A Dynamic Analysis on Information Security Risk Factors and Risk Analysis Tools

Ahmed Yaser Mohd Zabawi[1], Rabiah Ahmad[1], Siti Zarifah Sarif[2], Siti Rahayu Selamat[2]
Information Security and Network Research Group,
Fakulti Teknologi Maklumat dan Komunikasi
UniversitiTeknikal Malaysia Melaka
76100 Durian Tunggal, Melaka.
yaserzabawi@gmail.com, Rabiah@utem.edu.my

***Abstract*- Identifying potentially risks in information system such a challenging task. The impact of rapid technological development, information security risk analysis is an important action and components required for an organization operation, especially for organizations that involve business. Many studies shows that recent business trend expose to modern digital threats and attack due to the tremendous changes in ICT. The emergence of new threats and attack indicator for new factors that influence new risk. The current risk analysis tools are not able to analyze it well. There are traditional method used previously which is qualitative and quantitative; both of this methods have their respective advantages for analyzing the information. It is recommended by many studies that recent organization must choose the effective risk analysis tool in order to get the best factors that contributes to information security threats. In addition, it is valuable to have a taxonomy of risk factors that potentially a threat to information system. This study explore various type of risk analysis tools by looking at its capability in identify threats to Confidentiality, Integrity and Availability. The method was designed by first exploring the current market risk analysis tools and extracted its functionality in identifying risk to CIA. The analysis in this study shows that the present risk analysis tools able to introduce a schematic diagram of potential risk factors to information security. In addition it gives a list of recent tools with technical description that provide better guideline in performing risk analysis.**

I. INTRODUCTION

It has been widely accepted that the structure and type of information technologies have changed enormously over the last decade. The simple stand-alone batch applications evolved into distributed computing environments, including real time control, multitasking and distributed processing. As the world seen that tremendous changes in ICT introduced cloud computing technologies which potentially exposed to various type of threats and vulnerabilities. Many industries completely depend on the use of advanced ICT integrated with additional facilities according to a specific task. The application for critical sectors such as meteorology activities, defense and security require high demand of advanced and futuristic of information technology. Relying too much on the advancement ICT increase chances to be expose for cyber-attacks, crime and vulnerabilities. Building a secure system is a must towards protecting information assets within the advanced system. Identifying potential risk factors is an initial step in producing effective and secure solution. This research is developed to explore potential method and its capability in identifying information security risk and extract various information security risk factors discovered by previous related research. This article is structured as follow, Section II describe information searching method, Section III list risk analysis tools inclusive with technical description. Section IV provide risk factors that reported significantly associated with Confidentiality, Integrity and Availability. The final section (Section V) reports the risk factors covered by existing risk analysis tool and Section VI conclude overall study.

II INFORMATION SEARCHING AND ANALYSIS

There are many ways to manufacture, mining and produce and extract information on further details, with the help of the internet, finding information become much easier. Information can be obtained from different sources. For this research`, there are many search engines that have been used. Among the most commonly used are Google, Google Scholar and also Scopus Database. Resources from the UTeM library also proved to be very useful.

Risk analysis is one of the risk management process for an organization. To obtain accurate data, detail research is necessary in order to identify potential risks exist and losses that may occur in organization[1]. According to [13]. the discussion of risk analysis should be done by large groups (6-10 people) and from various departments. Each member must be proficient on the organization and activities performed by the organization such as the manager. Since there is a high potential risk to appear, the discussion should be done always by group member and they should make regular intervals to make the discussion.

Tom Walsh (2003) [1] addressed that managing risk is an important step in dealing with any business. It is impossible to reduce all threats occur in the running system. Performing a risk analysis process allow us to identify best method in managing threats. Risk Factors Analysis (RFA) is

the study of factors which can or may pose a risk to the organization.

Each factor is assessed based on the level of losses that may be incurred and the organization based on its ability to threaten an organization in term of information security policies which is Confidentiality, Availability and Integrity.

III. RISK ANALYSIS

Information Risk and Security continue to be a top of mind for many organizations. Constant attack by certain parties like hackers shows their ability to hack into an organization ease. In addition, it also proves the security vulnerabilities of information used by an organization. Through the losses incurred, most organizations have realized to plan more wisely and effectively to safeguard and protect the organization and personal information.

Firstly, process of data protection and risk management requires a risk analysis process and to perform risk management, it requires accurate data of risk analysis or in other words, it requires accurate assessment of risk management. Therefore, this can prove that risk analysis playing an important role in protecting information. If the organization did not take seriously with risks that got potential pose a threat, it may have a big impact on the organization and is likely to be able to make the organization into bankruptcy. For example, due to vulnerability of data security, there are various parties take that opportunity to hack into the internal information of an organization.

