VOL. 10, NO. 23, DECEMBER 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences


www.arpnjournals.com

A COMPARATIVE STUDY FOR RISK ANALYSIS TOOLS IN INFORMATION SECURITY

AY. Zabawi, R. Ahmad and SF. Abdul-Latip
Faculty of Information and Communication Technology Universiti Teknikal Malaysia Melaka Durian Tunggal, Melaka
E-Mail: yaserzabawi@gmail.com

ABSTRACT

Identifying potential information security risk is a challenging task. This is due to the evolution of Information Communication Technology in daily business which may introduce possible digital threats. Many studies have attempted to develop risk analysis tools, yet it is unable to produce the best factors for information security threats. Failure in identifying various types of information security risks will affect the development of effective countermeasure. It has been highlighted in many studies that conventional techniques used to analyze risks can be divided into two categories known as quantitative and qualitative methods. The limitation of the tools introduced in previous research which provide insufficient information may consequently contribute to threat in information security. In addition, the rapid growth of the Internet technology may also increase possible threats to information security. The main focus of this study is to compare the risk analysis tools available in the market, identify their method and summarize their factors. A comparative analysis covers performance of analysis and security services. The result shows that current information security risk analysis tools introduced various types of risk factors. None of the tools however can consider qualitative and quantitative data in parallel. It is believed that qualitative information could increase the dimension of risk factors and produce better accuracy in the analysis. Further investigation is highly required to solve the outlined issue. This paper describes different approaches in several risk analysis tools, which methods are used in different steps and presents the risk factors identified by previous selections of studies.

Keywords: information security, risk analysis, quantitative, qualitative, tools.

1. INTRODUCTION

Nowadays, better knowledge and good management are required to ensure that online business can be done securely and more effective. Information security plays an important role for various parties. It is the core of the business not only to computer experts but also to business managers who are responsible for ensuring data security (Wawrzyniak, 2006). To get more accurate output and comprehensive view of the risks that may be encountered, information about the covered entity is required as well as related information such as details information about business partners. Due to the success and continuity of organizations vastly depend on the availability and effectiveness of information technologies, protection of information is 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 plays a major role in identifying security controls to protect computer and related infrastructures. The process is used to ensure that information systems assets are protected against accidental or deliberate damage. The technical challenge in performing risk analysis described in different types of vulnerabilities exists in any control systems. This paper is organized as follow; Section II provides an explanation about risk assessment in details. Next, in Section III we describe methods used to analyze risks i.e., qualitative and quantitative. The description covers the advantages and disadvantages of both methods. The multi-factors of threats with description and explanation using table will further discussed in Section IV. In section V we introduce hybrid model and soft computing inclusive with technical description that will be developed to improve the current risk analysis tools. The final section provides a conclusion of the overall study.

2. LITERATURE REVIEW

UNDERSTANDING RISK ASSESSMENT

Presently, information security risk assessment plays a vital role in business activities (Digital Government, 2015). Risk assessment involves several steps which include risks analysis, risk mitigation and risk management. An effective risk assessment may support the organization decision maker to produce an effective security plan or mitigating the risks. Thus, identifying potential risk is extremely important.

Today many business activities using the internet as the platform to penetrate a wider market (George *et al*., 2003). However, these businesses will be exposed to a greater threat if security measures are not considered since the internet is an insecure channel. Vulnerable systems used may be exposed to any potential threads that can result in the loss to the organization assets. This proves the importance of information security in determining the success of a business.

The importance of risk assessment

The main purpose of conducting a risk assessment is to describe the current status of security which includes identifying organization assets, the security threats to the assets and the control in place to protect the assets (Bozo N. and Ljiljana R., 2009). Therefore, preparing and implementing a risk assessment can reduce the effect of undesirable incidents.

Information security management process

Information security management process consists of several steps (Wawrzyniak, 2006) as we summarize it in Figure-1 and should be carried out periodically. These steps should be based on the security policies that have been set for the organization.

