A Review of Cybersecurity Element in Fraud Prevention and Detection Mechanisms

Malar Gunasegaran[1], Rohaida Basiruddin[2], Ruaa Binsaddiq[3]
[1,2] Azman Hashim International Business School, Level 10, Menara Razak, Universiti Teknologi Malaysia, Jalan Sultan Yahya Petra, 54100 Kuala Lumpur, Malaysia.
[3]College of Business Administration, University of Business and Technology, Jeddah, Saudi Arabia.
malar@graduate.utm.my[1], rohaida@ibs.utm.my[2], r.binsaddig@ubt.edu.sa[3]

Article history

Received:
1 Dec 2021

Received in revised form:
6 Dec 2021

Accepted:
10 Dec 2021

Published online:
22 Dec 2021

*Corresponding author
malar@graduate.utm.my

Abstract

Fraud is highly alarming in all sectors, and it is also seen as problematic globally. Although relevant bodies and individuals have carried out efforts in combating fraud, it appears that fraud in its various forms is a problem that is still increasing in recurrence and severity. As a result, organizations need to equip themselves with effective prevention and detection mechanisms. Furthermore, these prevention and detection mechanisms need to take into account the latest technology, which is related to cybersecurity. Cybersecurity is one of the recent areas of national and global security concerns of the 21st century. By addressing cybersecurity, organizations will thrive in a digital economy in which secured cyberspace is available for them to operate effectively. Thus, this article proposes enhanced fraud prevention and detection mechanism from the COSO framework to mitigate frauds, including cyber-attacks. Furthermore, this study also presents insights into future research work.

Keywords: *fraud prevention, fraud detection, COSO, cybersecurity, public sector*

1. Introduction

Fraud is on the rise globally, and it continues to be a major issue among organizations. It affects reputation and financial health [37]. Besides, several organizations have been found not to upgrade their prevention measures or strategies in combating frauds in the current scenario in which frauds are getting more sophisticated and increasing the number of cases [8]. Many studies have focused on fraud mechanisms' effectiveness, such as fraud prevention programs, good governance, and sound internal control procedures. These factors are the most critical in reducing fraud.

From a broader perspective, prior research focused more on factors leading to fraud occurrence, the impact on risk management and control, and detection mechanisms in general [1,46]. Nevertheless, those studies have mainly concentrated on the private sector [21]. As a result, exploration related to this area is still at a 'primaeval stage'. Therefore, this study proposes a component of cybersecurity in fraud prevention and detection mechanisms, which have not been thoroughly practised, especially in the public sector. We complement the work of Mat et al. [29] in addressing cybersecurity issues and fraud prevention in the public sector since there have not been many studies conducted concerning these areas.

* *malar@graduate.utm.my*

Furthermore, cybersecurity has become a significant global issue due to the worldwide rise in internet traffic flows and users. As a result, many organizations have developed a cyber-security policy framework that can fundamentally help in combating cybercrimes [2]. Such frameworks are very important since they provide measures that help safeguard critical information infrastructure, thereby reducing the existing national vulnerabilities [26]. As a result, there is a need to enhance understanding of fraud prevention and detection mechanisms in organizations and empirically investigate its implementation and execution effectiveness.

2. Discussion on Control Environment of COSO's Element Towards Fraud Prevention and Detection

The COSO framework consists of five elements: control environment, risk assessment, control activities, information and communication, and monitoring [11]. Research conducted by Nawawi & Salin [33] stated that standards, policies and procedures are placed under the control environment elements of the COSO framework. The standards, policies and procedures involve the most basic and crucial components that must be recognized since they provide a foundation for implementing internal control across organizations, at every level (lower, middle and top) both horizontally and vertically [11]. Besides, this framework aids to facilitate efficient and effective operations in ensuring the external and internal reporting is of high quality and compliant to the relevant regulations and laws [16]. Furthermore, policies and well-designed procedures ensure that the objectives of an organization are achieved successfully [40]. Moreover, organizations can take remedial actions when something goes wrong, and as a result, it helps reduce, prevent and detect fraud at the workplace [12].

