Effective Dealing with Insider Threats a Comparison of Qualitative and Quantitative Research

Chamara Withanachchi[1*]

[1]*IIC University of Technology, Cambodia.*

Author's contribution

The sole author designed, analysed, interpreted and prepared the manuscript.

Review Article

ABSTRACT

This paper studies and compare qualitative and quantitative research paper to find what research methodology is having disengages and disadvantages of such research. This paper is based on mainly two articles to do the said comparison. This will be discussed about the relevant articles that have been selected on the main theme of the research study. It can be understood that these findings are also based on the literature review of the study because all the data are gathered from secondary resources.

1. INTRODUCTION

In this study, there are different identifications of the research studies, aims, and objectives along with the research questions and rationales. Moreover, the identification of the research philosophy and discussing the research design.

This will be discussed about the relevant articles that have been selected on the main theme of the research study. It can be understood that these findings are also based on the literature review of the study because all the data are gathered from secondary resources. It can be observed that there are also different kinds of

_____

*Corresponding author: E-mail: chamaraw@rpgiv.info;

methods of literature that are discussed in the study. There are also different types of discussions on the research design as well as strategies and those are used in each research article [1]. There are also different types of research methods in the literature review used in these two articles that are chosen based on the theme. It can be noted that there are also different and relevant discussions of design and strategy that have been used in each of the studies and there will also be some kinds of discussions that are also related and attached to the descriptive piece of literature review, which are dealt with the "Effective dealing with insider threat of corporates".

People are the single largest vulnerability to security. The risk of insider threat is increasingly prevalent and requires comprehensive mitigation strategies. Insider threats can be grouped into three categories: malicious users that deliberately attempt to cause damage, oblivious users whom cause damage by 'cutting corners' and disregarding extant business processes, and external users who use legitimate, authorised credentials to cause damage, or exfiltrate information with malicious intent [2].

2. IDENTIFICATION OF THE RESEARCH STUDIES, AIMS AND OBJECTIVES, RESEARCH QUESTIONS AND RATIONALES (ARTICLE "A")

In this section, the research studies, aims and objectives, research questions, and rationales of article A that is chosen on the "Effective dealing with insider threat of corporates" have been discussed. The first article that is chosen on the theme is "A New Take on Detecting Insider Threats: Exploring the use of Hidden Markov Models" [3]. It can be noted that this article is written by three authors. It describes the threats of the malicious insiders that affect the possible organizational culture as well as the business environment at the same timeframe. In this study, there are new detectors of insider threats with the help of hidden Markov models.

The research aim of the journal article is given below

It can be observed that the main module or the journal paper has aimed to design their systems, whereas each of the components can be alternated without replacing the other variables. Therefore this alteration allows the employees to use their critical thinking and also re-thinking for the entire system [4]. However, the main aim of

the article is to articulate the whole usefulness and utility of the HMM model for detecting the core inside threats. On the other hand, there are also some of the important parts that will be also discussed in the study regarding the HMM model [5]. On the other hand, it can be observed that the researchers have also aimed to use the approach that is related to anomaly detection and also using the normal behavior of the users as the core sequence.

Research Objectives and Questions are listed below

- To identify the threat of the organizational computer system to the insiders
- To identify the core advances of the insider threats in the organizational culture
- To assess the degree of harm of the insider threats to the industry and also research towards prevention and detection.

Research Questions

- What is the threat of the organizational computer system to the insiders?
- What are the core advances of insider threats in the organizational culture?
- How the degree of harm of the insider threats to the industry and also research towards the prevention and detection can be measured?

2.1 The Rationale of the Study

The main rationale of the study includes different types of problems and issues that are used in the research article for identifying insider threat detections. The tools and techniques are also used for the machine learning task. The research paper can contribute to the main development and testing, that is based on the novel methods. It can be done with the help of the hidden Markov model, which helps to learn the normal behavior and identifying the deviations, those are the main indications of the threat. There are also different types of ventures and categories, by which the researchers are much able to detect the insider's threats within the limited timeframe [6].

On the other hand, a defined system has also been described in the study that includes the identification of the "reasonable false-positive rate". Therefore, "Effective dealing with insider threat of corporates" can be done with the help of HMM model and it also determines the rate of human deviation from their behavior [7]. Apart from that, the HMM model also is used to

visualize the models and helping the researchers to gain the most pertinent information that includes severe repercussions within the organizational culture.

