Countermeasure against Insider Threat Regarding Psychological State of Organizational Members and Business Impact of Information Resources

Yuki Kodaka *
*Department of Informatics
The Graduate University
for Advanced Studies
Tokyo, Japan
e-mail: y_kodaka@nii.ac.jp

Hirokazu Hasegawa †
†Center for Strategic Cyber
Resilience Research and Development
National Institute of Informatics
Tokyo, Japan
e-mail: hasegawa@nii.ac.jp

Hiroki Takakura †
†Center for Strategic Cyber
Resilience Research and Development
National Institute of Informatics
Tokyo, Japan
e-mail: takakura@nii.ac.jp

***Abstract*—Compared to external cyberattacks, insider threats caused by organizational members can spread more widely within the organization even at an early stage, leading to significant impacts, such as business interruptions. When illicit activities are disguised as routine operations, it becomes difficult to detect them from behavioral records, such as violations of access privileges to information resources. Therefore, this paper proposes a countermeasure against insider threats regarding the psychological state of organizational members and the business impact of information resources. In addition to system operation record, the psychological state of each member is estimated using Human Resource data, such as stress tests, demotions, and salary reductions, which are held by the organization. Based on these assessments, we assess the risk of potential insider threats. Additionally, we assess the impact on the organization if information resources are leaked or become unusable, based on their operational usage. To mitigate these risks, we propose implementing countermeasures to prevent staged sabotage activities or automatically roll back executed sabotage actions. This approach aims to minimize business downtime and suppress further malicious activities, reducing the impact on business operations. However, not all Human Resource data can be used due to legal, ethical, and privacy concerns that vary across countries. Future work should examine how the accuracy of risk assessment changes when the number of assessment items is reduced.**

Keywords-insider threat; psychological state analysis; business impact analysis.

I. INTRODUCTION

Nowadays, information systems face several security threats. Among them are insider threats, which originate from internal elements, such as members of the organization that are supposed to be trusted. Traditional security measures were focused on external intruders, such as hackers. However, due to the significant impact and difficulty of countering insider threats, addressing these threats has become a pressing issue.

Insider threats are perpetrated by individuals with knowledge of systems and business processes, as well as authorised access privileges. Unlike external threats, insiders have easy access to an organization's information systems and information resources, making them more likely to cause widespread damage. According to a study by the Ponemon Institute [1], the cost of lost sales and technology due to business interruption caused by insider threats is $8.3 million in 2018 and $15.38 million in 2022, an increase of 85%.

According to the Vormetric insider threat report [2], 89% of respondents expressed concern about insider threats, whereas only 11% of respondents believed they were adequately prepared to address these threats. An effective countermeasure against insider threats involves detecting signs of unauthorized activities in advance or promptly responding when such activities occur. Insider threats are usually accompanied by unusual or suspicious activities before the actual attack [3]–[5]. However, it is challenging to distinguish between normal and malicious activities based solely on system activity. Furthermore, insider threats may intentionally hide their actions, making it even more difficult to detect the early signs of an attack. Additionally, since a huge amount of access records are generated on the system, it is difficult to manually or automatically detect malicious activities among them. Consequently, it is necessary to limit the access records to a manageable volume that allows for effective analysis.

Therefore, this paper proposes a countermeasure against insider threat regarding the psychological state of organizational members and the business impact of information resources. Since the members of an organization are potential sources of insider threats, they possess extensive knowledge about the organization. On the other hand, the organization also has a lot of information about its members, which is utilized for the countermeasures against insider threats. The risk assessment of potential insider threats is conducted for the organization's members, taking into account their psychological states. Specifically, risk assessments are conducted for each of the two categories of insider threats, i.e., sabotage activities against systems and data. Based on the results, any operation seen as progressing sabotage activities is monitored within the target information system. As a countermeasure, if sabotage activities are progressing step-by-step while hiding malicious actions, the proposed system prevents them at the previous step. If sabotage activities are suddenly executed, the proposed system quickly rolls back the executed operations to minimize downtime. The contaminated data by operations that cannot be rolled back, such as deletion, tampering, and encryption, is replaced using backup data.

This paper is organized in the following sections. Section II refers to related work to this paper. Section III describes the assumptions of the proposed system. After that, we explain the design of the proposed system. Section IV describes the challenges in realizing implementation of the proposed system. Section V concludes this paper and presents future work.