The crucial issue concerning policies and procedures in the internal control system under the control environment component is compliance. Policies and procedures seem to become worthless if constantly breached and overridden by employees. Some may argue that internal control is pointless and time-consuming or "red tape" [12]. Due to this, it is significant to illustrate a righteous example of compliance to internal control procedures by the highest authority in the organization. This example will then be repeated to the organization's lowest layers by the lower-level management. The KPMG survey shows that internal controls overridden by some employees for their gain and maybe trying to defraud a company or an organization [12]. In contrast, employees who have behaved morally and ethically tend to have a favorable influence on their organization [28].

Thabit et al. [42] argued that the control environment is further affected by the structure and accountability relationships of the organization. The control environment widely influences an organization's decisions and activities and provides the basis for the overall internal control system. If this foundation is not strong and the control environment is not positive, the overall internal control system will not be as effective as it should be.

In addition, the present perspective on most organizations does not ensure that their internal control mechanisms are adequately implemented and would impact the organizations' effectiveness in sustaining control. Cases occurring within government organizations, including misuse of the control system, are potential

signs that these organizations might have a flawed system of internal control in which it can be abused for their own gain, for instance, through the permits issuance, tenders, and funds misuse. Previous studies on the public sector have illustrated that due to the least practices in fraud control in some areas of the public sector, the level of fraud and corruption seems to remain high [22].

Based on those findings, fraud seems to occur frequently, especially in tendering, issuing permits, and misusing funds. In addition, Perumal et al. [36] have mentioned that the tendering and all permit-issuing services have been converted to be delivered online. As a result, awareness of cybersecurity needs to be instilled among public sector employees, mainly those involved in providing services. Then, cybersecurity in this context can overcome any form of fraud that may occur.

3. Revisiting Fraud Prevention and Detection Mechanisms

First and foremost, fraud prevention calls for measures to avoid it in the first place. Then, once the prevention measures have not been fully effective, reliable and quick fraud detection is needed [6]. Instinctively, fraud detection must be utilized and operated constantly while fraud grows. Understandably, the conventional approach for fraud detection and prevention, such as auditing, is not adequately efficient and only enables fraud to be detected months after the transactions were completed. Due to that, effective detection and prevention measures are required.

Krambia-Kardis [24], in his study, described that all kinds of bodies are taking extra and distinctive moves to overcome fraud since the traditional red flags method has been viewed as ineffective. The famous red flags methodology includes the utilization of fraud pointers. The presence of red flags are signs meant intended to alarm auditors to the likelihood of dishonest doings; they actually do not predict the existence of fraud but signify situations related to fraud. Both asset misuse and fake financial reporting tend to be the most important overheads for lots of companies.

It has been found that numerous fraud detection methods are currently being used with the intention of lessening the immediate and circuitous expenses connected with all types of fraud. These diverse tactics consist of employee reference checks, telephone hotlines, vendor contract reviews, fraud vulnerability reviews, analytical reviews and sanctions [10,43], yet they are not limited to apply only those strategies. Organizations that have experienced fraud cases have implemented more concrete actions like fraud detection and prevention training and whistle-blowing rules. Meanwhile, those organizations which are not found to be victims of fraud have a tendency to depend further on immaterial deterrence methods such as fraud reporting policies or code of conduct [38].

Enforcement, training and controls need to be integrated so that fraud can be prevented effectively. With the given attention, it is hoped that the most effective solution can be recommended to reinforce the institutionalization of government policy to overcome frauds in the public sector and to instill awareness on the importance of protecting the public's assets and revenues among government servants [19,47].

