Available at
https://ejournal.ubibanyuwangi.ac.id/index.php/jurnal_tinsika (30 June 2024)
DOI:-

Jurnal Teknik industri, Sistem informasi dan Teknik informatika, 3(1), 2024, 41-47

Insider Threats: The Analysis using Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)

OCTAVE is usefull to determine and rank threats to an organization's vital resources

Luqman Hakim[1)]

[1)]*Program Studi Teknik Informatika, Fakultas Teknik, Universitas Bakti Indonesia*
Jalan Kampus Bumi Cempokosari No.40, Cluring - Banyuwangi 68482 (10pt Italic)

mailto:luqman@ubibanyuwangi.ac.id

Abstract – A good document management can lead to a good management of cybersecurity [1] specially to prevent ransomware. Ransomware is one of the cybersecurity threats that locks the computer via encryptions and one of the ways to prevent ransomware is to detect the existence of insider threats [2]. In a study, insider threats are defined as people who work in the company, have access to the system and take intentional or unintentional actions that affect the IT system [3]. According to Ponemon Institute data, the frequency of insider threats went up 47% between 2018 and 2020, and the cost of these occurrences raised to $11.45 million. The study additionally showed that it usually takes organizations 77 days to contain an event regarding an insider threat. The statistics are concerning, and organizations need to be ready to deal with this threat [4]. For the recent years (2020 to 2022), it was increased again by 44% [5]. A study suggests that one factor in insider threats is user habits / behaviour [6]. This is what underlies this research and writing to determine user behaviour in these small companies so that they can determine whether an insider threat really exists or not by conducting a risk assessment [7].

Keywords *–Unintentional Insider Threat, Insider Threat, SME, Risk Assessment, Human Element, OCTAVE.*

I. INTRODUCTION

Given that it occurred twice in the last two years, a ransomware attack on a small company's data center in Surabaya, Indonesia, raises major concerns about the need to further investigate the possibility of insider threats. In this instance, the company employs roughly 100 people, distributed over two locations. NAS is one of the company's most important and secret assets, and each location has a Domain Controller that oversees the shared drives from NAS to every PC. The organization and usage of assets are not well defined inside the corporation, and this contributed to the company's lack of awareness of its own resources during the disaster. This study aims to evaluate the company's cybersecurity capabilities based on the frequency of ransomware attacks. The results will inform an internal threat assessment that will concentrate on vital assets and user behavior within the organization..

A. Research Problem

The company that discussed this research has been able to run the business in the civil and architecture sector in daily operation activities but however when they are facing an attack of ransomware, they realise that there is something that needs to be done to solve that and prevent the same thing from happening in the future. The company has been able to activate and run a local domain controller that manages all the users and computers access rights but however this ability is not fully or completely setup so there is a gap between strategic planning [8] and the actual settings within the company.

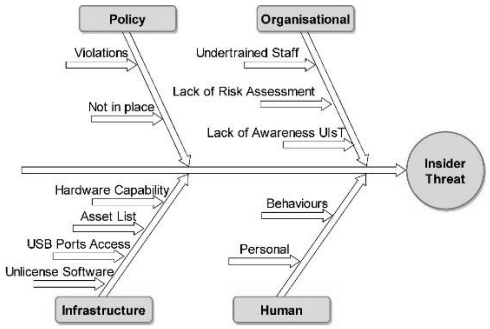

Figure 1.1 Above is the fishbone of problems that happened in the company.

B. Research Objective and Hypothesis

This research aims to:

a. Identify important assets available in the discussed company.
b. Assess the danger of vital assets in the discussed company.
c. Identify insider dangers.
d. Provide rules for computer security.

*) Corresponding author (Luqman Hakim)
Email: luqman@ubibanyuwangi.ac.id

Submitted: 1 June 2024; Revised: 12 Jube2024; Accepted: 29 June 2024; Published: 30 June2024

Available at https://ejournal.ubibanyuwangi.ac.id/index.php/jurnal_tinsika (30 June 2024)
DOI:-

One sort of insider threat is the inadvertent insider threat, or UIsT [9], which occurs when someone with access to the organization's system causes harm and damage without malevolent intent. According to those definitions, the following are the research hypotheses: One sort of insider threat is the inadvertent insider threat, or UIsT [9],, which occurs when someone with access to the organization's system causes harm and damage without malevolent intent. According to those definitions, the following are the research hypotheses:

a. Establish the list of important assets.
b. Assessing the impact and risk to vital assets.
c. Identifying sorts of insider dangers.
d. Defining UIsT actors based on Active Directory user and computer assignments.
e. Defining UIsT actors' habits using system logs.

