Faculty of Information and Communication Technology

DEVELOPING COST AND RISK ASSESSMENT TOOL FOR HYBRID APPROACH IN INFORMATION SECURITY RISK ANALYSIS

Ahmed Yaser bin Mohd Zabawi

Master of Science in Information and Communication Technology

2019

DEVELOPING COST AND RISK ASSESSMENT TOOL FOR HYBRID APPROACH IN INFORMATION SECURITY RISK ANALYSIS

AHMED YASER BIN MOHD ZABAWI

A thesis submitted
in fulfillment of the requirements for the degree of Master of Science in Information and Communication Technology

Faculty of Information and Communication Technology

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2019

DECLARATION

I declare that this thesis entitled “Developing Cost and Risk Assessment Tool for Hybrid Approach in Information Security Risk Analysis” is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature : …….

Name : …….

Date : …….

APPROVAL

I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in terms of scope and quality for the award of Master of Science in Information and Communication Technology.

Signature	:	…….
Supervisor Name	:	…….
Date	:	…….

DEDICATION

This thesis is dedicated to my parents, wife, family and my siblings.
For their love, support, help and encouragement.

ABSTRACT

Identifying potential information security risk is a challenging task which is due to modernization and new technologies which introduce possible threats to various type of digital system. Many studies proved that the current risk analysis tools are not able to analyze the threats well. It is a must for an organization to choose the suitable methods for better analysis. There are four key elements that need to be considered which are security threats, business impact, security measures and their cost. There are many existing risk analysis tools that were developed such as ISRAM and CORAS that have same purpose, which is to reduce the risk of causing a threat, however these tools used different approach to analyses the risk. The main focus of this study is to develop a new risk analysis tool based on hybrid approach and compare it with the existing tool. The proposed risk analysis tool is known as Cost and Risk Assessment tool (CARA) aims to trace the threats by combining both qualitative and quantitative methods, where both of these methods have their respective advantages for analyzing the information. CARA used Monte Carlo method where it applied probability theory in cost estimation. The results from the study show that the qualitative information could increase the dimension of risk factors and produce better accuracy in the analysis.

ABSTRAK

Mengenal pasti potensi risiko keselamatan maklumat adalah tugas yang mencabar, disebabkan oleh pemodenan dan teknologi baru yang memperkenalkan kemungkinan ancaman kepada pelbagai jenis sistem digital. Banyak kajian membuktikan bahawa alat analisis risiko sekarang tidak dapat menganalisis dengan baik. Adalah satu kemestian bagi sesebuah organisasi untuk memilih kaedah yang sesuai untuk analisis yang lebih baik. Di samping itu, terdapat empat elemen utama yang perlu dipertimbangkan iaitu ancaman keselamatan, kesan perniagaan, langkah keselamatan dan kos. Terdapat banyak alat analisis risiko yang telah dibangunkan setiap tahun seperti ISRAM dan CORAS di mana mempunyai tujuan yang sama, iaitu untuk mengurangkan risiko yang menyebabkan ancaman kepada organisasi, tetapi alat tersebut cuba untuk selesaikan risiko dengan pendekatan yang berbeza. Tujuan utama kajian ini adalah untuk membangunkan alat analisis risiko yang baru berdasarkan pendekatan hibrid dan membandingkan dengan alat analisis risiko yang sedia ada. Alat analisis risiko yang dicadangkan dikenali sebagai Cost and Risk Assessment Tool (CARA) bertujuan untuk mengesan ancaman dengan menggabungkan kedua-dua kaedah kualitatif dan kuantitatif, dimana kedua-dua kaedah ini mempunyai kelebihan masing-masing untuk menganalisis maklumat. CARA menggunakan kaedah Monte Carlo di mana ia menggunakan teori kebarangkalian di dalam penganggaran kos. Keputusan dari kajian menunjukkan bahawa maklumat kualitatif dipercayai dapat meningkatkan dimensi faktor risiko dan menghasilkan ketepatan yang lebih baik dalam analisis.