Othman et al. [35] suggest that the most effective fraud detection and prevention mechanisms employed in the public sector are operational audits, enhanced audit

committees, improved internal controls, implementation of fraud reporting policy, staff rotation, fraud hotlines and forensic accountants. On the other hand, it has also been proven that training in ethics or code of conduct, raising fraud awareness activities, training in privacy values and training for personnel included in activities of fraud control are also seem to be efficient measures for fraud prevention [30].

Furthermore, seven studies have been done in the area of fraud prevention and detection mechanisms. It has been discovered that the most successful technique for detecting fraud was through analytical procedures [4,5,15,34,39,40,44]. Although these studies were carried out in the area of fraud prevention and detection measures, none was addressing on cybersecurity in terms of fraud prevention and detection. It has also been found that there is an occasional use of cybersecurity in detecting fraud, especially in the public sector. The National Institute of Standards and Technology, 2013a describes cybersecurity as a data protection method by detecting, preventing and reacting to cyber-attacks. In other words, the sophistication of cybersecurity emanates fewer from the gadgets that we use than from the individuals behind them. In its glossary, the National Cyber Security Careers and Studies Initiative [23] describes cybersecurity as "the activity or process, ability or capability or state by which information and communications systems and the information contained in them are protected from and/or defended against harm, unauthorized use or modification or exploitation."

3.1. Cybersecurity

Based on the literature, cybersecurity is an important detection and prevention mechanism of fraud but only been emphasized in the private sector. According to Davis et al. [14], cybersecurity is also crucial in enabling governmental organizations to adapt to different technological changes and the complexities of globalization. Furthermore, the National Institute of Standard and Technology (NIST) defines cybersecurity as a procedure of defending information by detecting, preventing and reacting to attacks [7]. Therefore, cybersecurity is also seen as one of the potential fraud detection and prevention mechanism in which it helps organizations in combating cyber-fraud.

Other studies have also shown that the acquisition of appropriate cybersecurity training is a fundamental move toward resolving the growing number of intrusions and attacks on personal or institutional information in terms of technological fraud known as cybercrime. Misinformed information protection and insufficient data security expertise offer hackers the ability to maliciously access and use information from other individuals or organizations [9].

Cybersecurity has also become a significant global issue due to the worldwide rise in internet users and high internet traffic flows. The various elements of cybersecurity and cyber-crime prevention have gained considerable attention in many countries, based on technological growth and capacity building which are among the Millennium Development Goals that should be accomplished in achieving Sustainable Development by the year 2030 [32]. Governments agree that a big step towards achieving sustainable economic development is to reduce the high incidences of cybercrime. Furthermore, it is important to note that cybercrime prevention gives space for

strategic growth in trade and industry, which facilitates improved economic growth in the long run [17].

4. Underpinning Theory

Different theories have explained the causes of fraud, and the two most cited theories are Cressey's Fraud Triangle Theory [13] and Wolfe and Hermanson's Fraud Diamond Theory [45]. They both describe the components that lead perpetrators to commit fraud. Among both theories, the Fraud Triangle Theory seems to be more relevant because it contributes to fraud prevention and detection mechanisms. One of its contributions in terms of organizational perspective is the increased sensitivity to fraud. Due to that, organizations' management will be more alert to fraud prevention and detection mechanisms [31]. Besides, research by Nawawi & Salin [33] shows that fraud happens in organizations due to weak internal control by employees pretending of not being mindful and understanding of the existence of policies and procedures and at the same time creates the opportunity for fraud to take place. Therefore, organizations need to ensure the effectiveness of the policies and standard operating procedures since opportunities and reasons for internal fraud are always present.

Moreover, Fraud Triangle Theory strengthens the fraud prevention and also detection of organizations. Some employees may interpret an employer's failure to eliminate the opportunity and motivation for fraud to be committed over time as a sign of a "slack organizational culture" concerning fraud. As a result, employers in organizations need to make sure that fraud prevention and detection mechanisms being efficiently practised so that there will be no room for employees to commit and engage with fraud. This seems to be another advantage of using the Fraud Triangle to mitigate fraud [25]. According to Joseph et al. [20], it has been found that breaking the fraud triangle is the key to fraud prevention and detection. Therefore, an organization must remove one of the components in the fraud triangle in order to lessen the probability of fraudulent activities. Opportunity has been found as one of the elements that need to be removed since it is most directly affected by internal control systems and generally caters to the most actionable route to detect and prevent fraud [3].