II. METODE PENELITIAN

Figure 2.1 depicts the framework's three core areas, which are:

1. Assets are the input. This example will require data input from the future company because it is a company case study. This input can include physical data, immaterial data, or corporate information, such as asset classification. During this step, assets are identified and classified, with reference to current data sources. This data source could be physical data from the field or the outcomes of joint observations with business members.
2. There is a process. In the process area, there are two major sources or components that serve as the primary criteria: humans and assets. Conducting a risk assessment of the first stage's outcomes. At this time, the emphasis is on critical assets, which will employ OCTAVE Allegro, and human behavior, which will use HAIS-Q. Both of these procedures will generate results, which will then be evaluated and aligned. For example, are there vital assets that are well-managed by employees? This will provide information for the examination of the insider threat itself. In addition, it will be updated to reflect the company's excellence. The control side of the document is increasingly being explored; document mapping standards such as ISO/IEC 27001 and NIST SP 800 53 are employed.
3. Output includes reports, SOPs, and guidelines. A suggestion is made, followed by the development of standards of practice (SOPs). At this step, all research output will be converted into a report, which will subsequently be upgraded into company guidelines and SOPs.

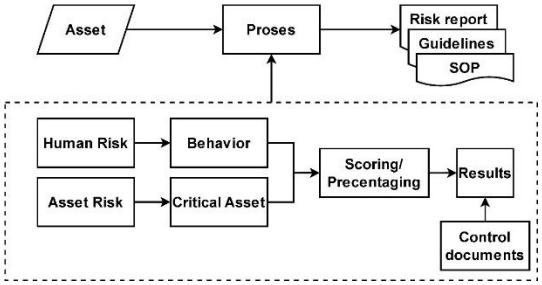

Figure 1.2 The research framework

A. Risk Identification

Use OCTAVE Allegro to assess essential assets and identify threats. It helps the company to think about how people, technology, and facilities interact with information in the context of the daily activities and services it supports.

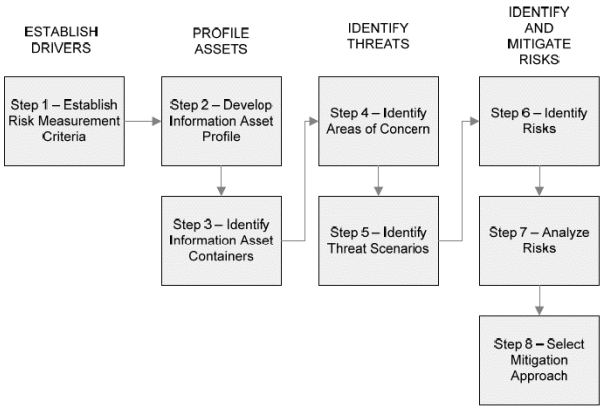

Figure 2.1 The OCTAVE Allegro process

Based on risk feature that has been identified, Table 2.1 below is the mapping indicator against the standard and or control that will be use during the research. This mapping will help organisation to develop and create the mitigation plan that will be implemented by creating the SOP and or guidelines.

Table 2.1 Indicator of problem mapping

Indicator	ISO 27001	NIST SP800 53 Rev5
The existence of malware	A.18.1.2	Software Usage Restrictions CM-10
	A.12.5.1, A.12.6.2	User-Installed Software CM-11
	A.12.2.1 Controls Against Malware	AT-2, SI-3
The use of computer at work	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	Awareness and Training Policy and Procedures AT-01

A standard set of worksheet templates will be used during this section. This worksheet is defined in the following Tables. For example, Table 2.2, Table 2.3 and

Submitted: 1 June 2024; Revised: 12 Jube2024; Accepted: 29 June 2024; Published: 30 June2024

Table 2.4 will be used for determining and define the risk measurement based on the defined criteria.

