Macrothink Institute™

Business and Economic Research
ISSN 2162-4860
2019, Vol. 9, No. 1

Evaluating Information Security System Effectiveness for Risk Management, Control, and Corporate Governance

Mouhamadou Sow (Corresponding author), DBA, MBA, CFE, CRMA, ITIL

School of Management, University of Phoenix, City University of Seattle, National American University, Texas Wesleyan University, United States

Tel: 1-716-867-3214 Email: msow@national.edu

Christina Gehrke, MBA, CPA, CMA, CIA

School of Management, City University of Seattle

521 Wall Street, Seattle, Washington 98121, United States

Tel: 1-206-239-4867 E-mail: cgehrke@cityu.edu

Received: December 4, 2018 Accepted: December 20, 2018 Published: January 29, 2019

doi:10.5296/ber.v9i1.13994 URL: https://doi.org/10.5296/ber.v9i1.13994

Abstract

Using Grounded Theory, this study addresses factors related to forensic accounting, as well as various issues that can arise due to lack of security measures. The study identifies issues related to lack of security measures and cybersecurity crimes, and their impact on corporate-governance practices within organizations. This qualitative research study was phenomenological in nature and participants included a group of twelve employees in the field of forensic accounting, auditing, and information security systems across several organizations in the Southwest United States who were interviewed about cybersecurity and information security. Specific research literature provides a framework for this study, indicating the need for information technology that reinforces data safety and increases the effectiveness of corporate governance. The forensic accounting system depends on auditing and risk-control factors because in their absence, organizations may be unable to keep data confidential. Larger firms must adopt security measures that advanced technology provides within the accounting system to help develop fairness and transparency within the forensic accounting system. The study proposes means of increasing good corporate-governance practices and decreasing the risk in larger organizations using the latest technology.

Keywords: Forensic accounting, Auditing, Information security, Information systems, Governance, Risk, Controls

1. Introduction

The vulnerability of forensic accounting increasingly calls for the participation of information security teams that stay current with the field of digital forensics. Information security normally defines the role of forensic accounting in gathering account-related information produced in the course of doing the business of the organization. In such a role, information security usually resides in and depends upon accounting applications and operating systems. However, the more important role of the organization's information security team is to work closely with the forensic accountants to clarify and support their objectives from a business perspective (Klimburg & Zylberberg, 2015). Since computers preserve all accounting data, information security systems must ensure that only the right people have access to the accounting data. Access control helps the forensic accountants to monitor the accuracy of the data extracted and the effectiveness of forensic accounting depends on all processes in information security.

This study evaluated the performance of the information security systems in organizations and audit, with respect to the forensic accounting initiatives related to risk management, control, and corporate governance. Information security systems enables forensic accountants to verify the validity of firewall logs and access, Intrusion Detection Systems (IDS) data, and transaction rights that are all important to maintaining controlled access to forensic accounting data, which are significant in managing bankruptcy, business valuation efforts, and misallocation of funds (Williams, 2015). Insurance claims may also trigger a forensic accounting event in determining worth. Forensic data plays the key role in proving fraud in forensic accounting (Van Akkeren & Buckby, 2017).

Information security auditing is a relatively new concept in the field of information technology (Simkin, Norman, & Rose, 2014). However, this quickly growing subject is at the cutting edge of the cybersecurity field and corporate-risk control and management. Information security auditing assesses and ensures that the computerized system of an organization performs exactly as designed, and the additional technology to protect those systems also works as designed to secure the systems and data properly (Klimburg & Zylberberg, 2015). The level of the accounting expertise in the organization might constitute a source of stress if the latest technology skills are lacking.

The purpose of evaluating information security is to assure that the controls are in place to manage risk and these controls are working as designed. This research sought to understand the issues related to lack of security measures, cybersecurity crimes, and their impact on corporate-governance practices within organizations. Evaluation of the organization's information security auditing and forensic accounting may be a future goal of the organization, which it must achieve to consider governance, risk management, and implementation of effective controls. The study indicates the factors related to forensic accounting, as well as various issues that can arise due to lack of security measures, and considers governance, control, and risk-management aspects.