II. Related work

A. Insider Threat Detection

There are works on insider threat detection methods based on access logs and access order to files. Gates et al. proposed a method to create profiles from user activities to files and use them for insider threat detection and risk mitigation [6]. Toffalini et al. proposed a masquerader detection method that measures the similarity between user access history and newly recorded accesses [7]. These studies utilize only information available on the system for insider threat detection.

In addition to the information obtained from the system, there are works on insider threat detection methods that take into account the psychological state of the user. Greitzer et al. proposed a framework that utilizes psychological data in addition to traditional security audit logs to make the prediction of potential insider threats possible [8]. In subsequent research, they proposed a method for modeling psychological predictors of potential insider threats and identifying high-risk employees [9]. Kandias et al. proposed a method for predicting insider threats based on narcissism, a personality trait identified as a sign of insider threat [10]. In subsequent research, they explored the prediction of insider threats from social media, considering psychological aspects [11]. Additionally, they proposed a method for predicting insider threats based on users' negative comments on videos, viewing these comments as indications of malevolent insiders to law enforcement and authorities [12]. Taylor et al. proposed an insider threat detection method based on changes in the English language in emails [13]. While previous studies have focused on risk assessments related to members, they have not addressed the risks associated with information resources. Additionally, no classification or analysis has been conducted regarding the varying motives and targets of insider threats based on their objectives. Our approach evaluates risks by considering both member attributes and behaviors, while also incorporating assessments of information resources. This allows us to identify high-value or business-critical assets likely to be targeted, enabling proactive monitoring. Furthermore, we propose countermeasures to prevent insider attacks, going beyond mere detection.

B. Case Studies of Insider Threats

There are works on insider threat cases that investigate the motives and background of the insiders. In sabotage activities against systems, it was often observed that technical staff members used administrative privileges to carry out these actions [14]. The motives cited included job-related stress, dissatisfaction with the organization, and a desire for revenge. The causes of stress and dissatisfaction were financial issues, such as annual salary and bonuses, as well as missed promotions and advancement opportunities. Demotion or dismissal was specifically mentioned as a cause of seeking revenge [15]. Mental illnesses, such as alcoholism, drug addiction, panic disorder, and seizure disorder, along with family circumstances, like relationships with spouses, were found to influence the offender's behavior. Additionally, some offenders had a history of previous arrests.

In sabotage activities against data, it was often non-technical members of the workforce who carried out these actions [16]. The motives included financial gain to cover medical expenses related to addiction problems and financial assistance for family and friends [15]. Additionally, some activities were driven by emotional reasons, such as desire and need [16].

III. Proposed system

In order to prevent activities that pose a threat to organizational operations, the proposed system performs a risk assessment of potential insider threats using information on members. Based on the results, the system monitors the operations of members with high insider threat risk. As countermeasures, the system prevents staged sabotage activities by these members and swiftly rolls back unexpected sabotage activities to minimize damage. For the contaminated data, the system uses backup data to provide replacements.

A. Assumption

First, this subsection explains the insider threats targeted by the proposed system and the assumptions about information used held by the organization for risk assessment.

1) Two categories of insider threats: This system focuses on preventing electronic sabotage of information resources by insiders. Sabotage means making resources unusable for others. Preventing physical sabotage is beyond the scope of this paper because it is difficult to protect information resources once physical access is gained. Additionally, since the theft of information assets cannot be undone once it occurs, theft prevention is also out of scope.

Insider threats are divided into two categories: data sabotage and system sabotage. Since the expected sabotage activities differ between these two categories, the proposed system provides specific countermeasures for both data sabotage and system sabotage.

In the case of data sabotage activities, examples include deletion, modification, and encryption of the contents. Additionally, modifying access privileges and operations on upper-level directories (deletion, modification of access privileges) are also considered sabotage activities against data because they render the data unusable by other members.

On the other hand, in the case of system sabotage activities, activities, such as system shutdown, Operating System destruction, and network blocking are considered sabotage, as well as the deletion, modification, and embedding of malicious code in the system's source code.