In related to the impact area produced by the OCTAVE allegro, it will correlate with the results in the behaviour assessment of the staff member. In relation to the assessment carried out using the HAIS-Q, because this is a questionnaire, we will use a Likert scale to determine the index value. The Likert scale formula that was used to analyse the data by computing the proportion of each element [10].

$$X_i = \frac{\sum S}{S_{max}} \times 100\% \quad [1]$$

Description:
S_{max} : Maximum score
$\sum S$: Scores
X_i : Value of each aspect of the questionnaire

Table 2.2 OCTAVE Allegro Worksheet 1 [11]

Allegro Worksheet 1	Risk Measurement Criteria Reputation and Customer Confidence		
Impact Area	Low	Moderate	High

Table 2.3 OCTAVE Allegro Worksheet 2 [11]

Allegro Worksheet 2	Risk Measurement Criteria – Financial		
Impact Area	Low	Moderate	High

Table 2.4 OCTAVE Allegro Worksheet 3 [11]

Allegro Worksheet 3	Risk Measurement Criteria – Productivity		
Impact Area	Low	Moderate	High

Table 2.5 Impact area priority sets [11]

Allegro Worksheet 7	Impact Area Prioritization Worksheet
Priority	Impact Area

To describe the impact of the any possible threats, then the area should be written in worksheet 7 as described in Table 2.5 above. While asset profile from the finding assets list, will be written in worksheet 8 as shown in Table 2.6 below.

Table 2.6 Asset profile [11]

Allegro Worksheet 8	Critical Information Asset Profile		
(1) Critical Asset What is the critical information asset?	(2) Rationale for Selection Why is this information asset important to the organization?	(3) Description What is the agreed-upon description of this information asset?	(4) Owner(s) Who owns this information asset?
(5) Security Requirements What are the security requirements for this information asset?			
☐ Confidentiality	Only authorized personnel can view this information asset, as follows:		
☐ Integrity	Only authorized personnel can modify this information asset, as follows:		
☐ Availability	This asset must be available for these personnel to do their jobs, as follows:		
	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.		
(6) Most Important Security Requirement What is the most important security requirement for this information asset?			

B. Develop of the guidelines and SOP

Guidelines and SOPs will be developed based on the results of current control mapping, policies, and research findings. If a gap exists, new policies or rules must be developed to address it; otherwise, the rules will relate to existing controls and standards. If there are any substantial differences, the SOP will explain the procedure in further detail, such as how to create a new user account. In this case, it is critical to understand who will be involved and what the inputs and outputs will be.

III. RESULTS AND DISCUSSION

The research location in this paper is in a company engaged in the engineering, construction, and architecture (AEC) sector in the city of Surabaya. according to Table 3.1 below, the number of main premises/offices is more than one in a city.

Submitted: 1 June 2024; Revised: 12 Jube2024; Accepted: 29 June 2024; Published: 30 June2024

Table 3.1 Company information

Name	Amount
Main Office	2
Branches	3
Hybrid Employees	30
Remote Employees	50
Onsite Employees	20
Servers	4
Workstations	50

Table 3.2 Company statistics before implementation

Event	Value
User active in AD	10
Password expiry	Never
Access Rights control	Disabled
Auto lock timeout	Disabled

According to Table 3.2 above we can see that there are some negative controls that exist in the company, for example there is no password expiration for the user.

As a stage in conducting an assessment for critical assets which in this case is carried out using OCTAVE Allegro, then some of the steps below are a manifestation of an 8 series of steps contained in OCTAVE Allegro.

Step 1 – Establishing Risk Measurement Criteria.

In this step will establish a set of qualitative metrics (risk measurement criteria) against which we can gauge how a risk may affect the organization's mission. In this step will create some output that is recorded in worksheets 1 to 3 that shown in Table 3.3, Table 3.4 and Table 3.5.

