Risk Assessment Method for Insider Threats in Cyber Security: A Review

Nurul Akmal Hashim[1], Zaheera Zainal Abidin[2], Nurul Azma Zakaria[4], Rabiah Ahmad[5]
Information Security, Forensic and Networking Research Group (INSFORNET),
Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Melaka Malaysia

A.P. Puvanasvaran[3]
Faculty of Manufacturing Engineering
Universiti Teknikal Malaysia Melaka, Melaka Malaysia

***Abstract*—Today's in manufacturing major challenge is to manage large scale of cybersecurity system, which is potentially exposed to a multitude of threats. The utmost risky threats are insider threats. An insider threat arises when a person authorized to perform certain movements in an organization decides to mishandle the trust and harm the organization. Therefore, to overcome these risks, this study evaluates various risk assessment method to assess the impact of insider threats and analyses the current gaps in risk assessment method. Based on the literature search done manually, we compare four methods which are NIST, FRAP, OCTAVE, and CRAMM. The result of the study shows that the most used by an organization is the NIST method. It is because NIST is a method that combines the involvement between human and system in term of collection data. The significance of this study contributes to developing a new method in analyzing the threats that can be used in any organization.**

***Keywords*—Insider threats; manufacturing; risk assessment; cyber security; threats; risk**

I. INTRODUCTION

The industrial revolution (IR) 4.0 for the manufacturing area is mostly based on advances in the areas of autonomous robots, big data, augmented reality, cloud computing, internet of thing and cybersecurity [1]. Malaysian as a dependent nation needs to increase the value chain to become a high-quality manufacturing base using technology to make the country more competitive at regional and global levels. Besides that, IR 4.0 encourages companies to use computerization and data exchange in manufacturing technologies that create smart robot where machines are linked to the internet and to a system that can depict the whole production chain[2].

However, nowadays it shows that cybercrimes cases are reported and increased over than 40%. Organizational security professionals are worried about workers with low-security awareness may provide required information accidentally under the trickery hackers [3]. The insider threat is considered as a part of social engineering, which we also call as unintentional insider threat (UIT). It is worth noting that insider threat about intentional leakage has begun to raise the courtesy of researchers recently [3], [4].

The term insider threat refers to threats originating from people who have been given access rights to an IS and misuse their privileges, thus violating the IS security policy of the organization. Criminology research has extensively studied this kind of behavior, even though it does not always lead to committing a crime. In the same way, attacks can be non-malicious while performing the tasks in an organization like carelessness, lack of knowledge, or intentional circumvention of security. Internal Intrusion Detection System (IDS) protect organizations against insider attacks.

Therefore, to reduce and analyze insider threats is by using risk assessment. Risk assessment is the procedure that evaluates the information system and the security characteristics of information like confidentiality, integrity, and availability [5]. The evaluation is based on related information security technology and management criteria. Through risk assessment, we can understand the security situation and take targeted security measures which control the risk within an acceptable range. The basic risk assessment model is shown in Fig.1.

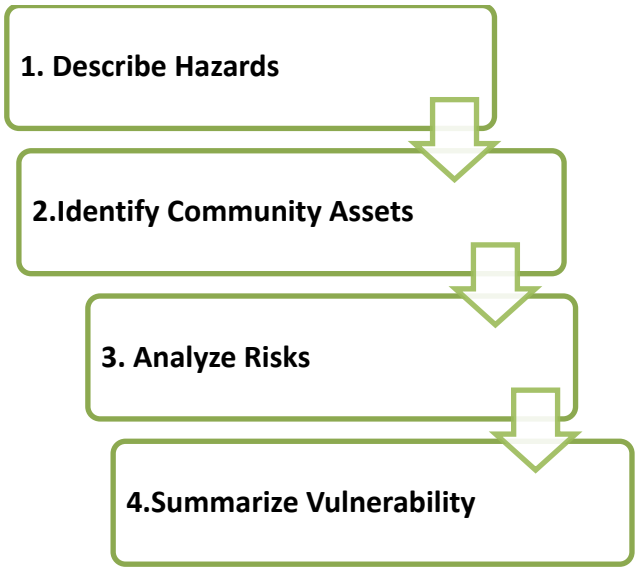

Fig. 1. Risk Assessment Basic Model [6]

