International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-7 Issue-5s, January 2019

Fraud Risk Assessment: A Tale of the Possible Corporate Executive Fraud and the Perceived Cyber-security

Geetha A Rubasundram

Abstract: ***Cyber-security is the body of technologies, processes, and practices designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access. However, the dilemma arises when the attack comes from within the organization (an insider), especially from Corporate Executives with authority. Recent cases of fraud have reflected the perceived ethical environment and values as being misleading, with stakeholders being taken for a ride by Corporate Executives who often have the capability of appearing to be dynamic, charming and adding value for the organization. The Corporate Executive reflects the typical white-collar tendency: successful, reputational with everything to lose in the event of the fraud being discovered. The methodology used is Action Research, with the researcher carrying out a pro-active Fraud Risk Assessment to investigate the perceived strength of the cyber security and relevant Information Systems, especially with the risk of collaboration between the Corporate Executive, other employees and vendors.***

Keywords: ***Corporate Executive Fraud, Cyber-security, Collaborative Fraud, Digital Evidence, Fraud Risk Assessment***

I. INTRODUCTION

In the modern business world, Information Systems (IS) play important roles integrating stakeholders, their information requirements and business operations. Regardless of industry or size, ISis relevant at every stage to improve efficiency and to reach out to stakeholders, changing the way the world does business. Amongst these systems, Enterprise Systems also known as Enterprise Resource Planning (ERP) Systems have impacted organizations (Rikhardsson & Kraemmergaard, 2006).It is a common perception that with the ERP system, errors or fraud maybe prevented and detected due to the control mechanisms and policies in place. However, the issue would be when an authorized user or an insider is a risk. Hunker and Probst (2011) discuss that the insider could have privileged access; and could even include recently discharged employees whose system credentials have not been revoked or even software developers who designed the organization systems and has access to the system. Insider threats can be very damaging to the organization, especially when it involves collaboration with the Corporate Executive, as it would be harder to detect and more complex due to the authority and power of the Corporate Executive. Most Executives travel substantially for their work. Due to this, flexible systems have been developed over the years which is accessible over the internet and via various types of devices including notebooks, mobiles, PDA's etc.

Manuscript published on 30 January 2019.
***Correspondence Author(s)**
Geetha A Rubasundram, School of Accounting & Finance, Asia Pacific University, Malaysia.

The flexibility also comes with the crucial requirement of stringent controls, including cyber security. Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and users assets (UN –ITU, n.d.). Organization and user assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems and the totality of transmitted and/or stored information in the cyber environment. The general security objectives comprise: Confidentiality, Availability and Integrity. Karyda and Mitrou (2007) discuss the far-reaching consequences of the new fraud activities that are caused by the new technologies and as well as due to anonymity of the cyber-criminal activities which are not restricted by geographical boundaries. Therefore, it is crucial for organizations to assess the risk of fraud caused by technology.

A. Corporate Executive Fraud

Choo & Tan (2006) define Corporate Executive Fraud as an intentional financial misrepresentation by trusted executives of public companies. However, the writer of this paper contends that a Corporate Executive Fraud risk could include more that the rather narrow definition provided, as it involves an Insider Threat. Insider Threat is when a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data, and intentionally exceeds or uses that access in a manner that negatively affects the confidentiality, integrity, or availability of the organization's information or information systems (Lori et al, 2013). An Insider Threat can be even more damaging to an organisation where there is collaboration between the top executives and the external software vendors. When the Corporate Executive is involved, the damages of the fraud is significantly higher due to the capability of the individual to override controls, bully subordinates and also have the personality to seem trustworthy and capable.

