**Uranus : Jurnal Ilmiah Teknik Elektro, Sains dan Informatika**
**Volume. 3, Nomor. 1, Tahun 2025**
e-ISSN : 3031-996X; dan p-ISSN 3031-9951; Hal. 36-47
DOI: https://doi.org/10.61132/uranus.v3i1.649
*Available online at:* https://journal.arteii.or.id/index.php/uranus

# Insider Threats: The Cybersecurity Analysis using OCTAVE Allegro which are combined with HAIS-Q

**Luqman Hakim**
Program Studi Teknik Informatika, Fakultas Teknik, Universitas Bakti Indonesia, Indonesia

Address: Jalan Kampus Bumi Cempokosari No.40, Dusun Cempokasari, Sarimulyo, Kec. Cluring, Kabupaten Banyuwangi, Jawa Timur 68482
*Email correspondence: luqman@ubibanyuwangi.ac.id*

***Abstract.*** *There are various types of cybersecurity threat in the globe, one of which is an insider threat. Because the current vulnerability generates an insider threat, SMEs suffer. In this situation, the company suffers a loss of profit and trust. Because of the speed and intensity of cybersecurity, particularly internal threats, SMEs must conduct regular vulnerability assessments. Insider threats to cyber security are a major issue in today's environment. Insider threats come in a variety of flavours, one of which is the unintended insider threat, or UIsT. This type of threat is a real one, and it is important to understand who and how they can become an insider threat.*

***Keywords****: Cybersecurity, Threats, Insider, SMEs*

## 1. INTRODUCTION

A company in the Architecture, Engineering, and Construction (AEC) industry in Surabaya, Indonesia, was targeted by ransomware and lost 2TB of data. The attack begins within a LAN network connected to an outside network, which finally allows malware to execute ransomware. This thesis will measure and test whether the insider threat really exists in the organization. What factors can cause someone to be categorized as an insider threat and why. This research departs from some of the current literature, which describes a variety of aspects of inadvertent insider risks to the actors involved. This research will produce recommendations or policies for minimizing and reducing the insider threat.

## 2. RESEARCH PROBLEM

The challenges for SMEs are getting bigger, especially when we talk about cybersecurity. with the existing characteristics of SMEs, the challenges also follow those types or characteristics. Research shows that most of the challenges of SMEs is less awareness of the cyberthreats, less cybersecurity budget, less human resources in ICT, less guidelines on ICT and there is a low support from the management [1]. Those challenges are applied for SMEs in the construction industry section where they do activities for building and civil engineering. Another research shows that 49% of the 113 SMEs are not using IT Tools for their daily activity, where one of the IT Tools that has been mentioned is Document Management [2].

*Received: Desember 17, 2024; Revised: Desember 27, 2024; Accepted: Januari 13, 2025;*
*Online Available : Januari 14, 2025*

## 3. RESEARCH OBJECTIVE AND HYPOTHESIS

This research aims to:

a. To define the critical assets that are available in the discussed company.

b. To conduct the risk assessment of critical assets in the discussed company.

Unintentional insider threat, or UIsT, is one type of insider threat [3] where someone who has access to the system of the organization and had no malicious intent that causes harm and damage to the organization. Based on these definitions, these are the hypothesis of this research:

a. Define the list of critical assets.

b. Calculating the impact and risk for those critical assets.

## 4. RESERACH METHOD

By looking at the figure 1.2 there are three parts of the method that can be done. As the main thing to solve this problem is the input in the form of initial data. This initial data consists of literature reviews [4], [5], [6] from various sources or journals that have been conducted by previous researchers. Then the data from the problem identification or problem formulation results. Then we proceed to several key aspects of this research, namely data obtained from interviews [7], [8] and calculations using HAIS-Q[9], [10] and OCTAVE Allegro [11], [12]. As for the data that is equally important, it includes information or documents from the company or case studies that are currently being researched. This will be very helpful in showing accurate results.

OCTAVE Allegro helps us determine which assets are critical in a company by filling out several forms for which templates have been provided. HAIS-Q will produce output that can serve as a reference for mitigation because it contains several fundamental and comprehensive questions about the potential for cybersecurity vulnerabilities within a company.