5. Future Research

Based on what has been discussed, cybersecurity has been found as one of the detection and prevention mechanisms that are not actively implemented yet in the public sector. Organizations might fail to effectively allocate resources to information systems in the most vulnerable areas with the absence of cybersecurity. Studies have consistently shown that most cybercrime or cyber-attacks-related problems emerge from a shortage of skilled IT workers in an organization. Most scholars disclose that some employees lack the necessary knowledge and skills to protect private or public data or information effectively, thereby making it more vulnerable to hackers [27]. For instance, based on a study done by Haris@Harib et al. [18], to fight against cyber-attacks, the Cybersecurity of Malaysia has adopted the National Cyber Security Policy in which policy is to strengthen the defence of the country. The policy's

vision is to make the infrastructure is in secure, robust and self-reliant. In addition, the Malaysian public sector has implemented a cybersecurity policy to protect fraud since government procurement systems nowadays are made online. Therefore, this newly proposed cybersecurity element in the fraud prevention and detection mechanisms framework will contribute to future research by proposing other elements that are appropriate to be implemented in these mechanisms.

6. Conclusion

Previous studies on fraud prevention and detection mechanisms have concentrated primarily on the private sector [4,5,15,34,39,40,44]. On the other hand, limited studies were conducted on fraud detection and prevention in the public sector. In addition, those researches center for the most part on fraud alertness, categories of fraud occurring in the public sector and several fraud deterrents and discovery actions. Nonetheless, not one was upheld through information gathering. Hence, this review bridges the gap by exploring the execution of fraud prevention and detection mechanisms, suitable preventative and detection measures based on the existing ones, and introducing a new measure of cybersecurity as a detection and prevention mechanism. In addition, the proposed element will result in enhanced fraud prevention and detection mechanism framework. Validation and further extension of the enhanced framework with the proposed element through an empirical investigation will be the future direction of this research.

Acknowledgment

This research has received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

[1] Aghghaleh, S. F., Iskandar, T. M., & Mohamed, Z. M. (2014). Fraud Risk Factors of Fraud Triangle and the Likelihood of Fraud Occurrence: Evidence from Malaysia. Information Management & Business Review, 6(1).
[2] Alabdulatif, A. (2018). Cybercrime and Analysis of Laws in Kingdom of Saudi Arabia (Doctoral dissertation).
[3] Ann Riney, F. (2018). Two-Step Fraud Defense System: Prevention and Detection. Journal of Corporate Accounting & Finance, 29(2), 74-86.
[4] Apostolou, N. Crumbley, D.L., 2008. Auditors' responsibilities with respect to fraud: a possible shift?CPA Journal. Retrieved on 17 December 2014 from http://www.nysscpa.org/cpajournal/2008/208/essentials/p32.htm
[5] Bierstaker, J.L., Brody, R.D., Pacini, C., 2006. Accountants' perceptions regarding fraud detection and prevention methods. Managerial Auditing Journal, 21(5), 520-535.
[6] Bolton, R.J., Hand, D.J., 2002. Statistical Fraud Detection: A Review. Statistical Science, 17(3), 235– 255. doi:10.1214/ss/1042727940.
[7] Bozkus Kahyaoglu, S., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. Managerial Auditing Journal, 33(4), 360–376. https://doi.org/10.1108/MAJ-02-2018-1804.
[8] Buang, A. (YBhg Tan Sri Dato'), (2010), Keynote Address "Setting the Tone for Fraud Risk Management" presented at Corporate Fraud Conference 2010, Crowne Plaza Mutiara, Kuala Lumpur, 5 – 6 July 2010.
[9] Butler, B., & Lachow, I. (2012). Multilateral approaches for improving globalsecurity in cyberspace. Georgetown Journal of International Affairs, 5-14.
[10] Carpenter, B.W. and Mahoney, D.P. (2001), "Analyzing organizational fraud", Internal Auditor, April, pp. 33-38.
[11] COSO. (2013). Internal Control: Integrated Framework (Executive Summary). Retrieved from http://coso.org/IC-IntegratedFramework-summary.htm.
[12] CPA Australia (2008), "Internal control for small business", available at: www.cpaaustralia.com.au/~/media/corporate/allfiles/document/professionalresources/business/internal-controls-for-small-business.pdf (accessed 31 January 2017).
[13] Cressey, D. R. (1950) The criminal violation of financial trust. American Sociological Review 15 (6): 738 – 743
[14] Davis, J. I., Libicki, M. C., Johnson, S. E., Kumar, J., Watson, M., & Karode, A. (2016). A framework for programming and budgeting for cybersecurity. RAND Corporation Santa Monica United States.