Risk assessment considers four factors: hazards, assets, threats, and vulnerabilities. This research focuses on assets, analyzing assets, the relationship between threats and vulnerabilities, and the value of the risk of computing systems[7]. Many security techniques and mechanism have been developed to counter the insider threats such as National Institute of Standards & Technology Special Publication 800-30 (NIST SP 800-30), The Operationally Critical, Threat, Asset and Vulnerability Evaluation (OCTAVE) process, The Facilitated Risk Assessment Process (FRAP), and The Central Risk Analysis and Management Method (CRAMM).

Currently, risk assessment has been applied to almost every aspect of the industry. A risk is defined as the impact on the uncertain target; the impact can be positive or negative [8]. According to Hubbard, risk management includes risk identification, assessment and prioritization, and subsequent reduction, monitoring, and control of negative events [8]. With the joint efforts of scholars and experts, there are several popular risk assessment models that can meet different needs.

Rest of the paper consists of following sections: Section 2 presents the related work that unveils the methods of the risk assessment. Result and Discussion are covered in section 3. Finally, section 4 concludes the paper and discusses future work.

II. Related Works: Review of the Risk Assessment Methods

The studied-on risk assessment method in cybersecurity have been used to identify insider threats will be discussed. Furthermore, an analysis of the related works of the risk assessment method to ease the security condition task is offered.

A. National Institute of Standards & Technology (NIST)

The method described in NIST SP800-30 is a combination of quantitative and qualitative. The NIST 800-30 is primarily a model rather than a specialized method [9], [10]. It still contains a complete guide to defining all aspects of an effective risk management plan. It also contains the criteria and processes needed to assess and mitigate risk. It is suitable for better large organizations such as government agencies and large corporations. NIST SP800 supports organizations, CIOs (CIOs), security officers, IT consultants, and anyone who is generally involved with risk management in the organization [11].

The first step in NIST is to identify assets. System characteristics describe the boundaries of the system and the resources and information that make up the system. The characterization system defines the scope of the risk assessment effort, describes the operational authorization (or certification) boundaries, and provides the information necessary to define the risk (eg, hardware, software, system connectivity, and responsible department or support staff). There are two ways to identify an asset [12]. First, system-related information can be applied to describe the IT system and its operating environment. The second method is to use information gathering techniques to solicit information related to the IT system process environment. Common information gathering techniques include questionnaires, live interviews, document review and the use of automated scanning tools. The target asset can be a single or multiple interrelated system. In the latter case, the domain of interest and all interfaces and dependencies must be well defined before applying the method. Fig. 2 below shown a basic NIST step.

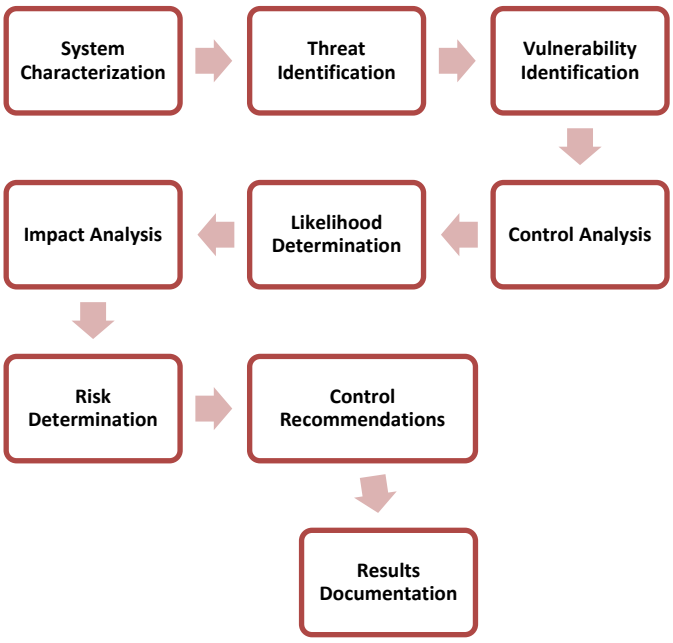

Fig. 2. NIST Basic Model [12]

B. The Operational Critical, Threat, Asset and Vulnerability Evaluation Process (OCTAVE)

The OCTAVE method was developed by the Software Engineering Institute (SEI) at Carnegie Mellon University. This approach was established to help organizations identify and assess the risks of information systems, improve their capabilities and protect themselves from these risks [13]. The OCTAVE method consists of a set of rules and a skilled analysis team. The team is made up of people within the organization and is designed to conduct risk assessment procedures. Collect opinions from the analysis team and participants through questionnaires and surveys [15], [16].