2.2 Identification and Discussion of the Research Philosophy Underpinning the Rationale For the Research Design in Each Study, Concerning Research Methods Literature. Use of Relevant Extracts (Article "A")

In the case of the identification and discussion of the research philosophy, there are different rationale of research design. In the article, "A New Take on Detecting Insider Threats: Exploring the use of Hidden Markov Models", positivism philosophy is used where the researchers have clearly described the problems and mitigating solutions for insider threat detection. Different aspects are used in the case of "user's normal behavior". There are also different types and natural choices of modeling the products that help in finding the anomalous sequences in the dataset [8]. With the help of positivism research philosophy, the Hidden Markov Models (HMM) have been presented in the best possible manner. There are also some of the important formulae, like the Hidden Markov Model that can be substantially presented with the help of positivism research philosophy.

In this section, it can be observed that the research philosophy that has been selected in the study underpinning the research rationale. Based on the whole research rationale, the whole discussion in this section is elaborated. There are different types of research methodologies, by which the design instruction detection system can be utilized. With the help of positivism research philosophy helps to find out the ideal candidates for the consideration of insider-threat detection. There are also different dimensions of the CERT database, which contains different types of Log files and also describes different kinds of activities at the same timeframe.

2.3 Discussion of the Research Design and Strategy Used in Each Study Using the Research Methods Literature (Article "A")

It can be observed that the study has a research design that is based on the anomalous behavior indicator. It is one of the important research designs that help find out insider threats. It can

be observed that different kinds of aspects are related to the normal intrusion systems that are much relevant to events regarding malicious activities in general [9]. On the other hand, the research design is also very helpful for correlating the main aims and objectives of the study with insider threat detection. With the help of this research design, the pipeline of the whole study is also based accurately, that are modular in shape. There are also different types of arrangements that are placed within the format of the research design and the features can be also used in an alternative manner. On the other hand, the model can also be changed accordingly to the feedbacks and the models can also be changed completely without simultaneously having proper feedbacks and components.

2.4 Discussion of the Design and Use of Data Collection Tools Concerning Research Methods Literature (Article "A")

In this article, which is based on "A New Take on Detecting Insider Threats: Exploring the use of Hidden Markov Models", the data collection methods are applied and described. In this section, the design, as well as the data collection tools regarding the literature of the study, are elaborated. The data collection processes have been ventured with the help of user's actions that are completely based on the insider threat suggestions [10]. It also collaterally retrospects to the core behavior and personal characteristics those are equally important for the researchers while developing the article based on "A New Take on Detecting Insider Threats: Exploring the use of Hidden Markov Models". On the other hand, relevant datasets are also collected from the basic actions that are derived from the basic actions and proformas of the HMMs [11].

3. IDENTIFICATION OF THE RESEARCH STUDIES, AIMS AND OBJECTIVES, RESEARCH QUESTIONS AND RATIONALES (ARTICLE "B")

The title chosen for the second article is "Corporate Governance Issues and Control in Conditions of Unstable Capital Risk", which have been published by the "International Journal of Economics and Financial Issues". This article has been chosen on the main theme of the study that is related and attached to the "Effective dealing with insider threat of corporates". However, it can be understood that the main aim

of the study includes issues regarding corporate governance and control in different conditions of inappropriate capital risks. This article is related to insider threats, which will be explained while demonstrating the objectives and research questions of the study.

It can be noted that the research objectives of the study are listed below

- To identify the initial division of property that ended in the dominance of the bank's participation
- To identify the methods for assessing new private corporations that were accompanied by insider abuse and violations of the social rights in Russia
- To assess the specific motivations of many insiders that includes large shareholders and managers.

The research questions are also described below

- What are the methods to identify the initial division of property that ended in the dominance of the bank's participation?
- What are the methods for assessing new private corporations that were accompanied by insider abuse and violations of social rights in Russia?
- How the assessment of specific motivations of many insiders that includes the large shareholders and managers can be done in the best possible manner?

There is no doubt that corporate governance is a system of relationships between managers, the board of directors, shareholders and stakeholders on the management of the company [12].

4. THE RATIONALE OF THE STUDY

The main title of the study is "corporate Governance Issues and Control in Conditions of Unstable Capital Risk", which happens due to insider threats and problems. It can be understood that there are also different types of assumptions that are also included in the same situation are also explained in the study. It can be understood that there are different types of governance issues and controls in conditions where capital risks are engraved within it. On the other hand, it can be observed that there are also different types of notifications regarding "deep and wide-ranging transformations" of the Russian Economy that have been caused due to several technological as well as scientific

processes [13]. It also involves different aspects of formulations that have elements like a market economy as well as political democracy. Moreover, the main role that is played has a deep connection with the corporate governance practice. In this concept, there are also different types of large corporations that are engaged within the der practices and harm the economical growth or development of the country. There are also some of the important characteristics of the "Effective dealing with insider threat of corporates", where the appearance of the national economy is very important and therefore competition increases with the international as well as from the domestic sources. Some threats are related to scrupulous corporate threats [14]. Due to this core reason, there are some possibilities regarding the formal approach of the disclosure. There are also different standards regarding "agency standards", where more than 50% of Russian companies are in the possibilities of presenting the disclosure.