2) Information held by the organization:

- Information about members
  In general, Asian countries have been slow to implement background checks, whereas many countries in Europe and the United States have adopted them. In the U.S., employers are legally required to conduct background checks before hiring due to the liability for negligent hiring, which refers to the failure to properly investigate an employee's background. Background checks can include debt and credit checks, health checks, nationality verification, criminal background checks, and social media and internet checks [17]. It is assumed that organizations possess this information at the time of hiring or during employment.
  The organization is assumed to collect information about the personality traits of its members through aptitude tests or other methods during the recruitment process. For instance, a five-factor personality test can provide information on traits, such as openness, honesty, extroversion, cooperativeness, and neuroticism [18].
  Furthermore, the organization is assumed to have information on stress check tests conducted periodically on its members, possibly in the form of an Employee Assistance Program (EAP) [19].
- Information about information resources
  In order for an organization to protect and effectively utilize its information resources, appropriate risk management commensurate with their value is necessary. ISO/IEC 27001 recommends that, as a first step in risk management, an organization should understand its information assets. Information resources are selected data and systems that an organization manages, such as information systems, databases, software, personnel information, customer information, financial information, and product technology information. The information asset register is used to identify these information resources. The register includes details, such as asset name, asset description, asset owner, asset location, and asset value. As an example of the method for calculating asset value, there is an approach that evaluates the asset from the perspectives of confidentiality, integrity, and availability, with each aspect being rated on three levels, making a total of nine levels [20]. It is assumed that the organization maintains an information resource management ledger for risk management purposes.

B. Outline of Proposed System

To detect and counter sabotage activities by insider threats, the proposed system conducts three types of risk assessments. Figure 1 shows the conceptual diagram of the insider threat risk assessment performed by the proposed system. Member risk assessment evaluates the potential risk of members becoming insider threats. Information resource risk assessment evaluate the impact when targeted and destroyed. Insider threat risk assessment combines the results of the member risk assessment and the information resource risk assessment to evaluate overall insider threat risk.

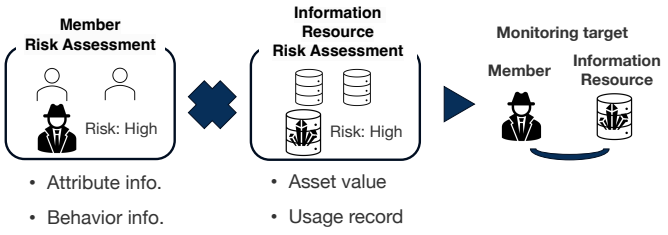

Figure 1. Conceptual Diagram of Internal Threat Risk Assessment.

C. Architecture of Proposed System

The architecture of the proposed system is shown in Figure 2. The proposed system consists of five modules: member risk assessment, information resource risk assessment, insider threat risk assessment, operation monitoring, and detection and action, as well as two databases: directory service and sabotage activity operation path database. The sabotage activity operation path database stores operation paths to achieve sabotage activities for each of the two threat categories. The following section describes the system processing procedure using Figure 2, and the details of member risk assessment, information resource risk assessment, insider threat risk assessment, and operation monitoring are explained in Sections III-D, III-E, III-F, and III-G.

1) The member risk assessment module evaluates the risks of each member based on the assessment items described in Section III-D and sends the results to the insider threat risk assessment module
2) The information resource risk assessment module evaluates the risk of each information resource based on its asset value and usage as recorded and sends the results to the insider threat risk assessment module
3) The insider threat risk assessment module evaluates the insider threat risk based on the member risk assessment and the information resource risk assessment
   If judged as an potential insider threat, it sends the combination of members and information resources to the operation monitoring module
4) The operation monitoring module identifies the operations required to execute the insider threat from the sabotage activity operation path database and sends those operations to the detection and action module
5) The detection and action module monitors target log records generated by the directory service and servers, and takes certain actions
   As countermeasures, it takes actions, such as changing privileges to prevent sabotage activities and rolling back operations after they have occurred