Armaghan[2] said in his article 2012, To analyze the risk with more efficient and effective in this age, there are a lot of automated tools can be used. The main purpose of risk analysis is to provide detailed information to potential threats to decision makers in an organization. Therefore, it is important as decision-makers to select the best of risk analysis tool that suitable to an organization.

There are various types of risk analysis tools that have been developed. In addition, all the tools have their own strengths and weaknesses based on different situation. Among the well-known risk analysis tools currently is ISRAM, CRAMM, OCTAVE and others. However, all of those risk analysis tools are divided into two different major groups according to the methodology used either qualitative or quantitative.

The main purpose of the organization need to take seriously the issue of information security is to maintain the confidentiality, availability, integrity, accountability, authenticity and reliability.

This article will describe some of the methodology and tools that commonly used at this time to analyze risk. The purpose of this study is to explain detail that organization needs to know with easily. It is because the organization will spend a lot of money for any method they choose. This study will help them to understand the methods that are often used at present. The best way to make a comparison between tools that has been developed by looking at their objectives whether the method chosen by them able to meet their organization's objectives.

a. Risk Analysis methods.

Nowadays, there are many people studies on this issue and they have also developed various risk analysis tools to prevent recurrence of similar risk or probability of another imminent risk due to weaknesses in the organization. Risk analysis tools fall into two categories which is qualitative and quantitative.

Risk Analysis	**Quantitative Methods**
Advantages	- It gives more accurate image of risk. - It allow 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 of nowadays. - Complicated environment make it look more difficult by using 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 1.0 Quantitative methods

Quantitative methods use a mathematical approach and statistical tools to represent risk in risk analysis [3]. As an example, "there are a lot of viruses attacking manager's computer". In this situation, we can see a lot of virus attacking computer, so the quantitative methodology will give results; it is risky to be a threat if many viruses attack computers. However, Dariusz [3] has Identified risk analysis tool that uses quantitative methods are not efficient for the intensive use of information security management. Therefore, this method is rarely used in the field of business. Risk analysis tool that uses quantitative methods are ISRAM, CORA, IS, RISKWATCH and etc.

Risk Analysis	**Qualitative Methods**
	- Analysis is relatively easy and cheap. - It allows for putting in order risks according priority.

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

Table 2.0 Qualitative methods

Qualitative methods risk assessed with the help of adjectives instead of mathematic. Currently, most of developer 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. Risk analysis tool that uses quantitative methods are OCTAVE, OCTAVE-S, CORAS, CRAMM, FRAP and etc.

Most of the risk analysis tools regardless qualitative or quantitative implementing information security attributes which are confidentiality, availability and integrity. However, some studies should be conducted to prove the risk analysis tools have characteristics such as confidentiality, availability, integrity, reliability and others. This is necessary as to help users to select the best risk analysis tools to be used to solve different problems faced by individuals and organizations.

IV. Confidentiality, Integrity and Availability

Stan Gibilisco (2013) [4] said in her studies, confidentiality, integrity and availability are the attributes that should be included in all risk analysis tools to guide policy to protect the security of information in an organization. Confidentiality of information in the context of risk analysis tools, are the procedures to limit access to information, while integrity is the assurance that the information received is accurate and reliable. Lastly, the availability is guaranteed access to information by authorized persons.

Confidentiality prevents confidential or sensitive information from reaching the wrong person as well as to give access to people who are qualified to use the data. As an obvious example, the account number is information that should be kept confidential during online banking. Common method used is the data encryption to ensure that information is kept confidential. In addition, other procedures are users need to enter your user ID and password. Users can also take precautions to reduce the number of places where the information appears, and how many times it was actually sent to complete the transaction required [4].

Integrity in this context is to ensure that the data is accurate, reliable and consistent over its entire life cycle. Stan Gibilisco (2013) [4] also said data cannot be changed arbitrarily and steps should be taken to ensure that parties who can access and modify data. In addition, the measures were precautionary measures should be taken to identify if data is changed as a result of non-human-Caused such as server crashes. If unintended changes happen to the data they need to make sure to have backup data to restore the affected data to its correct state.

Availability is the best attribute to ensure that:

- All the hardware is in good condition.
- Perform hardware repairs if needed.
- Provide specific measures to prevent any damage
- Ensure sufficient communication bandwidth.
- Provide emergency backup power systems.
- Keeping current with all necessary system upgrades.
- Guarding again malicious actions.