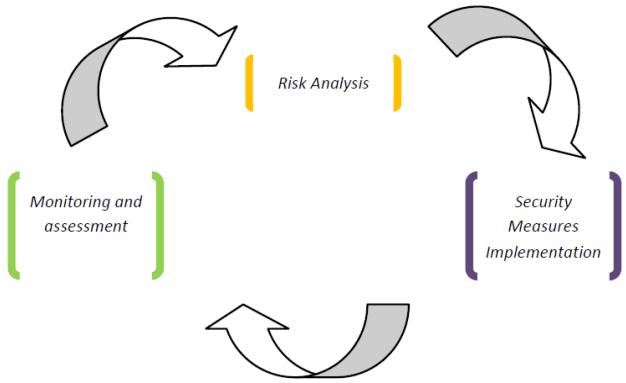

Figure-1. Security policy.

i) Risk analysis

Risk analysis is a vital method not only to identify and prioritize information assets but also to identify and monitor the specific threats against the organization; especially the likelihood of the threats to occur and their impact to the organization (Xiofang and Xin Tong, 2014).

ii) Implementation of security measures

Implementation of security measures has been discussed in (Implementing Security Measures, 2014) and has provided proposed solutions or actions to be carried out to reduce the risk and mitigate the effects. For example, ISRAM tool can be used to reduce the potential risks that may occur. In (Implementing Security Measures, 2014) also explained the common measures to secure the organization network is through the use of firewalls. However, mechanisms such as firewalls do not guarantee the confidentiality aspect of security to the organization. Therefore, to strengthen the security of the organization network, cryptographic algorithms can be used to guarantee the confidentiality aspect of security.

iii) Monitoring and assessment

The main objective of monitoring and assessment is to continuously monitor the security of organization in term of information, applications, network and system; and also to analyze risk acceptance, avoidance/reject, send/share or mitigating risk as situations change (Johnson, 2010). Besides, the purpose of monitoring is also to identify the impact of the tools whether or not it works effectively and able to analyze in light of the inevitable changes that occur.

The importance of risk analysis is to reduce threats on the organization assets, especially for organizations that conduct business activities. There are a variety of risk management tools introduced earlier by various parties such as by (Zain *et al*., 2010), (Bodin *et al*., 2005) and (Eren-Dogu and Celikogu, 2011). Generally, most of the tools introduced show the importance of protecting information (Wawrzyniak, 2006). Besides that most of the existing tools are making use of the previously developed tools as a measure to systematically identify threats that are likely to occur and can take appropriate action to significant risks that may pose threats. To produce the best risk analysis tools, several criteria must be taken into consideration to analyze the potential risks. There are a many risk analysis tools has been developed such as ISRAM, CORAS and other. Nevertheless, the purpose of these tools are not to guarantee complete protection coverage, but they are only to ensure and demonstrate the importance of the protection of information and also to suggest measures to be taken so that the threat can be minimized.

Decision making plays an important role to get accurate results and uncertainties could affect the protected data while various types of risk tool produced different inputs and outputs. Realizing this, analysis tools are important in finding the gap of information security risk factors. In addition, it will direct to discovering a new factors for risk in information security.

3. METHODOLOGY

We summarized tools used in the selection of previous studies. A static analysis was used to look at the description of tools and we also executed the demo and free software of the tool to study the performances. The analysis covers four dimensions; the tools, the method used the impact calculation and factors reported.

4. RESULT AND DISCUSSIONS

Current tools

The studies on this issue have grown since the past few years. Driven by technology advances, various risk analysis tools have been developed to prevent recurrence of similar risk or the likelihood of another imminent risk to occur due to vulnerabilities within the organization. Risk analysis tools fall into two categories which can be based on qualitative or quantitative methods. Risk analysis is the process of analyzing and determining the threat to individuals, businesses and organizations as well as government agencies which occur due to human actions and natural disasters (Rouse. 2010). Risk analysis is a vital method not only to identify and prioritize information assets but also to identify and monitor the specific threats against the organization; especially the likelihood of these threats to occur and their impact on the respective businesses.

Quantitative methods use a mathematical approach and statistical tools to represent risk in risk analysis (Wawrzyniak, 2006). However, risk analysis tool which based on quantitative methods are not efficient for the intensive use of information security management (Armaghan B., Rafhana AR. and Junaid A., 2012).

Therefore, this method is rarely used in the field of business.

According to (Wawrzyniak, 2006), in qualitative methods, risks assessment is performed with the help of adjectives instead of mathematical models. Currently, most of developer and researcher use qualitative approach as their methodology to develop new analysis tools. This 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 (Armaghan B., Rafhana AR. and Junaid A., 2012). The advantages and disadvantages of risk analysis assessment for both quantitative and qualitative methods are shown in Table-1 and Table 2 respectively.

Table-1. Quantitative methods.

Risk Analysis	Quantitative Methods
Advantages	- It gives more accurate image of risk. - It allows for determination of consequences of incidents occurrence in quantitative way, what facilitates realization of costs and benefits analysis during selection of protections. - It applies mathematical and statistical tools to represent risk.
Disadvantages	- Not suitable for intensive analysis nowadays. - In complicated environment it is more difficult to use mathematical models. - Quantitative measures depend on the scope and accuracy of defines measure scales. - Results of analysis may be precise and even confusing. - Analysis conducted with the applications of this method is generally more expensive, demanding greater experience and advanced tools.
Type of tools	- ISRAM, CORA, IS, RISKWATCH and etc.