ACKNOWLEDGEMENTS

Firstly, I would like to thank Allah for giving me the strength and chance to finish my study. I would like to acknowledge my gratitude to both of my supervisors, Prof. Ts. Dr. Rabiah Ahmad and Dr. Shekh Faisal Abdul-Latip for their supports and guidance throughout my study. To my beloved parent, Mohd Zabawi Abdullah and Mashitoh Abdul Rahman, thank you for their motivation, moral support and financial assistance in order for me to finish my study. To my wife, Nur Amalina Mohamad Hazawawi, thank you for your support and words of encouragement. It was a great help throughout the course of this research work. I would also like to thank to all who have given full cooperation throughout in completing my study.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATIONS

ALE	-	Annual loss expectancy
ARO	-	Annual rate of occurrence
CARA	-	Cost and risk assessment
CRAMM	-	CCTA risk analysis and management method
FRAP	-	Facilitated risk analysis process
ISRAM	-	Information security risk analysis method
PTA	-	Practical threat analysis
SLE	-	Single loss expectancy

LIST OF PUBLICATIONS

1. Ahmed Yaser Mohd Zabawi, Rabiah Ahmad and Shekh Faisal Abdul-Latip, 2016. An Analysis Technique for Cost Estimation in Information Security. *5th International Cryptology and information Security (CRYPTOLOGY2016).*

2. Ahmed Yaser Mohd Zabawi, Rabiah Ahmad, and Shekh Faisal Abdul-Latip, 2015. Analyzing Numerous Factors of Risk Analysis in Information Security. *ARPN Journal of Engineering and Applied Sciences*.

3. Ahmed Yaser Mohd Zabawi, Rabiah Ahmad, Siti Zarifah Sarif and Siti Rahayu Selamat, 2014. A Dynamic Analysis on Information Security Risk Factors and Risk Analysis Tools. *MUCET*.

CHAPTER 1

INTRODUCTION

Information security played an important role in various parties, it was the core of the business not only to computer experts but the manager who had responsible for ensuring data security. In order to get more accurate output and comprehensive view of the risks that might be encountered, information about the covered entity was required as well as related information such as details information about business partners. Due to the success and continuity of organizations vastly depended on the availability and effectiveness of information technologies, protection of information was highly on demand and more critical than ever. In information security life cycle, risk analysis process will be affected by all these changes. Risk analysis used to play a major role in recognizing security controls to ensure computer and related structures (Gerber and Von Solms, 2001). The process included analysis and determining, where it was used to ensure that information systems assets are protected against accidental or deliberate damage, and unforeseen events. Risk analysis technique was categorized into two; which were qualitative and quantitative. In evaluating field, there were three aspects need to be considered which were information security risk analysis, information security risk analysis assessment and information security management. In addition, hybrid model was new assessment method to enhance the performance of traditional method (Lee, 2014). Hybrid model was developed by combining those two methods; qualitative and quantitative in order to implement the components utilizing available information while minimizing the metrics to be collected

and calculated, for example Analytic Hierarchy Process (AHP) and fuzzy model. There were four aim of the hybrid model which were (Meritt, 1999, Lai and Lau, 2012; Lee, 2014):

i. To identify potential risk scenarios in the business environment of an industry.

ii. To filter potential risk scenarios in business operations of a company.

iii. To rate risk scenarios in risk matrix.

iv. To develop and select proactive activities that might minimise, or even prevent any negative impact from adverse risks.

The motivation of this study is due to the fact that information security risk analysis (ISRA) was a vital method to not only to identify and prioritize information assets but also to identify and monitor the specific threats that an organization induces; especially the chances of these threats occurring and their impact on the respective businesses (Kim and Gregg, 2005; Nikolić and Dimitrijević, 2009; Tularam and Attili, 2012; Ban and Tong, 2014; Dutton, 2016; Symantec Corporation, n.d.). A new hybrid risk analysis tool named CARA (Cost and Risk Assessment) was developed based on known threats, by combining qualitative and quantitative approaches. This system was proposed to get more accurate result and had a better approach to trace the threat. Thus, this was a useful technique for easing decision-making based on numerical data to back decision. The background of study was discussed in the first part regarding the risk analysis in information technologies. The definition of risk analysis and others were discussed briefly. Other than that, the existing risk analysis tools were described to understand the characteristics of them respectively. Furthermore, research questions and research objectives had been defined based on research motivations in subsection below. The research contributions were mentioned prior to this research. The outline of the thesis was shown in the last section of this chapter.