Hunker and Probst (2011) observe that to be considered an insider, there should be access to the system, the ability to represent the organization to others, have the required knowledge and be trusted by the organization. The violation of the position of trust in terms of the Corporate Executive Fraud reflects another legal element to proof reliance of the victim on the perpetrators words.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

The observation by Hunker and Probst (2011) relates closely to Donald Cresseys "Fraud Triangle" variables representing pressures or motivation to carry out the fraud, the opportunity to carry out the fraud and the final variable being to rationalise the act as being inconsistent with one's personal level of integrity. The rationalization of the intention can differ significantly, depending on whether it was carried out for the benefit of the individual(s) (Wells, 2007) or for the benefit of the corporation (Clinard&Quinney, 1973). Wolfe &Hermanson (2004) introduced the Fraud Diamond, extending the Fraud Triangle to include fraudster capabilities. The capability component takes into account the fraudster's position or function within the organisation which may furnish the ability to create or exploit an opportunity for fraud not available to others, which also includes the fraudster's ability to exploit internal control weakness. The fraudster's personality also plays a role in this model. Wolfe &Hermanson (2004) identify ego and confidence of non-detection or non-penalisation as well as the ability to coerce others to commit or conceal fraud; which is in line with Kelman& Hamilton (1989) "Crimes of Obedience" where an individual is caught in the dilemma of either carrying out a directive that is wrong or disobeying an order and suffering the consequences. Wolfe &Hermanson(2004) also believe that the fraudster has the ability to lie effectively and consistently; and to deal with the stress accordingly.Kassem&Higson (2012) discuss the New Fraud Triangle Model in their paper, citing Dorminey et al (2010). In this model, they suggest to expand the motivation component of the original fraud triangle, to include Money, Ideology, Coercion and Ego (MICE). Ideological motivators are able to justify the fraud by believing that their action would bring greater benefits, consistent with their beliefs (ideology). The other change to the model includes a personal integrity scale instead of rationalisation, which was introduced by Albrecht et al (1984)

Depending on the scenario, the IS maybe manipulated to carry out the actual fraud of financial misrepresentation, or it may just influenced as a cover up. Therefore, it is important to note that it maybe a simple case of asset misappropriation, right up to a financial statement fraud or just an error at times when there are discrepancies noted in the system. Since most organisations and individuals are aware of the evidences available to catch a fraudster, the fraudster tends to collaborate to take advantage of a tight control environment. Therefore, the ability to override controls is definitely a red flag as well as the various other red flags related to the "Crimes of Obedience", which would need to be taken into account when carrying out a risk assessment. The motivation, pressure and capability factors play a significant role especially to proof the intention of the fraudster, a key legal element required when proving fraud. Newman and Ellis (2011) discuss the possibilities and case laws where electronic evidence including email evidence was considered strong evidence to proof intent.

B. Fraud Risk Assessment

Enterprise-wide risk assessments help organizations identify critical assets, threats to those assets, and the mission impact of successful attacks. They also determine which controls to implement to identify and minimize critical risks. (Lori et al, 2013). O'Bell (2009) mentions that of the three conditions in the Fraud Triangle (opportunity, rationalization, and motivation); opportunity is the one condition that is manageable to address fraud risks. This condition is managed by designing and implementing a control environment that prevents, detects, and deters most fraudulent behaviour, whether conducted by employees, vendors, consultants or senior management. However, Rubasundram (2015) cautions that too many controls could make an organization bureaucratic, causing additional cost, resources and time to be incurred. Therefore it is recommended that organisations carry out periodic Fraud Risk Assessments to assess the risk and the required controls. This research paper focuses on a pro-active Fraud Risk Assessment. Rubasundram (2014, 2015) summarised the following steps to carry out a Fraud Risk Assessment & Management:

a) Management to initiate the Fraud Risk Assessment & Management by setting up a Fraud Risk Assessment & Management Team (FRAM Team) to set goals, objectives and the fraud risk appetite of the organization.
b) FRAM Team to carry out brainstorming activities, process mapping, necessary checks, audits & tests and discussions / interviews with other personnel to understand the following:
   I. The organizations environment, management, business, departments, processes , functions and owners
   II. Potential fraud scenarios and schemes, taking into account red flag areas such as management override of controls and personnel who may exhibit the factors identified in the Fraud Triangle, Fraud Diamond and The New Fraud Triangle.
   III. Identify the categories required and assess the likelihood and impact of the fraud schemes accordingly
   IV. Based on the above, do a review and gap analysis of the current controls in place and any additional or revised controls needed, in line with the organizations risk appetite and decided risk strategy
   V. Implement and monitor controls with periodic evaluation

II. EVIDENCE AND THE LEGAL ASPECTS TO BE CONSIDERED

As with any investigation, it is crucial that the legality of any evidence should be considered. Assuming that all investigations could possibly end up in court, it is crucial for the investigator to be mindful of the admissibility of evidence in court. Ryan and Shpantzer (2002) mention that the evidence should be relevant, material and competent, and its probative value must outweigh any prejudicial effect. This would include the legality of obtaining the evidence.