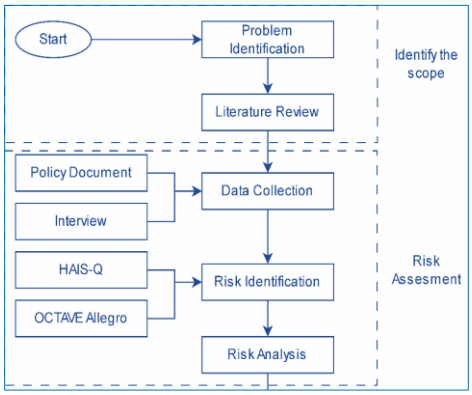


**Figure 1.** the research framework

**Risk Identification**

To evaluate critical assets and find threats, use OCTAVE Allegro where the processes can be seen at figure 1. It assists the business in considering how facilities, technology, and people interact with information in relation to the daily operations and services it provides.

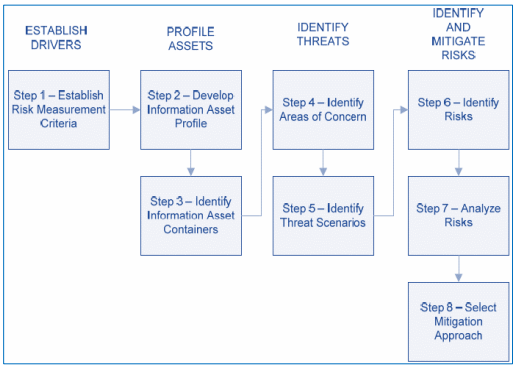


**Figure 2.** The OCTAVE Allegro process

Table 1 below shows the mapping indicator against the standard and/or control that will be used during the research based on the risk feature that has been discovered. By developing the SOP and/or guidelines, this mapping will assist the organization in developing and creating the mitigation plan that will be put into action.

**Table 1.** Indicator of problem mapping

| Indicator | ISO 27001 | NIST SP800 53 Rev5 |
|---|---|---|
| The presence of malicious software | A.18.1.2 | Software Use Limitations CM-10 |
| | A.12.5.1, A.12.6.2 | Software Installed by the User CM-11 |
| | A.12.2.1 Controls Against Malware | AT-2, SI-3 |
| Using a 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 | Policy and Procedures for Training and Awareness AT-01 |

In this section, a standard set of worksheet templates will be utilized. The following tables define this worksheet. Tables 2, 3, and 4, for instance, will be utilized to establish and determine the risk measurement according to the specified criteria.

The outcomes of the staff member's behaviour evaluation will be correlated with the effect area generated by the OCTAVE allegro. Since the HAIS-Q is a questionnaire, we will use a Likert scale to calculate the index value for the assessment. By calculating the proportion of each factor, the data was analysed using the Likert scale formula [13].

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

Description:

$S_{max}$ : Maximum score

$\sum \quad S$ : Scores

$X_i$ : The importance of every component of the survey

**Table 2.** OCTAVE Allegro Worksheet 1 *[14]*

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

**Table 3.** OCTAVE Allegro Worksheet 2 *[14]*

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

**Table 4.** OCTAVE Allegro Worksheet 3 *[14]*

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

**Table 5.** Impact area priority sets *[14]*

| Allegro Worksheet 7 | Impact Area Prioritization Worksheet |
|---|---|
| Priority | Impact Area |
| | |

The area should be recorded in worksheet 7 as indicated in Table 5 above to describe the impact of any potential risks. Worksheet 8 will be used to write the asset profile from the finding assets list, as indicated in Table 6 below.

**Table 6.** Asset profile *[14]*

| 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? | | | |
| □ Confidentiality | □ Integrity | □ Availability | □ Other |

**Creating The Standard Operating Procedure And Guidelines**

Current control maps, policies, and research findings will all be used to inform the development of guidelines and SOPs (Standard Operating Procedures). The rules will relate to current controls and standards unless there is a gap that needs to be filled by new policies or regulations. The SOP will go into more detail about the process, including how to create

a new user account, if there are any significant variations. Knowing who will be engaged and what the inputs and outputs will be is crucial in this situation.

## 5. RESULTS AND DISCUSSION

This paper's research site is a business located in the Surabaya city that works in the engineering, construction, and architecture (AEC) industry. There are multiple major offices or premises in a city, as shown in Table 7 below.