[15] Durtschi, C., Hillison, W. & Pacini, C., 2004. The effective use of Benford's Law to assist in detecting fraud in accounting data. Journal of Forensic Accounting,17-34.
[16] Financial Reporting Council (2005), Internal Control: Revised Guidance for Directors on the Combined Code, FRC, London.
[17] Galligan, M. E., Herrygers, S., & Rau, K. (2020) CYBER RISK IN A DIGITAL AGE.
[18] Harib, A. R. H., Sarijan, S., & Hussin, N. (2017). Information security challenges: A Malaysian Context. International Journal of Academic Research in Business and Social Sciences, 7(9), 397-403.
[19] Haron, R., Mohamed, N., & Paino, H. (2015). Misappropriation of assets: A decepticon of leakages in Malaysian public sector.
[20] Joseph, O. N., Albert, O., & Byaruhanga, J. (2015). Effect of internal control on fraud detection and prevention in district treasuries of Kakamega County. International Journal of Business and management invention, 4(1), 47-57.
[21] Kamaliah, K., Marjuni, N. S., Mohamed, N., Mohd-Sanusi, Z., & Anugerah, R. (2018). Effectiveness of monitoring mechanisms and mitigation of fraud incidents in the public sector. Administratie si Management Public, (30), 82-95.
[22] Khalid, M. A., & Said, J. (2016). Empirical Assessment of Good Governance in the Public Sector of Malaysia. Interdisciplinary Approach to Economics and Sociology, 9(4), 289–304. https://doi.org/10.14254/2071-789X.2016/9-4/18.
[23] Kissel, R. (2013), "Explore terms: a glossary of common cybersecurity terminology", National Initiative for Cybersecurity Careers and Studies, available at: https://niccs.us-cert.gov/glossary (accessed 17 November 2017).
[24] Krambia-Kardis, M. 2002, "A fraud detection model: a must for auditors", Journal of Financial Regulation and Compliance, Vol. 10 No. 3, pp. 266-78.
[25] Kumar, K., Bhattacharya, S., & Hicks, R. (2018). Employee perceptions of organization culture with respect to fraud–where to look and what to look for. Pacific Accounting Review.
[26] Luiijf, E., Besseling, K., & De Graaf, P. (2013). Nineteen national cyber security strategies. International Journal of Critical Infrastructures 6, 9(1-2), 3-31.
[27] Maahs, D. L. (2018). Managerial strategies small businesses use to prevent cybercrime.
[28] Manan, S.K.A., Kamaludin, N. and Salin, A.S.A.P. (2013), "Islamic work ethics and organizational commitment: evidence from employees of banking institutions in Malaysia", Pertanika Journal ofSocial Science andHumanities, Vol. 21 No. 4, pp. 1471-1489.
[29] Mat, B., Pero, S., Wahid, R., & Sule, B. (2019). Cybersecurity and Digital Economy in Malaysia: Trusted Law for Customer and Enterprise Protection. International Journal of Innovative Technology and Exploring Engineering.
[30] Mat, T. Z. T., Nazri, S. N. F. S. M., Fahmi, F. M., Ismail, A. M., & Smith, M. (2013). Assessing the fraud prevention mechanisms in Malaysian government agencies. Management & Accounting Review (MAR), 12(2), 141-169.
