welch et al. (2011). Companies should assign authentication, control access, use cryptography and audit trail analysis. Moreover, systems that detect fraud at management level should be developed.

REFERENCES

1. Bayraktar, A., (2007). Türkiye'de Muhasebe Hileleri Tarihi, Master's Thesis, Trakya Üniversitesi, Sosyal Bilimler Enstitüsü, Edirne.

2. Beneish, M. D., (1997). Detecting GAAP Violation: Implications for Assessing Earnings Management Among Firms with Extreme Financial Performance, Journal of Accounting and Public Policy, 16 (3), 271-309

3. Best, P. T., Rikhardsson, P. & Toleman, M., (2009). Continuous Fraud Detection in Enterprise Systems through Audit Trial Analysis, Journal of Digital Forensics, Security and Law, 4(1), 39-60.

4. Cerullo, M. J. & Cerullo V., (1999). Using Neural Networks to Predict Financial Reporting Fraud, Computer Fraud & Security, 5, 14–17.

5. Cressey, D. R., (1973). Other People's Money: A Study in the Social Psychology of Embezzlement, Montclair: Patterson Smith, N.J.

6. Cullinan, C. P. & Sutton, S. G., (2002). Defrauding the Public Interest: A Critical Examination of Reengineered Audit Processes and the Likelihood of Detecting Fraud, Critical Perspectives on Accounting, 13, 297-310.

7. Daoud, H. & Triki, M., (2013). Accounting Information Systems in an ERP Environment and Tunusian Firm Performance, International Journal of Digital Accounting Research, 1-35.

8. ERP Accounting Software: Preventing Fraud - Clients First. Retrieved September 15, 2016, from http://clientsfirst-tx.com/erp-accounting-softwarepreventing-fraud/

9. Fong, Q., (2014). Innovation of Techniques, Tools, and Technology in Audit: The Future of Electronic Audit and Fraud Detection, Term Paper, University of Waterloo.

10. Hunton J., Wright, A, & Wright S, (2001), Business and Audit Risks Associated with ERP Systems: Knowledge Differences Between Information Systems Audit Specialists and Financial Auditors, Working Paper.

11. Insurers: Victim Impact Statements. Victim Impact Statements, N.p., Retrieved December, 2016, from http://www.insurancefraud.org/the-impact-ofinsurance-fraud.htm#.VhktFOztlHw

12. Islam, A., Corney, M., Mohay, G., Clark, A., Bracher, S., Raub, T. &

Flegel, U, (2011). Detecting Collusive Fraud in Enterprise Resource Planning Systems, Chapter Advances in Digital Forensics, IFIP Advances in Information and Communication Technology, 12 (361), 143-153.

13. Kirkos, E., Spathis, C. & Manolopoulos, Y, (2007). Data Mining Techniques for the Detection of Fraudulent Financial Statements, Expert Systems with Applications, 32 (4), 995-1003.

14. Kuhn, J. R. & Sutton, S. G, (2006). Learning from WorldCom: Implications for Fraud Detection through Continuous Assurance, Journal of Emerging Technologies in Accounting, 3 (1), 61-80.

15. Küçükkocaoğlu, G., Benli & Y. K., Küçüksözen, C., (1997). Finansal Bilgi Manipülasyonunun Tespitinde Yapay Sinir Ağı Modelinin Kullanımı, İMKB Dergisi, 9 (36), 1-30.

16. Little, A.G. & Best, P.J., (2003). A Framework for Segregation of Duties in an SAP R/3 Environment, Managerial Auditing Journal, 13(5), 419-430.

17. MacDonald, E., (1998). Cendant's Former Auditor Suggests it was Misled, The Wall Street Journal, p. A3

18. Managing the Business Risk of Fraud: A Practical Guide, (2008), Publication sponsored by The Institute of Internal Auditors, Association of Certified Fraud Examiners, and The American Institute of Certified Public Accountants.

19. Persons, O., (1995). Using Financial Statement Data to Identify Factors Associated with Fraudulent Financial Reporting, Journal of Applied Business Research, 11(3), 38–46.

20. Sharma, P., (2004). Enterprise Resource Planning, 1st Edition, Aph Publishing Corporation.

21. Sharma, A. & Panigrahi, P. K., (2012). A Review of Financial Accounting Fraud Detection Based on Data Mining Techniques, International Journal of Computer Applications, 39 (1).

22. Stice, J., Albrecht, S. & Brown, L., (1991). Lessons to be learned - ZZZZBEST Regina and Lincoln savings, The CPA Journal, 52–53.

23. Turner, L. & Weickgenannt, A. B., (2013). Accounting Information Systems: The Processes and Controls, 2nd Edition, Wiley.

24. Uğurlu, M & Sevim, Ş., (2015). A Comparative Analysis on the Relative Success of Mixed-Models for Financial Statement Fraud Risk Estimation, Gaziantep University of Social Sciences, 14 (1), 65-88.

25. Welch, S., Madison, T. & Welch, O, (2011). An Analysis of Computer Fraud: Schemes, Detection, and Outcomes, Issues in Information Systems, 12(1), 206-212.