Based on the inputs provided, the analysis is done in a structured and organized manner. There are several pre- and post-assessment activities. The risk assessment process consists of three main steps and eight of these three steps.

The OCTAVE method can be extended to the OCTAVE standard, which is designed to meet the requirements of various situations. For example, a standard set can be applied to large organizations to small organizations. But the method is still the same and can be described as four main phases. The OCTAVE basic model is shown in the Fig. 3 below.

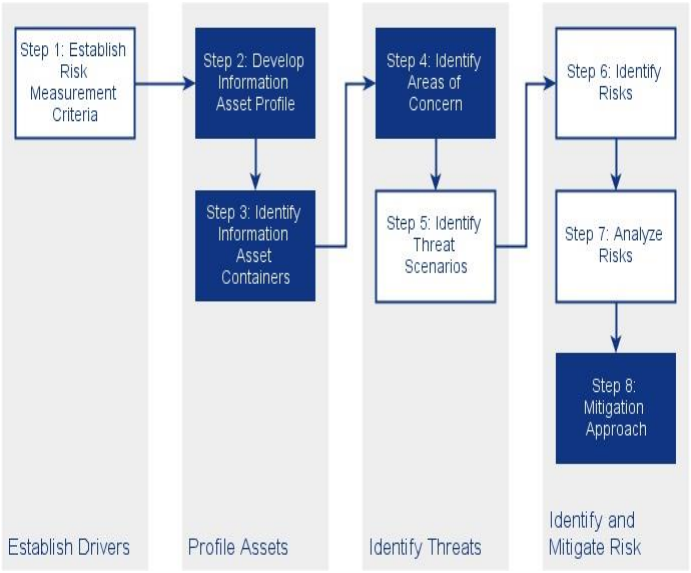

Fig. 3. OCTAVE Basic Model [13]

C. The Facilitated Risk Assessment Process (FRAP)

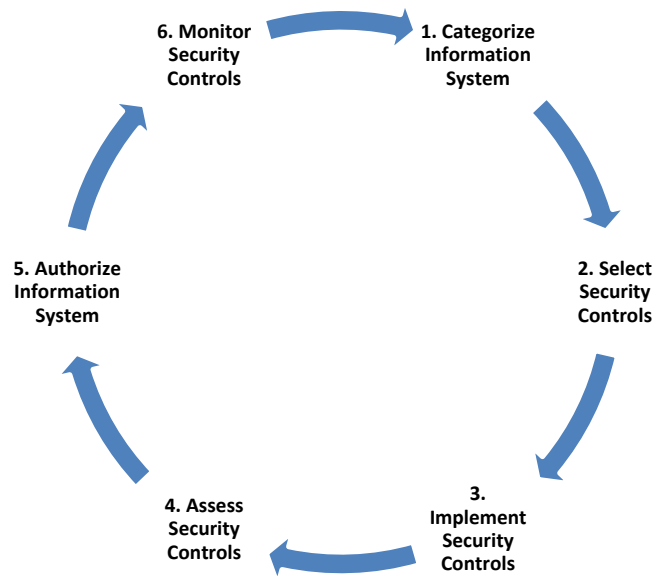

Fig. 4. FRAP Basic Model [18]