Table-2. Qualitative methods.

Risk analysis	Qualitative methods
Advantages	- Analysis is relatively easy and cheap. - It allows to prioritize the risks. - It allows for determination of areas of greater risk in a short time without bigger expenditures. - Perform risk analysis with the help of adjectives, not mathematical models. - It is more suitable for complicated risk analysis nowadays.
Disadvantages	- Unstable results - It depends on the ideas of those who undertake risk analysis. - It does not allow to determine the probability and results using numerical measures. - Cost-benefits analysis is more difficult during the selection of protections.
Type of tools	- OCTAVE, OCTAVE-S, CORAS, CRAMM, FRAP and etc.

There are several methods have been introduced in analyzing risk factors for complex data in information security. A method for medical research was introduced by (Narayana, Ahmad and Ismail, 2012) to analyze risk factors in healthcare information system. However the method was limited to static information system(unchangeable). Fuzzy- based threat analysis tool was introduced by (Zain *et al.*, 2010) as a mechanism to analyze information security risk on the same system. Although (Zain *et al.*, 2010) produced more accurate result, yet it did not consider behavioral information as parameter of analysis.

Risk analysis tools such as security policy decision making and security risk assessment, use analytic hierarchy process (AHP) as the evaluation technique. AHP technique also being used to analyze risk, based on business model (Suh and Han, 2003). For example, AHP is also used in evaluating information security investment as discussed in (Bodin *et al.*, 2005).

As a conclusion, each of qualitative and quantitative methods have their own pros and cons, yet by combining those two methods; qualitative and quantitative methods, the results of risk analysis assessment could be more accurate compared by using only one of those methods. This method, called hybrid model can be a new approach with a presence some new parameters that can be implemented and can be used in future in security field. A hybrid model which combines two or more existing models has been demonstrated by (Zhang *et al.* 2010). (Zhang et al., 2010) claimed that AHP offers a technical support for risk analysis by using the judgments of managers and systematically calculating the relative risk value (weight). However, (Eren-Dogu and Celikoglu,

2011) proved that Bayesian prioritization procedure provides a more effective way of risk assessment compared with the conventional approaches used in AHP (Eren-Dogu and Celikoglu, 2011).

Nevertheless, to produce an effective risk analysis tool, soft computing must be combined with the hybrid model. By combining both of their advantages and flexibility, it can produce more accurate results. Most of the current risk analysis tools using qualitative or quantitative method. However the question is, how to produce a tool that can analyze data by combining both qualitative and quantitative methods. To produce a better model, a combination of AHP and Fuzzy logic may be required in order to obtain the advantages of both approaches. For example, to analyze the risks associated with certain adjectives, AHP can interpret the risks into quantitative measurement, while fuzzy logic can determine the level of threat to the organization.

Multi-factor risks

The landscape of information security threat is constantly evolving. (Durbin, 2014) in the Information security forum identifies top six security threats for 2014 and highlighted the following statement:

"As we move into 2014, attacks will continue to become more innovative and sophisticated. Unfortunately, while organizations are developing new security mechanisms, cybercriminals are cultivating new techniques to circumvent them," (Durbin, 2014).

Based on empirical data by (Narayana *et al*, 2012) as shown in Table 4 and Table 5, some potential threats have been identified and the possible factors of these threats occur. All of these threats will be divided into two categories according to the risk assessment methodology which is qualitative or quantitative. Then, all of these threats will be reviewed and listed impacts resulting from threats successfully exploiting vulnerabilities. The impacts listed will calculate the level of threats by using a scale of "low", "medium", and "high". The definitions of impact ratings are described in Table-3 "Rebecca M. and Patrick D. NISTP, 2012".

Table-3. Definition of impact ratings

Magnitude of impact	Impact Definition
High	Misuse of the weakness may bring about the high unreasonable loss of major substantial resources or assets; may disrupt, abuse, or interfere an association's goals, notoriety, or passion fundamentally; or may bring about human passing or genuine harm (HIPAA Security rules, 2011).
Medium	Abuse of the weakness may bring about the immoderate loss of substantial resources or assets; may disrupt, abuse or interfere an organisation's goals, notoriety or interest or may result in human injury (HIPAA Security rules, 2011).
Low	Misuse of the weakness may bring about the loss of some substantial resources or assets or may influence an association's central goal, notoriety, or interest noticeably (HIPAA Security rules, 2011).