IV Risk Factors

		IS Attributes		
		Confidentiality	**Integrity**	**Availability**
Risk Factors	**Asset damages**			-Willful damages by outsiders or insiders
	Environmental support failure/natural disasters		-Natural disaster	-Fire at server. -Water damaged at the server.
	Terrorism	-Terrorist attacks -Information leakage		
	Law		-imposition of legal and regulatory obligation. - Insufficient enforcements of law	
	Owners responsibility		- Lack of information assets - Unreliable level of information assets Protection. - Lack of physical access control and Protection - Lack of Business Continuity Management - Lack of Disaster Recovery Planning	-Using old hardware. Example: processor version.

	IS Attributes		
	Confidentiality	**Integrity**	**Availability**

Risk Factors	**Time**		-Timing of occurrence (Critical or not) -Timing to detect the threat -Timing to react to solve that threat.	
	Authority Sharing			-1 server machine can have multiple server.
	Bug		-software have bug due to not fully test. -New software	
	Password encryption method	-some of software doesn't use latest encryption. Such as 128-bit Secure Sockets Layer (SSL) protocol.		
	Data redundancy		-database design not normalizes perfectly. -Bad architecture design.	
	Security		-software lack of security protection. Example software must provide 1 time password (confirmation by phone). -lack of security and monitoring systems. -software doesn't meet international security standard. Such as VerySign, WebTrust	
	Database technology implementation	-heterogeneous connectivity (involving multiple database server) *DML(data manipulation language) issues		
	Power failure/loss		-Interruption by service provider.	-Server down due to power failure. -Air-conditioning failure of the server.

Risk Factors	**Acts of human error/failure**	-Entry of wrong data by staff. -Accidental deletion or modification of data by staff. - Unauthorized access to, or modification or Disclosure of information assets. - Unauthorized exploitation of intellectual Property (plagiarism)	-Confidential Information being sent to the wrong recipient. -Storage of data/classified information in unprotected areas by staff. - Unethical competitors - Person who misuse/ misconfigure system security function, or ignore security policies And good practices. - Disclosure of information to institution Competitors - Poor information security studies -session log out time (software)	
	User		-Ignorance, carelessness, negligence or idle curiosity by user	
	Technological obsolescence		-Outdated application software. -Outdated system software.	-Outdated Hardware. -Obsolete network equipment.
	Hardware failures or errors		- Insufficient backup	-Insufficient storage space -Software Maintenance error
	Software failures or errors		-Application software failure. -Software maintenance error. - Complexity in Information Technology and System design - System Design Flaws and Weaknesses	
	Network infrastructure failures or errors		-Connection failure. -Unsecured wireless network. -network software failure. -network congestion	-Switch port problems. -Routers or switches hang.

	IS Attributes		
	Confidentiality	**Integrity**	**Availability**

IS Attributes

		Confidentiality	Integrity	Availability
Risk Factors	**Deviations in quality of service**	-Minimum technology of transfer (TOT) from contractors and technology vendors.		
	Operational Issues		-Lack of training for staff. -System documentation not systematically managed. -inadequate knowledge/skill by staff. - Lack of operation maintenance.	
	Malware Attacks		-Embedding of malicious code due to the usage of wireless and mobile technologies. Introduction of damaging or disruptive software.	
	Communications interception	- spoofing/impersonation due to unsecured network		
	Masquerading		-insiders -outsiders -service providers	
	Unauthorized use information application	-outsiders -insiders		
	Communication infiltrations	-Hackers due to unsecured network.	- Lack of Anti-Virus / Spyware protection	
	Social engineering attacks	-Gaining access to confidential information through social interaction by outsiders.		
	Technical Failure			-Technical failure of the host or storage facility.
	Deliberate acts of theft (including theft of equipment or data)	-Deliberate acts of theft by outsiders. -Deliberate acts of theft by insiders.		
	Misuse of system resources	-Misuse of confidential information by staff.	-Misuse internet access by staff.	