The Facilitating Risk Assessment Program (FRAP) was established by Thomas Peltier [17]. Peltier aims to implement risk management techniques in a cost-effective manner to adapt to the rapid development of the business sector. Peltier also emphasizes the involvement of employees in the organization, rather than the advice of external experts. Since the model is designed to prioritize time-cost efficiency, the program includes only the pre-FRAP meeting, the FRAP meeting and the FRAP meeting. In the pre-FRAP meeting phase, the goal is to introduce participants to FRAP and announce the procedures and goals of the meeting. Once the participants reach an agreement, they can hold a FRAP meeting. There are two steps involved during the FRAP meeting. The first step is to browse the logistics, introduce the entire team and briefly repeat what was discussed in the pre-FRAP meeting. The scope statement will then be exposed. In the second step, the FRAP team will review the elements to be reviewed, such as integrity, confidentiality and availability. The team also identifies threats, issues, and any other issues that may pose a vulnerability to the system. Next, the team will recommend controlling these vulnerabilities. After the FRAP meeting, the business manager, project leader and moderator will hold a meeting after the FRAP meeting and complete the action plan. The deliverables for this meeting include a summary of threats and existing controls, as well as a final report. The basic FRAP cycle model is shown in Fig. 4 below.

D. The Central Risk Analysis and Management Method (CRAMM)

The Central Computer and Telecommunications Authority (CCTA) Risk Analysis and Management Method (CRAMM) was developed by the British government in 1985. This tool has been developed and has been commercialized by Insight Consulting [19]. CRAMM is a qualitative tool that provides methods, calculations, and reports for security risk assessment.

The method and tool were developed mainly for application in large-scale organizations, but can be also applied to SMEs [20]. CRAMM can also be used to (a) Justify investment decisions in the security of information systems and networks, based on measurable results and (b) demonstrate the compatibility of the organizations' information systems with the British standard during an auditing process. CRAMM consists of five phases which shown in the Fig. 5.

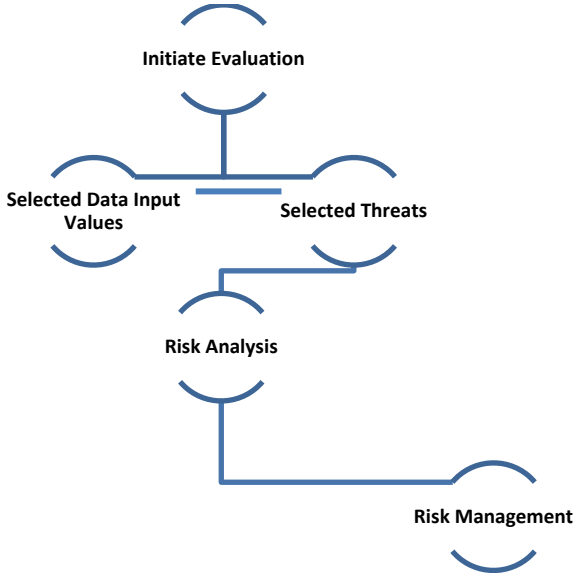

Fig. 5. CRAMM Basic Model [20]

III. Discussion

In general, OCTAVE and CRAMM methods are qualitative methods while FRAP is quantitative. NIST method is a combination of qualitative and quantitative types which is more dynamic and suitable for an organization. This makes the NIST model suitable for quantitative or qualitative research.

NIST risk assessment method is the most well-formed method. Each step has a specific target and enumerates several approaches to facilitate the procedure. Unlike the OCTAVE, CRAMM and the FRAP method, NIST method's collection to the data is not limited to participants' knowledge; it also includes conclusions and discoveries mentioned in other related documentation.

Furthermore, OCTAVE, CRAMM and FRAP merely offer descriptions of each step; while for the NIST method, each step enumerates all the possible approaches to process the data. On the other hand, the OCTAVE and FRAP method are usually applied to the business area while CRAMM specifically for an aviation area. Especially for the FRAP method, the author of the FRAP method, explicitly stated that the FRAP method is not designed to assess the compliance of security requirements.