Information security enables forensic accountants to confirm the validity of Intrusion Detection Systems (IDS) data, firewall logs, and access and transaction rights. Controlled admittance to accounting data is imperative, and this study aimed to use these forensic accountants and accounting data that is important to avoiding fraud in organizations (Van Akkeren & Buckby, 2017).

2. Literature Review

A literature review evaluates different types of research articles and studies that pertain to the topic in question and the research question(s) under consideration. The role of the literature review in any type of research study (qualitative or quantitative) is to offer evidence, identifying prior evidence (if it exists) to support the present hypothesis, and to determine its applicability in real-world settings. Because the research focused on the evaluation of the organization's information security auditing and forensic accounting initiatives related to governance, risk, and control within the organization, this section includes various studies that explain the information security system, auditing of the information security system, risks due to hackers, frauds related to the accounting, and risk-mitigating controls. Cybersecurity attacks is considered one of the biggest corporate risks and economic threats to the United States (Iyengar, Land, & Moffie, 2017). The magnitude of this risk was demonstrated by the Equifax cyber-attack where intruders accessed the personal data of about 143 million consumers in the United States (Equifax fallout, 2017).

The information security system must be balanced with proper measures that can assist in reducing the impact of cybersecurity risks and tracking cybersecurity threats. An information security system can help control risks and contribute to adequate corporate-governance practices. Internal auditors working closely with the information technology professionals can assess and ensure adequate measures are implemented to protect companies from cybersecurity threats (Iyengar et al., 2017).

Information system relates to the hardware, software, data, controls, procedures, and people within an organization (Guragai, Hunt, Neri, & Taylor, 2015), all these elements require adequate management and effective information management systems (IMS) to keep the organization's confidential information strictly private and maintain that privacy with the help of specific controls (security control) (Klimburg & Zylberberg, 2015). Lack of such controls can lead to risks of information outflow. Organizations need to assess whether they have adequate controls and oversight with the increasing risk of cybersecurity crime (Iyengar et al., 2017). Adequate controls include not only sound physical controls and a cybersecurity framework but a security culture throughout the organization (Iyengar et al., 2017). For those organizations that do not take the additional time to assess adequate controls or devote adequate resources to prevent security breaches to protect investors and customers there are potential penalties from regulatory agencies and other legal consequences (Iyengar et al., 2017).

The staff responsible for managing accounting data must have proper skills, education, and techniques for reducing the risks related to organizational information security (Klimburg & Zylberberg, 2015). Small organizations and those in emerging markets that do not have

adequately skilled employees risk greater chances of fraud and disloyal actions (Martinez-Figueroa, 2015).

Anderson, Bozek, Longstaff, Meitzler, and Skroch (2000) indicates the need for effective risk control using proper models and frameworks, as the risk facing the information security threatens governance of organizations. Furthermore, Cawi (2017) explains the role of the forensic accountants and various issues within the organization using forensic transactions, including confiscation, matrimonial disputes, unexplained wealth, and unauthorized financial valuation (Cawi, 2017). These are the risks threatening the firm and may require documentation for claiming damages during court procedures. A practice of prosecution of suspected employees can minimize threats toward information security.