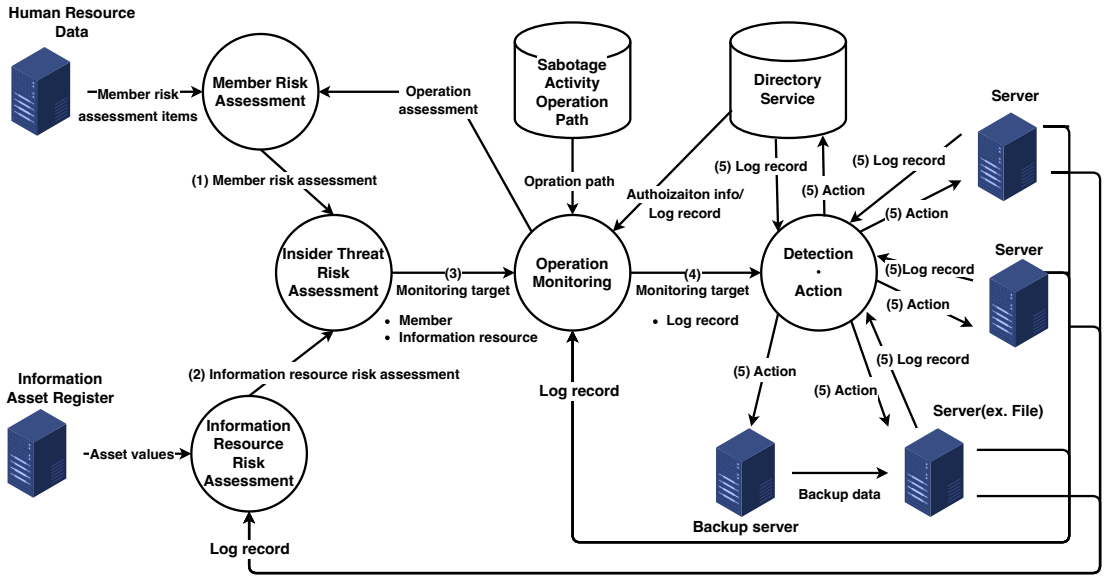

Figure 2. Architecture of Proposed System.

D. Member Risk Assessment

The member risk assessment module evaluates the risks of each member by two categories of insider threats from the information held by the organization.

a) Member risk assessment items: Based on a survey of multiple references analyzing case studies on insider threats, it was found that there are distinctive attributes common to organizational members who committed insider threats. The following assessment items are to be used for assessing the risk of insider threats among organizational members.

- Financial status (annual income, debt, credits) [3][5][8][21]
- Lifestyle status (family issues) [3][14]
- Health status (drug addiction, alcoholism, mental illness) [14]
- Criminal record (arrests) [3][21]
- Personality characteristics (excitement, neurotic tendency, hostility, lack of co-ordination, lack of conscience, self-love tendency) [3][5][21]
- Emotions (stress, lack of job satisfaction, anger, vengeance, lack of belonging to the organization) [3][5][21]
- Personnel (demotion, termination, job change) [5][14][21]
- Job type (technical position) [14]
- Privilege (administrative privileges) [16]

b) Member risk assessment items by two categories of insider threat: Using the above assessment items, member risk assessment is conducted for each of the two categories of insider threats. Based on the case studies of insider threats in Section II-B, we picked up the assessment items that are not identical but are considered to relevant as assessment items for each category of insider threats.

- System sabotage activities (18 items)
  Financial status (annual income, debt, credits), Life status (family issues), Health status (drug addiction, alcoholism, mental illness), Criminal record (arrests), Emotions (stress, lack of job satisfaction, anger, vengeance, lack of belonging to the organization), Personnel (demotion, termination, job change), Job type (technical position), Privilege(administrative privileges)
- Data sabotage activities (13 items)
  Financial status (annual income, debt, credits), Health status (drug addiction, alcoholism, mental illness), Personality traits (excitement, neurotic tendency, hostility, lack of co-ordination, lack of conscience, self-love tendency), Job type (technical position)
  Since the job type is non-technical position, the value needs to be inverted in the next step of binarization.

c) Binary conversion of risk assessment items: Each item is marked as 1 if applicable, otherwise as 0. For annual income, it is marked as 0 if above the industry, occupation, and age average, and 1 if below. For credits, a long-term payment delay is marked as 1, otherwise as 0.

d) Member risk assessment: Based on the attributes of each member, the risk assessments of sabotage activities against systems and data by member i are defined as follows:

$$R_{\text{system\_attribute\_member\_i}} = \frac{1}{n_{\text{system\_attribute}}} \sum_{x} v_{x,\text{system\_attribute\_member\_i}} \cdot w_{x,\text{system\_attribute}}$$
$$(0 \leq R_{\text{system\_attribute\_member\_i}} \leq 1) \quad (1)$$

$$R_{\text{data\_attribute\_member\_i}} = \frac{1}{n_{\text{data\_attribute}}} \sum_{x} v_{x,\text{data\_attribute\_member\_i}} \cdot w_{x,\text{data\_attribute}} \quad (0 \leq R_{\text{data\_attribute\_member\_i}} \leq 1) \tag{2}$$