[31] Maulidi, A., & Ansell, J. (2020). The conception of organizational fraud: the need for rejuvenation of fraud theory. Journal of Financial Crime.
[32] Michael, K., Kobran, S., Abbas, R., & Hamdoun, S. (2019, November). Privacy, data rights and cybersecurity: Technology for good in the achievement of sustainable development goals. In 2019 IEEE International Symposium on Technology and Society (ISTAS) (pp. 1-13). IEEE.
[33] Nawawi, A., & Salin, A. S. A. P. (2018). Employee fraud and misconduct: empirical evidence from a telecommunication company. Information & Computer Security.
[34] Oluwagbemiga, O.A., 2010. The role of auditors in fraud detection, prevention and reporting in Nigeria.Library Philosophy and Practice (ejournal). Retrieved on 20 December 2014 from http://digitalcommons.unl.edu/libphilprac/517
[35] Othman, R., Aris, N. A., Mardziyah, A., Zainan, N., & Amin, N. M. (2015). Fraud detection and prevention methods in the Malaysian public sector: Accountants' and internal auditors' perceptions. Procedia Economics and Finance, 28, 59-67
[36] Perumal, S., Pitchay, S. A., Samy, G. N., Shanmugam, B., Magalingam, P., & Albakri, S. H. (2018). Transformative cyber security model for Malaysian government agencies. International Journal of Engineering and Technology (UAE).
[37] Pickett, S. 2012. The Essential Guide to Internal Auditing. Pristina, Kosovo.
[38] PriceWaterhouseCoopers (PWC) (2003), Global Economic Crime Survey 2003, available at: www. pwcglobal.com/extweb/ncsurvers.nsf
[39] Rahman, R.A., Anwar I.S.K., 2014. Effectiveness of fraud prevention and detection techniques in Malaysia Islamic Banks.Procedia – Social and Behavioral Sciences 145, 97-102.
[40] Securities Commission (2007), "Commission guidance regarding management's report on internal control over financial reporting under section 13(a) or 15(d) of the Securities Exchange Act of 1934", available at: www.sec.gov/rules/interp/2007/33-8810.pdf (accessed 31 January 2017).
[41] Smith, G.S., 2012.Can an auditor ever be a first responder to financial frauds? Journal of Financial Crime, 19(3), 291 – 304.
[42] Thabit, T., Solaimanzadah, A., & Al-abood, M. T. (2017). The Effectiveness of COSO Framework to Evaluate Internal Control System: The Case of Kurdistan Companies. Cihan International Journal of Social Science, 1(1), 44.
[43] Thomas, A.R. and Gibson, K.M. (2003), "Management is responsible, too", Journal of Accountancy, April, pp. 53-55.
[44] Vinten, G., Alleyne, P., & Howard, M. (2005). An exploratory study of auditors' responsibility for fraud detection in Barbados. Managerial Auditing Journal.
[45] Wolfe, D.T. & Hermonson D.R. (2004). The Fraud Diamond: Considering the Four Elements of Frauds, The CPA Journal 74.12, 38-42.
[46] Zabihollah, R., & Richard, R. (2005). Prevention and Detection.
[47] Zahari, A. I., & Arshad, R. (2019). FRAUD DEVELOPMENT AND LINKAGES WITH CORRUPTION OCCURRENCES. Journal of Governance and Integrity, 2(2), 65-76.