According to Bhasin (2016), an appropriate forensic accounting system particularly in emerging economies helps to identify the level of corporate governance. In regions like Asia, the corporate-governance level of emerging organizations depends on the methods used for forensic accounting and auditing (Bhasin, 2016). The main issues arise from the ineffective internal controls and information leakage by employees, which reduce the overall effectiveness of corporate governance (Jusoh et al., 2018). The accounting information system (AIS) involves certain mandates that investigations must fulfill (Guragai et al., 2015). Currently organizations have cybersecurity systems that help to protect big data that is needed to conduct business. Most organizations with big data uses the data to find consumer information and keep the data records in a database (Kopp, Kaffenberger, & Jenkinson, 2017). Hackers attack the big data databases of the organization to execute their mission of doing significant damage to organizational information (Kopp et al., 2017). The cybersecurity controls that manage the data within a system can control significant risk exposure of the big data (Eastman, Versace, & Webber, 2015). Lowe, Bierstaker, Janvrin, and Jenkins (2017) studied improvement in the auditing system of an organization and suggested information technology as one of the useful tools that can help work in the accounting system to control errors (Lowe et al., 2017). Information technolgy issues may arise while in use for auditing, depending on the size of the organization that has implemented the system. Mergers and acquisitions can also play a negative role and increase the risk to security (Sherer, Hoffman, Wallace, Ortiz, & Satnick, 2016). Data privacy is a big problem for the companies during mergers and acquisition activities. Employees may choose to leak information to receive large amounts of money from competing organizations endangering corporate-governance activities (Williams, 2015).

This study focuses on the factors related to forensic accounting, as well as various issues that can arise due to lack of security measures. The existing literature supports the need of information technology for data safety that increases the effectiveness of overall corporate governance. A forensic accounting and security systems is based on auditing and risk-control factors, because in their absence the organization may be unable to keep the data private. As noted above, cybersecurity attacks is considered one of the biggest corporate risks and economic threats (Iyengar et al, 2017). Larger firms face increased threat exposure to their big databases that hackers can attack as demonstrated by the Equifax cyber-attack where intruders accessed the personal data of about 143 million consumers in the United States

(Equifax fallout, 2017). An urgent reason for properly securing the information technology in an organization to reduce the risk exposure to cybersecurity attacks.

3. Method

This qualitative research study was phenomenological in nature and based upon an interview method that utilized the various studies to explain information accounting systems, auditing of the information security system, risks due to hackers, frauds related to accounting, and risk-mitigating controls. Primary-data collection techniques used for fresh data collection were based on the research problem. Data was collected by interviewing twelve members of the Association of Certified Fraud Examiners (ACFE), and Information Systems Audit and Control Association (ISACA), located in Southwest United States. The twelve members included information security auditors (5), accountants (2), information security analyst (1), and information system managers (4) of various organizations. The members all held various professional credentials included Certified Public Accountant (CPA), Certified Fraud Examiner (CFE), Certified Information Security Auditor (CISA), Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM). The members interviewed were considered professionals in the field and knowledgeable about the research problem. The research problem focused on the lack of specialized skills on staff in the organization and lack of Internet security protocols to secure the information in the accounting systems. The research problem took into consideration the increasing number of fraudulent activities resulting from fewer security measures implemented by forensic accounting.

Researchers face many legal and ethical challenges when conducting their studies (Watts, 2011). In every study, researchers must comply with applicable code of conduct, legal requirements, and social responsibilities (Van Deventer, 2009). The researchers in this study collected and analyzed data collected from the interviews and present findings while avoiding bias, respecting ethical standards, and protecting the rights of participants.

Primary data was collected through interviews, then analyzed with the help of qualitative measures. Assumptions based on data measures were developed so that the answers of the interviewed professionals related to the research problem. The match between the interviewees responses and the research problem revealed the suggested solution, based on primary and secondary-data analysis. The primary data helped to analyze some observations highlighted during the interviews. The selections of the interviews were based upon the perceptions of twelve professionals and their express knowledge of information security, information security systems, risk, control, and corporate governance. Each individual face-to-face interview conducted for this study was 30-45 minutes in length using a set of semi-structured interview questions (Patton, 2015) and additional time for other responses and feedback. The actual questions during the interviews were fluid rather than ridged to be semi-structured and result in more in-depth discussion (Yin, 2015). For example, when asked “What are the information security & forensic accounting initiatives in your organization and what are the challenges”? One of the participants responded that our information security teams are asked to participate in forensic accounting because of their knowledge on digital

forensic realm. Information security supports the accounting team by working closely with our functional areas for access control and help accountants that the data they are pulling is accurate. They also support our team by being able to provide access to and verify the validity of firewall logs, who has logical access, group right and transaction rights. They also discussed the importance of awareness through evaluation of the controls.