TABLE I. COMPARISON AMONG SEVERAL RISK ASSESSMENT METHODS

Risk Assessment Methods	References	Types	Approach Phases	Resource Required
NIST	[1], [4], [12], [11], [21], [10], [22], [23]	Qualitative and Quantitative	• System characterization • Threat identification • Vulnerability Identification • Control analysis • Likelihood Determination • Impact analysis • Risk Determination • Control Recommendations • Result Documentation	Non-government organization
OCTAVE	[13], [14], [15], [20], [24]	Qualitative	• Profile threats • Identify infrastructure vulnerability • Develop a security strategy and plan	Internal and non-expert
FRAP	[16], [17], [25], [26]	Quantitative	• Pre-FRAP meeting • FRAP Session • Post-FRAP Process	Internal Manager
CRAMM	[18], [19]	Qualitative	• Asset Identification • Threat and vulnerability assessment • Countermeasure selection and recommendation	Qualified and experienced participant

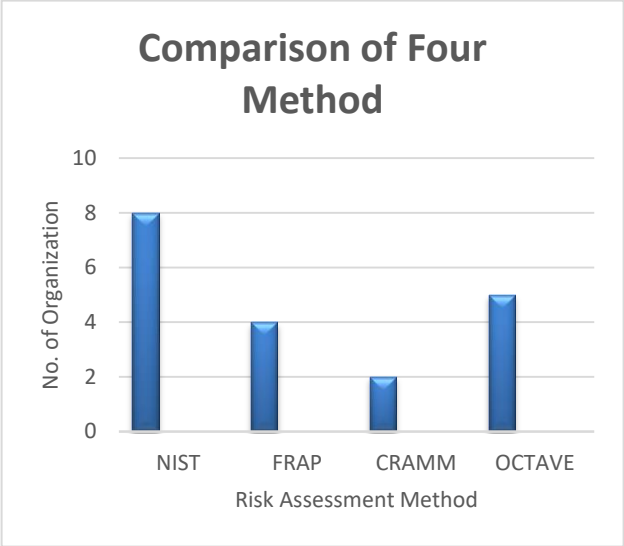

Fig. 6. Graph of four method

Both the FRAP and OCTAVE method is implemented to meet the business need and requires less time and resources. As mentioned earlier, the OCTAVE method has eight steps and needs knowledge from three levels – senior management, operational area management and staff. The FRAP method only has a pre-Frap meeting, FRAP session and post-FRAP discussion, which can be accomplished by the FRAP team in one day. Obviously, the OCTAVE method is more complicated than the FRAP method and requires more people's corporation.

In a word, the OCTAVE method is a workshop-oriented method and requires the participation from a different department. The FRAP method is designed for business analysis instead of a security assessment. The OCTAVE, CRAMM and FRAP is largely dependent on the participants' knowledge. As for the NIST method, the risk assessment process is refined into nine steps. Each step has a clear goal and all the possible approaches to accomplish the goal, which alleviate the bias brought by merely depend on participants' or security evaluator's knowledge.

The differences between all four methods have been simplified in Table I.

Figure 6 shows the comparison of the used method in the industry. Based on the graph it shows that NIST has 8 number of an organization has been used. Compared with FRAP 4 organization, CRAMM 2 organization and OCTAVE 5 organization. Findings of this study indicate that the NIST method more famous and well known used in an organization for risk assessment.

NIST method allows organizations to individually assess threats most relevant to their operations "and to develop a risk-based approach to resource allocation". It enables organizations to express their insider threat management efforts in terms of critical assets (identify); implemented controls and safeguards (protect); manifested threats (detect); formulated incident response strategies (respond); and business continuity plans (recover).

Therefore, the NIST method provides the most complete and scientific approach among all the methods.

IV. Conclusion and Future Works

Several case studies have been made to provides a risk-based detection method for insiders threats. It is not only to understand possible threats, but also help reduce overhead in the unified monitoring process. The results showed that the NIST method is well accepted in many organizations due to the systematic and convincing risk assessment planning. Besides this method is easy operative and practical. The framework can be improved further by assigning users to different classes according to their privileges and assigning different threshold values to each class.

Acknowledgment

The authors also would like to acknowledge Universiti Teknikal Malaysia Melaka. We also would like to thank the funding of this TRGS research grant: TRGS/1/2016/FKP-AMC/01/D00005 for funding this research.

References

[1] Y. Cherdantseva et al., "A review of cyber security risk assessment methods for SCADA systems," Comput. Secur., vol. 56, pp. 1–27, 2016.

[2] Z. Yunos, R. Ahmad, and N. A. Mohd Sabri, "A Qualitative Analysis for Evaluating a Cyber Terrorism Framework in Malaysia," Inf. Secur. J., 2015.