4.1 Identification and Discussion of the Research Philosophy Underpinning the Rationale for the Research Design in Each Study, Regarding Research Methods Literature. Use of Relevant Extracts (Article "B")

In this research study, the interpretivism research philosophy is used, where the perspectives of corporate governance are used greatly. There are also different types of insider thoughts and proximities, where the core effectiveness of management can be integrated [15]. There are also different types of corporate group financial attitudes, where the quality of financial management is also shown correctly. It can be observed that there are different kinds of strategic as well as tactical businesses that show common problems within the corporates [16]. With the help of interpretivism research philosophy, there are also diverse aspects of systems related to corporate governance that can be covered with the help of structural relationships. There are different types of elements that are created for the diverse implementation of production and reproductions [17]. There are different ventures regarding streamlining of roles and diverse methods for implementing their interests in the same period.

In this specific section, there are different derivatives related to the rationale of the study. The rationale of the study also includes the initial division of property. Different aspects reflect the

core dominance of banks in Russia and allowed their participation in the industrial sector. Different methods are relative to the establishment of different banks. There are also different types of strategies that combine different types of debt financing and equity aspects [15]. Moreover, the interpretivism research philosophy has also helped the researchers, where new private corporations have also experienced different kinds of insider abuse. These abuses are also much harmful to corporate organizational culture.

4.2 Discussion of the Research Design and Strategy Used in Each Study Using the Research Methods Literature (Article "B")

The descriptive research design is followed in the study, which is based on the "Corporate Governance Issues and Control in Conditions of Unstable Capital Risk". With the help of descriptive research design, different types of activities related to corporate governance and insider abuses are noted in the study [18]. According to the classified situations in Russia, it can be understood that there are also non-governance types of features and thereby it develops the national model for the corporate governance that are also being distinguished with the help of the descriptive research design [12]. It can be featured with the help of the descriptive research design that there are different types of permanent processes that are eventually showcased by the insiders for damaging the whole portfolio for the core corporate loss. In this process, managers have learned to deal with the insider threats of the organizational culture.

Dealing with insider threats should not be implemented in an organization as an act of compliance& discipline but should be integrated with day to day activities of employees. Dealing with insider threats programs should be typically integrated with organizational goals like performance improvement, competitive edge, innovative practices and best practices identified within projects, and the general enhancement of knowledge for mitigating threats through a collaborative approach. Content is the subject matter contained in any document. It is the content that helps categorize a plain paper into a document. Content cannot exist by itself; it needs a container, and physical space to reside. A document without any content can still exist but will be called a plain piece of paper. The view is

that both content and document are interdependent. A term document is an easy connecter concerning Dealing with insider threats. Moreover, content typically in organizations means organizations` business capability and service offerings on their websites and other marketing collaterals. Content can be looked at as the essential component of explicit knowledge for mitigating threats [19]. Over a while, knowledge for mitigating threats industry has evolved and broadened the definition of content as existing in all kinds of physical formats including digital formats like text files, wikis, spreadsheets video, and audiotapes.

In the context of dealing with insider threats, a very clear understanding of content/data, information, and knowledge for mitigating threats are essential for any organization as each one has its processes and method of capturing sharing and reuse. Data is the raw material and is also a physical arrangement of numbers carrying signals. Devoid of any contextual value, data is inadequate for a meaningful transaction. Information is the cognitive arrangement of those signals. Data becomes information when it is supported by a context in a social environment [20]. One level up, it transforms into knowledge for mitigating threats when it provides the environment for constructive analysis and enables users to make decisions. Knowledge for mitigating threats arises out of a belief system on the physical arrangement of cognitive signals. This theory puts the onus of acquiring knowledge for mitigating threats converting information into knowledge for mitigating threats on the users wherein data and information serve as raw material.

4.3 Discussion of the Design and Use of Data Collection Tools Concerning Research Methods Literature (Article "B")

Detailed discussion, which is on the data collection tools are described in this section. It can be observed that there are different tools like the online website tools and techniques that are used in developing the whole journal article [21]. There is the maximum usage of the secondary resources that has been replicated and showcased in the primary order. There are also different types of data collection tools used in developing the research article that can be sourced with the help of the internet and webpages.