It is common practice for businesses to retain electronically stored information because it is convenient and cost-effective to store records in electronic format and because regulations require companies to maintain certain business records.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Electronic evidence or e-evidence is electronically stored information on any type of computer device that can be used as evidence in a legal action. Therefore, information and communication systems are now breeding grounds for electronic-evidence (e-evidence) in audits, investigations, or litigation. Business records are subject to regulation and to pre-trial discovery, subpoena, or search warrant. The business records include e-mail and IM records to create a "chain of evidence" proving illegal activity (Volonino, 2003).

Ryan and Shpantzer (2002) discuss the uniqueness of the digital evidence or e-evidence in terms of competency since it can be easily duplicated and modified, and the required survival of the Daubert threshold test as well as the collection, storage, processing and presentation of the evidence. In the federal court system, Federal Rules of Evidence (FRE) 901 and 902 govern authentication. FRE 901(a) notes that evidence is authenticated if there is "evidence sufficient to support a finding that the matter in question is what its proponent claims." FRE 901(b) then provides a list of potential ways that a litigant can satisfy this standard. For example, the easiest way to authenticate the data is under FRE 901(b)(1), which allows a witness with personal knowledge to authenticate that the data is what it is claimed to be. If such testimony is unavailable, courts have permitted electronic data to be admitted under FRE 901(b)(4), which permits authentication through distinctive characteristics such as the document's "appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances." The court permitted other emails to be authenticated under FRE 901(b)(3) by allowing the comparison of email addresses and formats to permit related emails into evidence. Under FRE 902(7), business emails can be self-authenticating with information showing the origin of the transmission or other identifying marks. (Newman and Ellis, 2011)

Since this was a pro-active risk assessment, the researcher were allowed access to employees and documents, but were advised to be discreet and to ensure that the objective of the risk assessment being fraud related was not to be communicated. Also, constant communication with the Manager in Charge was required, and approvals needed to be given for each step of the risk assessment as well as the documentation requirement.

The overall research was limited hence the researcher took an alternative route to assess the risk, since it would have been difficult to get direct access to server logs and network logs of the organization, which may have affected the integrity of the evidence. However, the researcher assumed that if the case did ever proceed to litigation, the documents could be extracted via discovery etc. According to Rule 26 of the Federal Rules of Discovery (Fed. R. D.), each company has the duty to preserve documents that may be relevant in a case. This duty to preserve is fundamental to, and inseparable from, the duty of disclosure. When involved in a legal action, companies are bound by the duty of disclosure to turn over requested e-records in readable format by a specified date (Volonino, 2003).

The researcher strategized the assessment to be a multi-layered assessment to include profiling and predictive modeling (Greitzer and Frincke, 2010; Hunker and Probst), which was then to be compared to the documented evidence collected for collaboration and consistency. The researcher classified the users according to pre-defined work groups. This included internal and external users who had access to the system, as well as by accessibility according to work responsibility and authorisation. This was then compared to the daily network, system, servers, firewall logs etc. The researcher refers to the paper by Hunker and Probst (2011), which discusses two alternate solutions in relation to Insider Threats that are based on technological and sociological or organizational groups, with a final socio-technical approach combining both the groups. The sociological group examines the psychological aspects and motivation of the insider; that is, why and under what circumstances an insider becomes an insider threat, and also the organizational and cultural factors that affect the insider and shape his response to the security environment, which links to the pressure or motive and rationalization aspects of the Fraud Triangle. Technical approaches use system policy and specifications to prevent, or failing that, identify and minimize the damage done by the threatening insider which links to the opportunity aspect of the Fraud Triangle. Greitzer and Frincke (2010) also integrate psychosocial and cyber indicators as part of the model, and acknowledge the challenges of the method.