Table 3.3 Risk Measurement Criteria – Reputation and Customer Confidence

Allegro Worksheet 1	Risk Measurement Criteria – Reputation and Customer Confidence		
Impact Areas	Low	Moderate	High
Reputation	Reputation is minimally affected; little or no effort or expense is required to recover.	Reputation is damaged, and some effort and expense are required to recover.	Reputation is irrevocably destroyed or damaged.
Customer Loss	Less than 10 % reduction in customer	20 to 50 % reduction in customer	More than 50 % reduction in customers
	s due to loss of confidence	s due to loss of confidence	due to loss of confidence

Table 3.4 Risk Measurement Criteria – Financial

Allegro Worksheet 2	Risk Measurement Criteria – Financial		
Impact Areas	Low	Moderate	High
Operating Costs	Increase of less than 20 % in yearly operating costs	Yearly operating costs increase by 30 to 50 %.	Yearly operating costs increase by more than 50 %.
Revenue Loss	Less than 20 % yearly revenue loss	20 to 40 % yearly revenue loss	Greater than 50 % yearly revenue loss

Table 3.5 Risk Measurement Criteria – Productivity

Allegro Worksheet 3	Risk Measurement Criteria – Productivity		
Impact Areas	Low	Moderate	High
Staff Hours	Staff work hours are increased by less than 1 day(s).	Staff work hours are increased between 2 to 4 day(s).	Staff work hours are increased by greater than 5 day(s).

Table 3.6 Impact Area Prioritization Worksheet

Allegro Worksheet 7	Impact Area Prioritization Worksheet
priority	Impact Areas
1	Reputation/customer confidence
2	Financial
3	Productivity

Identifying Areas of Concern (see Table 3.6) which involves searching through each container to find any potential problems, then noting each area that is found. The regions were subsequently expanded to include threat scenarios, which were then documented to determine whether they had an impact on the security needs. But before that, we need to define the priority of impact area (see Table 3.6) that will use for next steps.

Submitted: 1 June 2024; Revised: 12 Jube2024; Accepted: 29 June 2024; Published: 30 June2024

Step 2 – Developing an Information Asset Profile
The information we need about your information asset is gathered in the actions below so that the structured risk assessment process may start. Worksheet 8 or the Critical Information Asset Profile will be used to document this information.

Step 3 – Identifying Information Asset Containers.
This step consists of just one activity: defining three crucial security-related aspects of the idea of information asset containers, including how the asset is protected, how well it is safeguarded, and how vulnerable and dangerous the containers are.

Step 4 – Identifying Areas of Concern
The first stage on this step is to create a risk profile for the information asset by exchanging ideas and searching for threat elements in potential threat situations. Areas of concern can be mapped by adhering to the Information Asset Risk Environment Maps and the Information Asset Risk Worksheet publications. After completing the Information Asset Risk Worksheet, the containers are examined to identify and document any potential problems.
Based in above area of concern, the risk scenario will be created which is a part of step 5, and this is shows in Table 3.7 below:

Table 3.3 Risk scenario from area of concern

No.	Area of Concern	Risk Scenario		Consequence
1	Distribution and attack of malware	Actor	Staff	All access to certain files will be hampered and tend to be inaccessible
		Mean	Browsing and download untrusted source	
		Motive	Unintentional	
		Outcome	Destruction and Modification	
		Prevention	Secured the data server	
2	Bypassing access to the server	Actor	Staff	Causing data leaks, malware, and loss of access to the shared drives and files.
		Mean	Gain access to the shared drive using NET USE command	
		Motive	Unintentional	
		Outcome	Interruption	
		Prevention	Correct the settings to standard	
3	Misuse of access	Actor	Staff	Leads to loss of
		Mean	Gain Access	
		Motive	Unintentional	trust in employees and possible compromised systems

Step 6 – Identifying Risks.
Record a value of "high," "medium," or "low" in the "Value" section of column (8) after assessing the outcome in relation to each of the impact categories using the risk measurement criteria and.
By completing the risk equation by determining how the organization is affected. Below is the equation to get the risk.

Risk =Threat (condition) + Impact (result) [11]
Risk = [Step 4 and 5] + [Step 6]

Step 7 – Analyzing Risks.
The Information Asset Risk Worksheet paperwork must be cited in the activities. Reviewing the risk assessment criteria comes first, then coming up with a relative risk value that can be used to analyze the risk and choose the best course of action.