Based on Grounded Theory, used by many Information Systems researchers, this study emerges in the "voice" of participants (Halaweh, 2012). The theory involves generating theory from given source data. Interviews were used to collect the data for this study. The responses were coded, the codes grouped into concepts, and relationships between concepts were analyzed and classified into categories for potential findings. Since the interviews were recorded, the researcher transcribed the data to identify pattern among the responses.

4. Results

The findings of this study confirm that information security teams should be completely aware of the techniques concerning fraud risk assessment, and necessary steps should be taken in this regard (Kopp et al., 2017). The findings indicate there is a high risk towards the accounting system that can only be controlled by using security protocols. Creating awareness through the implementation of the controls using technology and through evaluation of the controls after a implementation period is necessary. There is also a need to realize the greater level of risk associated with third-party Virtual Private Networks (VPN), Internet, dial-in lines and deciding which of the information security teams to assess (Eastman et al., 2015). This study found the need to increase the corporate-governance practices in larger organizations using the latest technology. The results of the study confirmed the findings of Bhasin (2016) that audit of the forensic system can help to reduce fraud, calling for auditing using both internal and external audits. Organizations that have strict security checkups of the forensic accounting technology have good corporate-governance practices. The new findings relate to the insecure measures of the organizations and the ignorance of the managers about how to keep data secure. The secondary data reported in the literature review elaborates on how the lack of security keeps the firms at risk and potential damages that can occur in the future. Larger firms must adopt security measures with advanced technology within the accounting system, which can help to develop fairness and transparency within the forensic accounting system.

5. Discussion

The current study can use quantitative research methods for more elaborate, clarified results, to help make organizations aware of keeping skilled accountants, as well as to focus on the security system of the software used for their forensic accounting system. The organizations should also focus on securing the private data (e.g., transactions) through online platforms. Information security looks at the forensic accounting from a perspective of fraud-suspicion and awareness of the risk, by identifying the ways the data of the organizations can come under threat and be vulnerable and how to reduce risk of such occurrences. Further research can include deeper inquiry into developing an understanding about the types of security measures that are effective for reducing data theft/leakage as well as the impact of these

measures on the financial accounting system of the organization. In the further investigations the comparing and contrasting software and the internet security protocols can add value towards effective forensic accounting systems. Future researchers could use quantitative research with a larger sample size to find more accurate results through statistical data.

6. Conclusion

This research project has elaborated on the importance of an information security in the forensic accounting system to enable the organization to take steps toward risk management, governance, and control, with the help of a proper auditing practices. The organization's information security team can prove helpful in facilitating security systems. Auditing the forensic systems can help to reduce fraud and the best way to prevent fraud is to establish an effective internal control system using a good control environment (Bhasin, 2016). This research project concludes that information security systems hold great importance for the forensic accounting system, which in turn helps the organization to take appropriate steps to manage risks, governance, and control with the help of an appropriate audit system. Information security looks at forensic accounting from a perspective of fraud-suspicion, awareness of risk, and the ways the accounts of the organization can become under threat and vulnerable, to prevent such cases.

References

Anderson, R. H., Bozek, T., Longstaff, T., Meitzler, W., & Skroch, M. (2000). *Research on mitigating the insider threat to information systems-# 2* (No. RAND-CF-163-DARPA). Rand National Defense Research Inst Santa Monica CA.