Screenshots of the ERP system was also taken on an hourly basis every day during the period of monitoring. A "screenshot" is a snapshot or recording of an image displayed on a computer monitor which depicts what was visible on the monitor to an observer. The screenshot record is usually a digital image recorded by a receiving computer or other means of intercepting the video display, such as camera or DVR. The theory for admissibility was the receipt of testimony by a witness with personal knowledge of what defendant displayed under FRE 901(b)(1) as mentioned above(Federal Evidence, 2011).

The culture of an organization plays an important role when implementing insider threat practices. Insider threat indicators may vary between cultures and subcultures, some of which span multiple countries. Greater emphasis on hiring, training and motivating employees to act securely will generate great payoff for organisations (Warkentin and Willison, 2009). The tone from the top plays a crucial role in managing fraud or the risk of fraud. The tone at the top and the control environment as per the COSO framework sets the risk appetite of the organization. This should then be incorporated as part of the policies, procedures and processes of the organization. Example of this could be a requirement of the organization that all employees, contractors, and trusted business partners to sign nondisclosure agreements (NDAs) and undergo background checks; contractors' and trusted business partners' background checks should be commensurate with the organization's to ensure no undisclosed related party transactions.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

III. METHODS & MATERIALS

The researcher's main criteria when selecting the research methodology is as follows:

- Ability to carry out an in-depth study of the ERP System and overall Information System, documents, employees, culture, environment and processes without any limitations.
- To be able to carry out the necessary steps to test the current internal control environment and the Information System. The results were then to becompared with the Audit Trail, physical checks, documents, and interviews.

The researcher preferred to use Action Research to be able to achieve the above depth. Action Research enables research to take place in real life situations and to solve actual problems or issues, rather than just taking a more theoretical method (Kizito&Kuhne et al, 1997). The writer chose to use purposive sampling to ensure a more in-depth research to achieve the objectives of this paper.

The organization selected provided the writer of this paper access into their ERP systems, information, process, and documents. Due to the sensitivity of the case, the country, the organization, and the individuals involved will remain anonymous. However, the main essence of the case study, the actual interviews, minutes of meetings, brainstorming sessions within the key management team and other documents will be discussed, focusing on the cyber security and ERP system.

The key criteria's for selecting the organisation:

1. Red flags to denote possible fraudulent activities by the top management.
2. Issues with the Enterprise Resource Planning (ERP) system.

The main techniques used here was background checks especially to build the psychosocial profiles, comparison of screen shots over three months, final reports, comparison reports kept separately and discretely, interviews, emails confirmation and comparisons with the systems audit trails and access logs. Although the methodology followed typical Fraud Risk Assessment techniques, and ensured that the necessary privacy and investigative legislations were followed, the researchers were advised to be discreet during the investigations, hence physical access to individual computers and the servers was not allowed.

IV. RESULTS

Although the management was aware of the research and pro-active fraud risk assessment, they were unaware of the risks of the systems. The following red flags were noted during the pro-active investigation:

1. The relationship between the external IT vendors and key Corporate Executives.
2. The lack of expertise amongst the IT personnel
3. The many issues faced in the system from users. Although the system was running live, the vendors still had access and the capability to amend the system information from the back end. Hence, it would seem like an authorised access even though it was via a remote access. They also claimed that logs for certain amendments were not available.

The vendors had been selected for their previous experience on similar projects. The researcher was unable to compare the tender bid documents since the management had ignored the request to provide the documents. However, background checks on the vendors company and the key personnel of the selected client company, showed a related party relationship that had not been disclosed.

The IT Personnel in the clients firm were mostly junior, with only one executive reflecting a leadership role and more advanced knowledge and experience. However, the role of the team was more of being followers under a rather authoritarian culture. They were aware of the risks that would be faced with the current arrangement of the system being live with simultaneous changes being made to the various ERP modules, however, they believed that their responsibility only included highlighting the risk to management.