5. CONCLUDING DISCUSSION OF THE ADVANTAGES AND DISADVANTAGES OF ADOPTING A QUALITATIVE AND QUANTITATIVE RESEARCH DESIGN IN DEVELOPING KNOWLEDGE FOR MITIGATING THREATS WITHIN THE SPECIFIC FIELD THESE TWO STUDIES ADDRESS

There are some advantages and disadvantages of adopting qualitative and quantitative designs that help in the core development of knowledge and mitigating insider threats. It can be acknowledged that, in the case of qualitative and quantitative designs, the researchers get the affirming of real data that cannot be countered by any individual or external sources. On the other hand, there are also some of the disadvantages, where the big data in the form of qualitative and quantitative designs cannot be managed by a single group of researchers, and thereby it needs an analyst to draw up their every step.

6. LIMITATIONS

Although there is ample research on Insider Threats, research linking with quantitative and qualitative research methodologies. The available research is cross-sectional making comparisons impossible. And finally, due to time constraints, the number of papers reviewed is limited.

ACKNOWLEDGEMENT

COMPETING INTERESTS

Author has declared that no competing interests exist.

REFERENCES

1. Singh S, Tabassum N, Darwish TK, Batsakis G. Corporate governance and Tobin's Q as a measure of organizational performance. British Journal of Management. 2018;29(1):171-190.

2. Modini, Jessemyn; Vanzomeren, Mark; Fowler, Stuart; Joiner, Keith; Lynar, Tim. Rising to the challenge of insider threats for middle powers international conference on cyber warfare and security; reading; 2020.
DOI: 10.34190/ICCWS.20.131 pp 521

3. Rashid T, Agrafiotis I, Nurse JR. A new take on detecting insider threats: exploring the use of hidden markov models. In Proceedings of the 8th ACM CCS international workshop on managing insider security threats. 2016;47-56.

4. Admati AR, A skeptical view of financialized corporate governance. Journal of Economic Perspectives. 2017; 31(3):131-50.

5. Barnes P, Stock market efficiency, insider dealing, and market abuse. CRC Press; 2016.

6. Collie J. A strategic model for forensic readiness. Athens Journal of Sciences. 2018;5(2):167-182.

7. Daiser P, Ysa T, Schmitt D. Corporate governance of state-owned enterprises: A systematic analysis of empirical literature. International Journal of Public Sector Management; 2017.

8. Singsa A, Sriyakul T, Sutduean J, Jermsittiparsert K. Willingness of supply chain employees to support disability management at workplace: A case of indonesian supply chain companies. Journal of Computational and Theoretical Nanoscience. 2019;16(7):2982-2989.

9. Darrat AF, Gray S, Park JC, Wu Y. Corporate governance and bankruptcy risk. Journal of Accounting, Auditing & Finance. 2016;31(2):163-202.

10. De Wet PR, Incorporation of a corporate leniency policy ("CLP") under the financial markets act ("FMA") as a means to limiting insider trading (Doctoral dissertation, University of Pretoria); 2018.

11. Dion M. Corporate citizenship as an ethic of care: corporate values, codes of ethics and global governance. In Perspectives on corporate citizenship. Routledge. 2017; 118-138.

12. Lebedeva TE, Akhmetshin EM, Dzagoyeva MR, Kobersy IS, Ikoev SK. Corporate governance issues and control in conditions of unstable capital risk. International Journal of Economics and Financial Issues, 2016;6(1S).

13. Du L, Tang W, Liu C, Wang S, Wang T, Shen W, et al. Enhancing engineer–

procure–construct project performance by partnering in international markets: Perspective from Chinese construction companies. International Journal of Project Management. 2016;34(1):30-43.

14. Fennelly LJed. Effective physical security. Butterworth-Heinemann; 2016.

15. Gas IA, Abdallah AE. Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. Big Data Analytics. 2016; 1(1):6.

16. Jacoby SM, The embedded corporation: Corporate governance and employment relations in Japan and the United States. Princeton University Press; 2018.

17. Zey MG. The mentor connection: Strategic alliances within corporate life. Routledge. 2020.

18. Jain T, Jamali D, Looking inside the black box: The effect of corporate governance on corporate social responsibility. Corporate Governance: An International Review. 2016;24(3):253-273.

19. Liu L, De Vel O, Han QL, Zhang J, Xiang Y. Detecting and preventing cyber insider threats: A survey. IEEE Communications Surveys & Tutorials. 2018;20(2):1397-1417.

20. Milosevic T, Social media companies' cyberbullying policies. International Journal of Communication. 2016;10:22.

21. Padayachee K. An assessment of opportunity-reducing techniques in information security: An insider threat perspective. Decision Support Systems. 2016;92:47-56.

Peer-review history:
The peer review history for this paper can be accessed here:
http://www.sdiarticle4.com/review-history/65500