Bhasin, M. L. (2016). Contribution of Forensic Accounting to Corporate Governance: An Exploratory Study of an Asian Country. *International Business Management, 10*(4), 479-492. http://dx.doi.org/10.2139/ssrn.2676488

Cawi, I. (2017). Expert report under scrutiny: A discursive construction of the role of a forensic accountant expert. (Unpublished Doctor of Philosophy thesis, School of Accounting, Economics and Finance, University of Wollongong, Australia). [Online] Available: https://ro.uow.edu.au/theses1/19

Eastman, R. Versace, M., & Webber, A. (2015). Big Data and Predictive Analytics: On the Cybersecurity Front Line. *IDC Whitepaper #254290*.

Equifax fallout. (2017). *Property Casualty 360-National Underwriter, 121*(10), 15.

Guragai, B., Hunt, N. C., Neri, M. P., & Taylor, E. Z. (2015). Accounting information systems and ethics research: Review, synthesis, and the future. *Journal of Information Systems, 31*(2), 65-81. https://doi.org/10.2308/isys-51265

Halaweh, M. (2012). Integration of grounded theory and case study: An exemplary application from e-commerce security perception research. *Journal of Information Technology Theory and Application, 13*(1), 31-51

Iyengar, R. J., Land, J. K., & Moffie, R. P. (2017). Cyber Insecurity: What Internal Auditors

Need to Know. *Internal Auditing, 32*(6), 15-23. [Online] Available: http://proxy.cityu.edu/login?url=https://search-proquest-com.proxy.cityu.edu/docview/1973321522?accountid=1230

Jusoh, Y. Y., Nor, R. N. H., Pa, N. C., Yahaya, J. H., Bakri, H., Maryann, N. E., & Zawawi, M. R. (2018). Knowledge Management in Forensic Accounting: The Future Trends. *Advanced Science Letters, 24*(7), 5212-5215. https://doi.org/10.1166/asl.2018.11704

Klimburg, A., & Zylberberg, H. (2015). *Cyber security capacity building: Developing access*. Oslo: Norwegian Institute of International Affairs.

Kopp, E., Kaffenberger, L., & Jenkinson, N. (2017). *Cyber risk, market failures, and financial stability*. International Monetary Fund

Lowe, D. J., Bierstaker, J. L., Janvrin, D. J., & Jenkins, J. G. (2017). Information Technology in an Audit Context: Have the Big 4 Lost Their Advantage?. *Journal of Information Systems, 32*(1), 87-107. https://doi.org/10.2308/isys-51794

Martinez-Figueroa, D. (2015). *Examining the growing need for trained forensic accountants in Puerto Rico: A case study.* (Ph.D. dissertation, Northcentral University, AZ). ProQuest Number: 10003792

Patton, M. Q. (2015). *Qualitative Research & Evaluation Methods: Integrating Theory and Practice (4th ed.)*. Thousand Oaks, California: SAGE Publications, Inc.

Sherer, J. A., Hoffman, T. M., Wallace, K. M., Ortiz, E. E., & Satnick, T. J. (2016). Merger and acquisition due to diligence part II-the devil in the details. *Richmond Journal of Law & Technology, 22*(2), 4.

Simkin, M. G., Norman, C. S., & Rose, J. M. (2014). *Core concepts of accounting information systems*. John Wiley & Sons.

Van Akkeren, J., & Buckby, S. (2017). Perceptions on the causes of individual and fraudulent co-offending: Views of forensic accountants. *Journal of Business Ethics, 146*(2), 383-404. https://doi.org/10.1007/s10551-015-2881-0

Van Deventer, J. P. (2009). Ethical considerations during human centered overt and covert research. *Quality and Quantity, 43*(1), 45-57. https://doi.org/10.1007/s11135-006-9069-8

Watts, J. H. (2011). Ethical and practical challenges of participant observation in sensitive health research. *International Journal of Social Research Methodology, 14*(4), 301-312. https://doi.org/10.1080/13645579.2010.517658

Williams, A. (2015). *Forensic criminology*. London: Routledge.

Yin, R. K. (2015). *Qualitative research from start to finish (2nd ed.)*. New York, NY: Guilford Press.