The users of the system had reported many issues especially from the Accounting modules. Emails to the vendors provided insights into the inability to save, missing data, unable to approve / reject transactions and typical other operational complaints. The vendors operated remotely, taking advantage of the timing differences between the geographical locations to carry out the patch updates with the assumption that it would not affect the systems data and information. The IT Personnel would open up access to the system via the Internet based on the requests of the vendors, and approval of the management.

Due to the crucial issues faced, the system came to almost a standstill for some modules. Hence, the users kept manual reports to report the activities that provided the researchers an ability to compare the reports in the system and the manual reports. The researchers also requested that the users print screen of their ERP system reports and activities on a daily basis as the researchers were concerned about the missing data from the system after transaction had been saved.

Daily checks against the server logs, network logs and ERP system logs did not report any unauthorized attempts of access, even during the times of authorised external access provided to the vendors. However, the risk of being hacked was still possible. IT Personnel carried out the monitoring of the system. The researcher was not allowed direct access to the logs either, and had to get print outs where requested. Due to the constraints of the research and assessment, the researchers eventually needed to use more manual methods to assess the risk of fraud. Some of the noted constraints included:

- Lack of direct access to documents and records
- Inability to communicate directly the intentions of the research
- The organization was reasonably new, hence comparisons with past reports and performance was not an option.
- The necessity and urgency to keep the assessment low key in order to not provoke any negative circumstances.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The researchers were able to proof the discrepancies in the data by comparing the screen shots of the system reports before and after the patches. It required a tedious assessment of each line item and report. The system logs at the point did not reflect that the vendors had even accessed the modules at times. The researchers then started interviewing the IT Personnel and corresponding with the vendors, ensuring that limited information was given out. The intention was mainly as an information gathering process. However, due to discrepancies and contradictory responses over the period of assessment, the researcher was able to obtain a voluntary confession on the limitations of the systems. Eventually, the vendors had to admit that the audit trails were not complete in the system, and certain modules did not even have any audit trails. The emails reflecting the correspondence between the investigators, users, IT Personnel, Executive Management were used as evidence here.

Therefore, this reflected that although the users were aware of the risks caused by the weakness in controls, they had ignored due to the element of "trust" and the ability to override the controls in place with their ability and capability; hence providing the element of opportunity. However, this affected the integrity of the system and the information contained over a long period of time.

The pressure or motive in this scenario is not discussed in depth since it was not focused especially on a reactive investigation. However, possible pressures or motive could have been due to a performance or financial pressures of the organization, and not so much on the individual corporate executive requirements. The rationalization would have been more towards the good of the company, regardless of the possible unethical means.

V. CONCLUSION

The research reflects that as long as there is a motivation to carry out fraud, with the right opportunity, most corporate executives would rationalize the fraudulent behavior if the ethical tone at the top or corporate culture were not strong. The capability factor also plays an important factor. It is interesting to note that in the above situation, the controls could have easily been manipulated due to collaboration and over-riding of controls. It would have been difficult to proof that unauthorized access had even happened due to the lack of audit trails and the most importantly, the weak control environment or tone at the top. The Corporate Executive being able to override the controls due to the "Crimes of Obedience" attributes would have reflected that the right controls were in place and were being followed by the authorized employee. Therefore, it is important to ensure that employees are trained and are made aware by HR policies on whistleblowing hotlines to prevent such situations. Apart from that, more controls to prevent collaboration and overriding of controls should be implemented.