[3] L. Xiangyu, L. Qiuyang, and S. Chandel, "Social Engineering and Insider Threats," in 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2017.

[4] V. Morgagni, N. Nostro, A. Ceccarelli, and F. Brancati, "Insider Threat Assessment : a Model-Based Methodology," pp. 3–12, 2014.

[5] Z. Lai, Y. Shen, and G. Zhang, "A security risk assessment method of website based on threat analysis combined with AHP and entropy weight," in Proceedings of the IEEE International Conference on Software Engineering and Service Sciences, ICSESS, 2017.

[6] Y. Y. Haimes, Risk Modeling, Assessment, and Management, Third Edition. 2008.

[7] E. Zio, "The future of risk assessment," Reliab. Eng. Syst. Saf., vol. 177, no. March, pp. 176–190, 2018.

[8] D. W. Hubbard, The Failure of Risk Management: Why It's Broken and How to Fix It. 2009.

[9] R. K. Abercrombie, F. T. Sheldon, K. R. Hauser, M. W. Lantz, and A. Mili, "Risk assessment methodology based on the NISTIR 7628 guidelines," in Proceedings of the Annual Hawaii International Conference on System Sciences, 2013.

[10] National Institute of Standards and Technology, "NIST SP 800-53A, Assessing Security and Privacy Controls in Federal Information Systems and Organizations," NIST Spec. Publ., 2014.

[11] J. Kouns and D. Minoli, Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams. 2010.

[12] National Institute of Standards and Technology, "BEST PRACTICES IN CYBER SUPPLY CHAIN RISK MANAGEMENT," Nist, 2016.

[13] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process. 2007.

[14] M. T. Jufri, M. Hendayun, and T. Suharto, "Risk-assessment based academic information System security policy using octave Allegro and ISO 27002," in Proceedings of the 2nd International Conference on Informatics and Computing, ICIC 2017, 2018.

[15] D. C. Felegeanu et al., "A combined method for the analysis and assessment of risks and industrial safety," Environ. Eng. Manag. J., 2016.

[16] M. Masky, S. S. Young, and T. Y. Choe, "A novel risk identification framework for cloud computing security," in 2015 IEEE 2nd International Conference on InformationScience and Security, ICISS 2015, 2016.

[17] T. Peltier, "Information security risk analysis," Philos. Trans. A. Math. Phys. Eng. Sci., 2005.

[18] T. R. Peltier, "Implementing an information security awareness program," Inf. Syst. Secur., 2005.

[19] Z. Yazar, "A Qualitative Risk Analysis and Management Tool - CRAMM," 2002.

[20] T. Yang, E. D. Berger, S. F. Kaplan, and J. E. B. Moss, "CRAMM : Virtual Memory Support for Garbage-Collected Applications," in Proceedings of the 7th USENIX Symposium on Operating Systems Design and Implementation - OSDI'06, 2006.

[21] A. Syalim, Y. Hori, and K. Sakurai, "Comparison of risk analysis methods: Mehari, magerit, NIST800-30 and microsoft's security management guide," Proc. - Int. Conf. Availability, Reliab. Secur. ARES 2009, pp. 726–731, 2009.

[22] V. Jovanovic and J. K. Harris, "Systems and software assurance - A model Cyber Security course," in 2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2016 - Proceedings, 2016.

[23] National Institute of Standards and Technology, "NIST SP 800-37 Revision 1 Guide for Applying the Risk Management Framework to Federal Information Systems. A Security Life Cycle Approach," p. 102, 2010.

[24] A. Sarkheyli and N. Binti Ithnin, "Improving the current Risk analysis techniques by study of their process and using the human body's Immune System," 2010 5th Int. Symp. Telecommun. IST 2010, pp. 651–656, 2010.

[25] M. Tseng, C. Byrne, K. A. Evers, and M. B. Daly, "Dietary intake and breast density in high-risk women: a cross-sectional study.," Breast Cancer Res., vol. 9, no. 5, pp. 12–15, 2007.

[26] A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, "Taxonomy of information security risk assessment (ISRA)," Comput. Secur., vol. 57, pp. 14–30, 2016.