Table 3.4 Risk Factors

V. Comparison of Risk Analysis Tools

Type of tools	**Qualitative tools**				
Characteristics	OCTAVE	OCTAVE-S	CORAS	CRAMM	FRAP
Confidentiality	**X**	**X**	**X**	**X**	**X**
Availability	**X**	**X**	**X**	**X**	**X**
Integrity	**X**	**X**	**X**	**X**	**X**
Accountability			**X**		
Authencity	**X**	**X**	**X**		
Reliability	**X**	**X**	**X**		
Flexibility	**X**	**X**			**X**
Self-Directed	**X**	**X**			
Evolved	**X**	**X**			

Table 4.1 Comparison of Qualitative tools and Quantitative tools

Type of tools	**Qualitative tools**				
Characteristics	OCTAVE	OCTAVE-S	CORAS	CRAMM	FRAP
Vendor name	Carnegie Mellon University SEI	Carnegie Mellon University SEI	European commission	Insight Consulting	Tom Peltier Auerbach publications
Languages	English	English	English	English, Dutch and Czech	English
Price	Free	Free	Free	Free	Free
Tools supporting Materials	-Training -Licensed material	-Used for medium/small business	-XML -UML	-CRAMM expert -CRAMM express	Standard

Table 4.2 Comparison of Qualitative tools and Quantitative tools

Type of tools	**Quantitative tools**

Characteristics	ISRAM	CORA	IS	RISKWATCH
Confidentiality	**X**	**X**	**X**	**X**
Availability	**X**	**X**	**X**	**X**
Integrity	**X**	**X**	**X**	**X**
Accountability				**X**
Authencity		**X**		
Reliability				
Flexibility				
Self-Directed				
Evolved				
Vendor name	National Research Institute of electronics and Cryptology and the Gebze Institue of Technology	Internatio nal security and technolog y Inc	Korea Advanced Institute of science and Technology	RIskwatch
Languages	English	English	English	English, Dutch and Czech
Price	Free	$7000-85000$	Free	15 000$
Tools supporting Materials	- Key risk mgt tools for information	N/A	N/A	- online and telephone Support, Help, FAQ

Table 4.3 Comparison of Qualitative tools and Quantitative tools

VI. CONCLUSION

In this modern age, there are a variety of methodologies exist to prevent the risk that may faced by an organization. With this research, it is hoped that it could explain some of the methodologies that have been developed with ease. We aimed to develop a comfortable and reliable framework that organizations can apply to compare different information security risk analysis methodologies. The framework was developed with the aim of analyzing methodologies in detail and recognizing some common criteria. The normal criteria have then been used to form the characteristics of the framework.

ACKNOWLEDGEMENT

The authors would like to thank Universiti Teknikal Malaysia Melaka (UTeM) and Ministry of Higher Education for FRGS fund (FRGS - FTMK, Malaysia for supporting this research.

REFERENCES

[1] Tom Walsh "Security Risk Analysis And Management: An Overview" URL:http://library.ahima.org /xpedio/groups/public/documents/ahima/bok1_048622.hcsp?dDocName=bok1_048622 (January 2011).

[2] Armaghan Behnia (2012) "A Survey Of Information Security Risk Analysis Methods" URL : http://dx.doi.org/10.6029/smartcr.2012.01.007 (February 2012).

[3] Darius Wawrzyniak "Information Security Risk Assessment Model For Risk Management" pp. 21-30(2006).

[4] Stan Gibilisco "Confidentialitu, Integrity and Availability (CIA)" URL: http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA (May 2013).

[5] Nurzaini M. Z. (2009), "Fuzzy Based Threat Analysis In Total Hospital Information System" pp.85 – 90.

[6] Zeki Yazar(GSEC, Version 1.3) (2002). A Qualitative Risk Analysis and Management Tool- CRAMM.

[7] Hinton, C. "CRAMM." December 2001. URL: http://www.scmagazine.com/scmagazine/sc-online/2001/review/059/product.html (22 March 2002).

[8] SANS Institute. "Facilitated Risk Analysis And Management Tool-FRAP" 2002. URL: http://www.sans.org/reading-room/whitepapers/auditing /qualitative-risk-analysis-management-tool-cramm-83 (2002).

[9] Thomas R. Peltier "Facilitated Risk Analysis Process" August 2000. URL: http://www.ittoday.info/AIMS/DSM/85-01-21.pdf (06 August 2002).

[10] Hadley J. "Risk Analysis Using FRAP : Is it Silo Thinking?" URL: http://decision-analytics-blog.lumina.com/risk-assessment/is-facilitated-risk-analysis-process-frap-just-silo-thinking/html (18 July 2013).

[11] Hank Marquis " 10 Steps to do it yourself CRAMM" URL: http://itsmsolutions.com/wp-content/uploads/2013/01/DITYvol4iss50.pdf (12 July 2008)

[12] "A Practitioner's View of CRAMM." September 1997. URL: http://www.gammassl.co.uk/topics/hot5.html (22 March 2002).

[13] Gary Stoneburner, Alice Goguen, Alexis Fringa(2002) "Risk Management guide for information technology Systems" URL: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf (July 2002)