REFERENCES

1. Albrecht S, Howe K & Romney M. (1984), *Deterring Fraud: The Internal Auditors Perspective*, Institute of Internal Auditors Research Foundation
2. Best P.J, Rikhardsson P and Toleman M. (2009), Continuous Fraud Detection in Enterprise Systems through Audit Trail Analysis, *Journal of Digital Forensics, Security and Law*, Vol. 4(1)
3. Choo, F & Tan, K, (2007).*An American Dream Theory of Corporate Executive Fraud*, Elsevier – Accounting Forum,
4. Clinard MB &Quinney R, (1973).*Criminal Behaviour Systems, A typology*, New York: Holt, Rinehart & Winston
5. Cressey, D.R (1973). *Other people's money:* Montclair: Patterson Smith
6. Dorminey J, Fleming S, Kranacher M& Riley R(2011), *The Evolution of Fraud Theory*. American Accounting Association Annual Meeting, Denver, August, pp.1-58
7. Federal Evidence (2011), Authenticating Internet Screenshot Evidence under FRE 901, *Federal Evidence Review*
8. Greitzer, Frank L and Frincke, Deborah A (2010), Combining Traditional Cyber Security Audit Data with Psychosocial Data : Towards Predictive Modelling for Insider Threat Mitigation. Insider Threats in Cybersecurity, New York: Springer, pp.85-114
9. J. Hunker and C. W. Probst, (2011). Insiders and insider threats - an overview of definitions and mitigation techniques," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, 2(1), pp. 4–27
10. Karyda, Maria and Mitrou, Lilian (2007), Internet Forensics: Legal and Technical Issues DOI: 10.1109/WDFIA.2007.4299368 · Source: IEEE Xplore
11. Kassem, R &Higson, A.W (2012), The New Fraud Triangle Model. *Journal of Emerging Trends in Economics and Management Sciences*, 3 (3), pp. 191-195
12. Kelman HC & HamiltonV.L(1989), *Crimes of Obedience.* New Haven CT Yale University Press
13. Kizito and Kuhne (1997), Sustaining the Benefits of Action Research In Decision Support Tools Development pp. 37-41
14. Lori, Flynn, Carly Huth, Randy Trzeciak, Palma Buttles (2013), Best PractisesAgainst Insider Threats in All Nations, Carnegie Mellon University, Research Showcase @ CMU
15. Newman, Zachary G and Ellis, Anthony (2011), *The Reliability, Admissability and Power of Electronic Evidence*, American Bar Association [online], Available at: http://apps.americanbar.org/litigation/committees/trialevidence/articles/012511-electronic-evidence.html [Accessed 5th June, 2016]
16. Rikhardson, Pall and Kraemmergaard, Pernille (2006), Identifying the impacts of enterprise system implementation and use: Examples from Denmark, International *Journal of Accounting Information Systems* 7 (1), pp. 36-49
17. Rubasundram G A (2014), Fraud Risk Assessment: A Tool for SME's to Identify Effective Controls. *Research Journal of Accounting & Finance*
18. Rubasundram G A (2015) .Perceived tone from the top during a Fraud Risk Assessment. *Procedia Economics and Finance*, Vol.28, pp.1-274
19. Ryan, Daniel J and Shpantzer, Gal (2002)–Legal Aspects of Digital Forensics Proceedings: ForensicsWorkshop, [online]. Available at: http://euro.ecom.cmu.edu/program/law-08-732/Evidence/RyanShpantzer.pdf - [Accessed 5th June 2016].
20. O' Bell Erick (2009), *5 Anti-Fraud Strategies to Deter, Prevent and Detect Fraud*, Corporate Compliance Insight
21. UN-ITU (n.d), U.N International Telecommunication Union (ITU)[online]. Available at: http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx [Accessed 5th June,2016]
22. Volonino, Linda (2003), Electronic Evidence and Computer Forensics, Communications of AIS, Volume12 Article 27
23. Warkentin, Merrill and Willison, Robert (2009), Behavioural and policy issues in information systems security: the insider threat, *European Journal of Information Systems* Vol. 18, pp. 101-105
24. Wells Joseph T. (2007), *Corporate Fraud Handbook – Prevention and Detection*, 2nd Edition, John Wiley & Sons
25. Wolfe, D.T &Hermanson, D.R (2004),The Fraud Diamond: Considering the Four Elements of Fraud. *CPA Journal* 74(12), pp. 38-42
26. Zahra SA, Priem RL &Rashees AA (2005), The antecedents and consequences of top management fraud, *Journal of Management* ,Vol.31, p.803

AUTHORS PROFILE

Geetha A Rubasundram is working in School of Accounting & Finance, Asia Pacific University, Malaysia.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)