**Table 7.** Company information

| *Name* | Amount |
|---|---|
| ***Headquarters*** | 2 |
| *Branches* | 3 |
| *Hybrid* ***Workers*** | 30 |
| *Remote* ***Workers*** | 50 |
| *Onsite* ***Workers*** | 20 |
| *Servers* | 4 |
| *Workstations* | 50 |

**Table 8.** Prior to deployment, company statistics

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

As can be seen from Table 8 above, the corporation has certain negative controls in place. For instance, the user's password does not expire. Some of the procedures listed below are an example of an eight-step series found in OCTAVE Allegro, which is used in this instance to assist in the assessment of important assets.

***Step 1: Developing Criteria for Risk Measurement.***

To assess how a risk might impact the organization's mission, a set of qualitative metrics (risk measurement criteria) will be established in this step. Worksheets 1 through 3 will produce some output in this step, which is displayed in Tables 9, 10, and 11.

**Table 9.** Reputation and Customer Confidence as Risk Measurement Criteria

| 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 customers due to loss of confidence | 20 to 50 % reduction in customers due to loss of confidence | More than 50 % reduction in customers due to loss of confidence |

**Table 10.** Financial Risk Measurement Criteria

| 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 reven | 20 to 40 % yearly revenue loss | Greater than 50 % yearly revenue loss |

| | | | |
|---|---|---|---|
| | ue loss | | |

**Table 11.** Productivity as a Risk Measurement Criteria

| 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 12.** Worksheet for Impact Area Prioritization

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

Finding Areas of Concern entails going through each container to look for any possible issues, then noting each one that is discovered (see Table 12). After that, the regions were enlarged to include threat scenarios, which were then recorded to see if they affected the security requirements. The effect area priority that will be used for the following actions must first be determined (see Table 12).

***Step 2 - Creating an Information Asset Profile***

The steps listed below collect the data we require about your information asset so that the structured risk assessment process may begin. This information will be recorded using the Critical Information Asset Profile or Worksheet 8.

***Step 3 - Finding Information Asset Containers***

Determining three essential security-related elements of the concept of information asset containers—how the asset is protected, how well it is safeguarded, and how vulnerable and hazardous the containers are—is the only task involved in this stage.

***Step 4 – Identifying Areas of Concern***

Creating a risk profile for the information asset is the initial step in this process, which involves brainstorming and looking for threat elements in possible threat scenarios. By following the Information Asset Risk Worksheet publications and the Information Asset Risk Environment Maps, areas of concern can be mapped. The containers are inspected to find and record any possible issues following completion of the Information Asset Risk Worksheet.

As part of step 5, the risk scenario will be developed based on the mentioned area of concern, as indicated in Table 13 below:

**Table 13.** Risk scenario from area of concern

| No. | Area of Concern | Risk Scenario | | Consequence |
|---|---|---|---|---|
| 1 | The dissemination and assault of malicious software | 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 | Getting around the server | Actor | Staff | Causing data leaks, malware, and loss of access to the shared drives |
| | | Mean | Gain access to the shared drive using NET USE command | |
| | | Motive | Unintentional | |
| | | Outcome | Interruption | |

| | | | | |
|---|---|---|---|---|
| | | Prevention | Correct the settings to standard | and files. |
| 3 | Abuse of access | Actor | Staff | Leads to loss of trust in employees and possible compromised systems |
| | | Mean | Gain Access | |
| | | Motive | Unintentional | |

***Step 6 – Identifying Risks***

After evaluating the result in respect to each of the effect categories using the risk measurement criteria and enter a value of "high," "medium," or "low" in the "Value" section of column (8). by figuring out how the organization is impacted and completing the risk equation. The formula to calculate the risk is shown below. Risk =Threat (condition) + Impact (result) [14]

Risk = [Step 4 and 5] + [Step 6]

***Step 7 – Analyzing Risks***

The activities must include citations to the Information Asset Risk Worksheet documentation. Prior to determining a relative risk value that may be utilized to assess the risk and choose the optimal course of action, the risk assessment criteria must be reviewed.

***Step 8 – Selecting Mitigation Approach*.**

This step's first objective is to sort all identified risks according to their values, which will aid in determining the risk's mitigation status. Implementing the selected risk-mitigation plan while considering the unique organizational circumstance of each risk is the second stage. To do this, the risk matrix will be utilized to identify the pool in which the mitigation strategy will be implemented.