In Table-4 and Table-5 we show threat assessment based on the data collected.

Table-4. Multi-factors risk analysis.

Risk Factors	Quali/ Quanti	Impact	Low	Medium	High
Large data inserted	Quanti	-reduce system performance -system may crash		√	
Power Failure	Quali	-Server down due to power failure. -loss of data -cannot proceed with work		√	
Asset damages	Quanti	-loss of data -losses		√	
Terrorism	Quali	-information leakage	√		
Bug	Quali	-loss of data -information leakage	√		
Hardware Failure/errors	Quali	-loss of data -work disruption		√	

Table-5. Multi-factors risk analysis (Narayana *et al*., 2012).

Risk Factors	Quali/ Quanti	Impact	Low	Medium	High
Authority Sharing	Quanti	-information leakage -data not secured	√		
Law	Quali	-losses	√		
Software Security	Quali	-loss of data -information leakage -virus and malware attack			√
Database technology implementation	Quali	-DML issues - heterogeneous connectivity		√	
Acts of human error	Quali	- unauthorized exploitation of intellectual property (plagiarism)			√
Operational issues	Quali	-data not systematically managed -inadequate knowledge		√	
Malware attacks	Quali	-loss of data -information leakage -plagiarism		√	
Communication infiltrations	Quali	-attack from hackers -loss of data		√	
Social engineering attacks	Quali	-outsiders gaining access to confidential information through social interaction	√		
Misuse of system resources	Quali	-information leakage -data not secured	√		
Technical failure	Quali	-loss of data -cannot proceed with work		√	
Technological obsolescence	Quanti	-working less satisfactory		√	
Software failure/errors	Quali	-loss of data -work disruption		√	
Staff shortage	Quanti	-poor with management		√	
Natural disaster	Quali	-loss of money -loss of data			√

The results of studies conducted from data threats that may occur as in Table 4 and Table 5, we can see various types of threats and categorized into qualitative and quantitative. There are many tools that have been developed to analyze the risk but it is focused on only one methodology. For example, ISRAM and CORA are only able to analyze the risk which can be calculated by using quantitative methods. But, risk analysis tools like OCTAVE and CRAM developed for the analysis risk based on qualitative method. In order to produce a tool that is able to analyze a quantitative and qualitative analysis in one tool, the research is being conducted with the aim of being able to produce a hybrid-based tool.

Hybrid model and soft computing

As a result of modernization, numerous research have been performed to produce more effective tools for analyzing risks to minimize the impact of the threats (H. G. Brauch *et al*., 2011). Therefore, combining risk assessment tools has been suggested as the best technique (Chi-Chun L. and Wan-Jia C. (2012)), (CESG, (2015)) and (Lin-Jun K. (2013)) to analyze threats for both qualitative and quantitative methods. Till now, the conventional method is not sufficient to analyze risks or threats. Hence, a more advanced method such as soft computing should be used to analyze the possible risks. Components of soft computing include;

- Fuzzy Logic (FL)
- Neural Networks (NN)
- Genetic algorithms (GA)
- Rough Sets (RS)
- Bayesian Network (BN)

By integrating two or more existing model through hybrid models, we may obtain both the advantages and flexibility for better result. In (Lee, 2014) has introduced some approaches that can be used to produce hybrid model as shown below;

- Rough - Bayesian network
- Rough Sets – Neural Network
- Fuzzy-Rough Sets
- Fuzzy- AHP

Most of today's assessment methods are based on hybrid models (Lee, 2014). The objective of our study is to study how qualitative and quantitative data can be measured in a single tool. Therefore, a combination of two techniques is necessary to produce a new tool.

5. CONCLUSIONS

There are various methods of risk assessment have been developed and among them there is a more advanced method. Studies have shown that the results of the risk assessment using existing risk analysis tools provide a good result as it can help to balance between losses and costs of implemented protections. They also help in planning expenditures, indicate legitimacy or lack of fundamentals to additional investment in Information Systems Security. However, the impact of modernization produces various types of threats that cannot be evaluated using only quantitative or qualitative methods alone. There

are some studies to produce a risk analysis tool that is more effective which combine both qualitative and quantitative methods. These hybrid techniques have been proven to be the best solution to obtain more accurate results. The combination of the two methods can help to improve the accuracy of the analysis such as, by combining fuzzy and AHP techniques. The limitation of this research is the system may not evaluate all threats as it will consider the most significant threats only. For the future works; we will develop a web based system, where user can calculate the estimation cost if any threats occur. In addition, the system can give insight in reducing the cost. Apart from that, it also can make evaluation of risks.