Step 8 – Selecting Mitigation Approach.
Sorting out all detected risks based on their values is the first task in this step, which will help with the decision-making process about the risk's mitigation status. The second step is to implement the chosen risk-mitigation strategy by adhering to each risk's specific organizational circumstance. To do that, the risk matrix will be used to determine in which pool is the mitigation approach will be proceed.

Table 3.8 Mitigation results from OCTAVE Allegro process

No	Area of concern to critical assets	Score	Probability	Pool	Mitigation
1	Distribution and attack of malware	18	High	1	Mitigate
2	Bypassing access to the server	13	Medium	2	Mitigate to defer
3	Misuse of access	15	High	1	Mitigate

According to the results in Table 3.8, the assessment of the risk in NAS devices is the spreading and attacking of malware is very large when associated with file distribution techniques or shared drives. Where it is possible for staff to browse to various websites to download the required pirated application. The same goes for staff who simply get the path of a network drive by running the NET USE command, which will also endanger the company. Then what is also dangerous is staff knowingly let other people or colleagues use unlocked computers.

Submitted: 1 June 2024; Revised: 12 Jube2024; Accepted: 29 June 2024; Published: 30 June2024

IV. CONCLUTION

The proposed approach can produce the intended results for both essential assets and human behaviour. According to the data, the most critical assets are the NAS infrastructure and the files that are saved inside. These files include DWG, office files (xlsx, docx, pptx, pdf), image files (png, jpg, tiff), and video files (avi, mp4, hevc). The association between the results shows that mitigating human behavior leads to the activity of downloading files to the computer, whereas the affected important assets are access misuse and malware assault and dissemination. It also demonstrates the importance of human interaction in dealing with insider threats.

REFERENCES

[1] J. OConnor, "Document Management Software to Prevent Ransomware," eFileCabinet. Accessed: Feb. 12, 2023. [Online]. Available: https://www.efilecabinet.com/document-management-software-prevents-ransomware/

[2] E. Alhajjar and K. Lee, "The US Cyber Threat Landscape".

[3] J. Hunker and C. W. Probst, "Insiders and Insider Threats: An Overview of Definitions and Mitigation Techniques," *J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl.*, vol. 2, no. 1, pp. 4–27, 2011.

[4] K. Sharma, "ManageEngine Log360," ManageEngine Log360. Accessed: Jun. 08, 2023. [Online]. Available: https://www.manageengine.com/log-management/

[5] Ponemon, "Insider Threats are Organizations' Biggest Cybersecurity Risk | Proofpoint US," Proofpoint. Accessed: Jun. 08, 2023. [Online]. Available: https://www.proofpoint.com/us/resources/infographics/ponemon-cost-of-insider-threats-report

[6] N. Khan, R. J. Houghton, and S. Sharples, "Understanding factors that influence unintentional insider threat: a framework to counteract unintentional risks," *Cogn. Technol. Work*, vol. 24, no. 3, pp. 393–421, Aug. 2022, doi: 10.1007/s10111-021-00690-z.

[7] R. Ross, "Guide for Conducting Risk Assessments." Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, Sep. 17, 2012. doi: https://doi.org/10.6028/NIST.SP.800-30r1.

[8] S. A. Ebad, "Lessons learned from offline assessment of security-critical systems: the case of microsoft's active directory," *Int. J. Syst. Assur. Eng. Manag.*, vol. 13, no. 1, pp. 535–545, Feb. 2022, doi: 10.1007/s13198-021-01236-2.

[9] M. Collins *et al.*, "2016 - Common Sense Guide to Mitigating Insider Threats, Fifth Edition," Jan. 2021, doi: 10.1184/R1/12890918.v1.

[10] H. Komikesari, M. Mutoharoh, P. S. Dewi, G. N. Utami, W. Anggraini, and E. F. Himmah, "Development of e-module using flip pdf professional on temperature and heat material," *J. Phys. Conf. Ser.*, vol. 1572, no. 1, p. 012017, Jun. 2020, doi: 10.1088/1742-6596/1572/1/012017.

[11] R. Caralli, J. Stevens, L. Young, and W. Wilson, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, CMU/SEI-2007-TR-012, 2007. [Online]. Available: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8419

Submitted: 1 June 2024; Revised: 12 Jube2024; Accepted: 29 June 2024; Published: 30 June2024