The findings in Table 14 indicate that there is a significant danger of malware spreading and attacking NAS equipment when it comes to file distribution methods or shared drives. where employees can visit different websites to download the necessary pirated application. The same is true for employees who only use the NET USE command

to obtain a network drive's path, putting the business at risk. Knowingly allowing coworkers or other individuals to access open computers is likewise risky.

**Table 14.** OCTAVE Allegro process mitigation outcomes

| No | Area of concern to critical assets | Score | Probability | Pool | Mitigation |
|---|---|---|---|---|---|
| 1 | The dissemination and assault of malicious software | 18 | High | 1 | Mitigate |
| 2 | Getting around the server | 13 | Medium | 2 | Mitigate to defer |
| 3 | Abuse of access | 15 | High | 1 | Mitigate |

## 6. CONCLUSION

The suggested method can yield the desired outcomes for both human behaviour and necessary assets. The research indicates that the NAS system and the files stored there are the most important assets. DWG, office files (xlsx, docx, pptx, pdf), picture files (png, jpg, tiff), and video files (avi, mp4, hevc) are some examples of these files. The correlation between the findings demonstrates that although reducing human behaviour encourages the downloading of files to the computer, access abuse and malware attack and distribution are the impacted critical resources. It also highlights how crucial interpersonal communication is in addressing insider threats.

## REFERENCES

C. and E. U. A. for Cybersecurity, Paggio, V., Bafoutsou, G., & Sarri, A. (2021). *Cybersecurity for SMEs: Challenges and recommendations*. Publications Office. https://doi.org/10.2824/770352

Caralli, R., Stevens, J., Young, L., & Wilson, W. (2007). Introducing OCTAVE Allegro: Improving the information security risk assessment process. *Software Engineering Institute, Carnegie Mellon University*. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8419

Collins, M., et al. (2021). Common sense guide to mitigating insider threats, fifth edition. https://doi.org/10.1184/R1/12890918.v1

García-Porras, C., Huamani-Pastor, S., & Armas-Aguirre, J. (2018). Information security risk management model for Peruvian SMEs. In *2018 IEEE Sciences and Humanities*

*International Research Conference (SHIRCON)* (pp. 1–5). IEEE. https://doi.org/10.1109/SHIRCON.2018.8592994

Gilbert, N. (2022). 31 crucial insider threat statistics: 2022 latest trends & challenges. *FinancesOnline.com*. Accessed December 3, 2022. https://financesonline.com/insider-threat-statistics/

Greitzer, F. L., et al. (2014). Unintentional insider threat: Contributing factors, observables, and mitigation strategies. In *2014 47th Hawaii International Conference on System Sciences* (pp. 2025–2034). IEEE. https://doi.org/10.1109/HICSS.2014.256

Irani, E. (2019). The use of videoconferencing for qualitative interviewing: Opportunities, challenges, and considerations. *Clinical Nursing Research, 28*(1), 3–8.

Komikesari, H., et al. (2020). Development of e-module using flip pdf professional on temperature and heat material. *Journal of Physics: Conference Series, 1572*(1), 012017. https://doi.org/10.1088/1742-6596/1572/1/012017

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, *42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2013). The development of the human aspects of information security questionnaire (HAIS-Q). In *ACIS 2013: Information Systems: Transforming the Future*. RMIT University.

Rafiah, K. K., Widianto, S., Kamal, I., Shofiana, A., Fajar, A. M., & Rudini, A. A. (2022). Digital readiness of SMEs: An insight from Indonesia. *AFEBI Management and Business Review*, *7*(1), Article 1. https://doi.org/10.47312/ambr.v7i01.517

Sarkar, K. R. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. *Information Security Technical Report, 15*(3), 112–133. https://doi.org/10.1016/j.istr.2010.11.002

Shapka, J. D., Domene, J. F., Khan, S., & Yang, L. M. (2016). Online versus in-person interviews with adolescents. *Computers in Human Behavior*, *58*, 361–367. https://doi.org/10.1016/j.chb.2016.01.016

Suroso, J. S., & Fakhrozi, M. A. (2018). Assessment of information system risk management with Octave Allegro at education institution. *Procedia Computer Science*, *135*, 202–213. https://doi.org/10.1016/j.procs.2018.08.167