1.1 Background of the study

Identifying potential information security risk is a challenging task. This is due to modernization and new technologies which introduce possible threats to various type of digital system (Mubarak, 2016). These threats might be the aftereffect of natural events, accidents or purposeful act to cause harm (Homeland Security, 2013; Renfroe, PSP and Smith, 2016; Ramirez and Fernández, 2016). Many studies proved that the current risk analysis tools are not able to analyse it well. There are traditional methods used previously which are qualitative and quantitative; both of these methods have their respective advantages for analysing the information. It is a must for an organization to select the appropriate methods for better analysis.

However, there are various numbers of possible threats arising due to the rapid development of information and communication technology. In addition, there are four key elements that need to be considered which are security threats, business impact, security measures and their cost (Gregg, 2005). There are many risk analysis tools that were developed every year such as Information Security Risk Analysis Method (ISRAM), CORAS, and OCTAVE. They have same purpose, which is to reduce the risk of causing a threat to the organization, but the tool attempt to hit the risk with different approach. Vulnerability of information security is extremely dangerous that could adversely affect the organization.

The main focus of this study is to develop a new risk analysis tool based on hybrid approach and compare it with the existing tool. In addition, this research is conducted to explore the importance of the assessment of the risks and explain the processes that need to be done to make the management of data security and also problems that may encounter in their organization.

1.2 Risk analysis in information technologies

Risk analysis is the process of analysing and determining the threat to individuals, businesses and organizations as well as government agencies. It occurs due to human actions and natural disasters (Rouse, 2010; New Zealand Government, 2014). Risk analysis is a vital method not only to identify and prioritize information assets but also to identify and monitor the specific threats that induces an organization; especially the chances of these occurring threats and their impact on the respective businesses.

Risk analysis tools fall into two categories which is qualitative and quantitative. Quantitative methods use a mathematical approach and statistical tools to represent risk in risk analysis (Wawrzyniak, 2006). However, risk analysis tool that uses quantitative methods are not efficient for the intensive use of information security management (Aven, 2016). Therefore, this method is rarely used in the field of business.

According to Wawrzyniak, qualitative methods risk assessed with the help of adjectives instead of mathematic (Wawrzyniak, 2006; New Zealand Government, 2014). Currently, most of developer and researcher use qualitative approach as their methodology to develop new analysis tools. It is because qualitative method is more flexible and more suitable then quantitative method. However, qualitative method does not provide complete output information to be used in the risk management process.

There are several of methods were introduced in analysing risk factors for complex data in information security. Medical research method was introduced to analyse risk factors in healthcare information system and the study was limited to static information system (Narayana, Ahmad and Ismail, 2012). Fuzzy based threat analysis tool was introduced as a mechanism to analyse information security risk on the same system. Although produced more accurate result, yet it did not consider behavioural information as parameter of analysis (Zain, Samy, Ahmad and et. al., 2010).

The hybrid model is a combination of two or more existing models. Some research is integration of two approaches (Sharmala, Ahmad and Yusoff, 2013, Lee, 2014; Agarwal, Kachroo and Regentova, 2016). By combining both of their advantages and their flexibility, it can produce more accurate results. Most of the current risk analysis tools using qualitative and quantitative method.

1.3 Research problem

There is one problem statement that is highlighted in this study. Based on the gap that had been found thru literature review, where not all current tools could evaluate both methods in one time which were qualitative and quantitative. These tools cannot evaluate different type of data in a single tool. This is because most of the tools nowadays used only one of the techniques either qualitative or quantitative. This method was not satisfactory to analyse the risks (Aven, 2016).

In addition, tremendous changes in Information Communication Technology (ICT) introduced cloud computing technologies which potentially exposed to various type of threat and vulnerabilities (Elky, 2006; Fovino, Masera and Leszczyna, 2014). For example, the oceanography industries completely depend on the use of advanced ICT integrated with additional facilities according to a specific task. Malaysia is serious in upgrading ICT system as part of main process in making sure oceanography research and development become a success. Relying too much on advanced ICT, is a potential for cyber threats and vulnerabilities to the internal system. By having propose risk analysis tools, it will produce inaccurate result in risk analysis.