ACKNOWLEDGEMENT

The authors would like to thank Universiti Teknikal Malaysia Melaka (UTeM) and Ministry of Higher Education for FRGS fund, FRGS/2/2013/ICT07/FTMK/02/3/F00186 (FRGS - FTMK, Malaysia for supporting this research. Not to forget the two most important people in my life, Father and Mother who have given me support, patience. I owe you both gratitude. Again thank you for being there when I needed you most.

REFERENCES

[1] Wawrzyniak, D. (2006) "Information Security Risk Assessment Model for Risk Management" pp. 21-30(2006).

[2] Rouse, M. (2010), Risk Analysis. URL: http://searchmidmarket security.techtarget.com/definition/risk-analysis (October 2010).

[3] Johnson, L.A. 2010. "Information Security Continuous Monitoring" URL: http://csrc.nist.gov/groups/SMA/forum/documents/Forum-121410-Continuous-Monitoring-AJohnson.pdf. (December 2010).

[4] Narayana, S., Ahmad. R., Ismail, Z. 2012. Adopting Medical Research Approach in Analyzing Information Security Risk. In Tech Publication.

[5] Zain, N.M., Samy, G.N., Ahmad, R., Ismail, Z., Manaf, A.A. 2010. Fuzzy based threat analysis in total hospital information. Advances in Computer Science and Information Technology, 1-14 system.

[6] Suh, B., Han, I. 2003. "The IS risk analysis based on business model". Information and Management, Vol. 41, No. 2, pp. 149-158.

[7] Bodin, L.D., Gordon L.A., Loeb, M.P. 2005. "Evaluation information security investments using analytic hierarchy process". Communications of the ACM, Vol. 48, No. 2, pp. 78-83.

[8] Bozo N. and Ljiljana R. 2009. "Risk Assessment of Information Technology Systems" Issues in informing Science and information Technology Volume 6. 2009

[9] George S., James X., Alan G., Barbara J., Alan S. 2003. IT Security "Information Technology Security Handbook" URL: https://www. infodev.org/infodev-files/resource/InfodevDocu ments_18.pdf

[10] Zhang, X., Huang, Z., Wei, G., Zhang X. 2010. "Information security risk assessment methodology research: Group decision making and analytic hierarchy process". In the Proceeding of IEEE the 2nd World Congress on Software Engineering, pp.157-60.

[11] Eren-Dogu Z.F., Celikoglu C.C. 2011. Information security risk assessment: Bayesian prioritization for AHP group decision making". International Journal Innovation Computer Information Control, Vol. 8, No.11, pp. 8019-32.

[12] Lee, M.C. 2014. "Information security risk analysis methods and research trends: AHP fuzzy comprehensive method." International Journal of Computer Science and nformation Technology (IJCSIT) Vol. 6, No1, February 2014.

[13] Kioskea. 2014. Implementing Security Measures" URL: http://en.kioskea.net/contents/639-implementing-security-measures (June 2014).

[14] Steve Durbin. 2013. Information security forum identifies top six security threats for 2014", (December 18, 2013).

[15] Xia B. And Xin T. 2014. "A Scenario-Based Information Security Risk Evaluation Method". International Journal of Security and Its Applications Vol. 8. No. 5, pp. 21-30.

[16] Digital Government. 2015. Building a 21st Century Platform to Better Serve the American People", URL: https://www.whitehouse.gov/ sites/default/files/omb/egov/digital-government /digital-government.html

[17] Armaghan B., Rafhana A. R. and Junaid A. C. 2012. "A survey of Information Security Risk Analysis Method". Smart Computing Review, vol. 2, no. 1, February 2012.

[18] Rebecca M. and Patrick D. 2012. National Institute Standards and Technology "Risk For Conducting Risk Assessments" NIST Special Publication 800-30 Revision 1.

[19] US Department of Health and Human Services. 2011. "The security Rule". URL: http:// www.hhs.gov/ocr/privacy/hipaa/administrative/securit

yrule/index.html

[20] H. G. Brauch *et al*. 2011. "Concepts of Security Threats, Challenges, Vulnerabilities and Risks"

[21] Chi-Chun L. and Wan-Jia C. 2012. "a hybrid information security risk assessment procedure considering interdependences between controls". An International Journal v. 39 pages 247-257.

[22] CESG. 2015. "A description of different risk management frameworks to help inform organizations who are considering selecting one." Information Risk Management Guidance.

[23] Lin-Jun K. 2013. "An Improved Information-Security Risk Assessment Algorithm for a Hybrid Model." International Journal of Advancements in Computing Technology (IJACT) V.5, Number 2.