where $n_{\text{system\_attribute}}$ is the number of assessment items related to system sabotage activities, $v_{x,\text{system\_attribute\_member\_i}}$ is the score of assessment item x for member i related to system sabotage activities, $w_{x,\text{system\_attribute}}$ is the weight of the assessment item x related to system sabotage activities, $n_{\text{data\_attribute}}$ is the number of assessment items related to data sabotage activities, $v_{x,\text{data\_attribute\_member\_i}}$ is the score of assessment item x for member i related to data sabotage activities, and $w_{x,\text{data\_attribute}}$ is the weight of the assessment item x related to data sabotage activities.

The weights are determined by the person in charge, based on the usability of the items and impact of the item on evaluation results. We set the total weight assigned to all assessment items to always be 1.

Based on the behavior of each member, the risk assessments of sabotage activities against systems and data by member i are defined as follows:

$$R_{\text{system\_behavior\_member\_i}} = \frac{1}{n_{\text{system\_behavior}}} \sum_{y} v_{y,\text{system\_operation\_member\_i}} \quad (0 \leq R_{\text{system\_behavior\_member\_i}} \leq 1) \tag{3}$$

$$R_{\text{data\_behavior\_member\_i}} = \frac{1}{n_{\text{data\_behavior}}} \sum_{y} v_{y,\text{data\_operation\_member\_i}} \quad (0 \leq R_{\text{data\_behavior\_member\_i}} \leq 1) \tag{4}$$

where $n_{\text{system\_behavior}}$ is the number of operations related to system sabotage activities, $v_{y,\text{system\_operation\_member\_i}}$ is the score of each operation y by member i related to system sabotage activities, $n_{\text{data\_behavior}}$ is the number of operations related to data sabotage activities, and $v_{y,\text{data\_operation\_member\_i}}$ is the score of each operation y by member i related to data sabotage activities. $v_{y,\text{system\_operation\_member\_i}}$ and $v_{y,\text{data\_operation\_member\_i}}$ are explained in the Subsection *G. Operation Monitoring*.

By integrating assessments based on attributes and behaviors, the risk assessment of sabotage activities against systems and data by member i is defined as follows:

$$R_{\text{system\_member\_i}} = \frac{1}{2}\left(R_{\text{system\_attribute\_member\_i}} + R_{\text{system\_behavior\_member\_i}}\right) \quad (0 \leq R_{\text{system\_member\_i}} \leq 1) \tag{5}$$

$$R_{\text{data\_member\_i}} = \frac{1}{2}\left(R_{\text{data\_attribute\_member\_i}} + R_{\text{data\_behavior\_member\_i}}\right) \quad (0 \leq R_{\text{data\_member\_i}} \leq 1) \tag{6}$$

E. Information Resource Risk Assessment

The information resource risk assessment module evaluates the impact when targeted and destroyed based on asset values and usage as recorded, and sends the assessment results to the insider threat risk assessment module. Information necessary for the assessment is obtained from the information asset register and log records of each server.

Assessment items for information resource risk assessment:

- Information asset value
  Normalize the asset value of each information resource obtained from the information asset register to a value between 0 and 1
- Number of users
  Number of users of each system/data within a certain period (e.g., 1 day, 1 week)
- Use frequency
  Use frequency of each system/data within a certain period (e.g., 1 day, 1 week)

The number of users and the use frequency are normalized from 0 to 1 by dividing each value of the system data by the total number of users and frequency of use within a certain period.

Based on the above assessment items, the risk assessment of information resource j are defined as follows:

$$R_{\text{resource\_j}} = \frac{1}{n_{\text{resource}}} \sum_{z} v_{z,\text{resource\_j}} \cdot w_{z,\text{resource}} \quad (0 \leq R_{\text{resource\_j}} \leq 1) \tag{7}$$

where n_{resource} is the number of assessment items included in the information resource risk assessment, $v_{z,\text{resource\_j}}$ is the score of each assessment item z of information resource j, and $w_{z,\text{resource}}$ is the weight assigned to the assessment item z.

The proposed system sets the weights based on key factors such as the type of information resource and its usage characteristics. The weight settings are adjusted differently for systems and data, with more importance assigned to items that have a greater impact on risk: For systems, the impact of destruction tends to align with the static asset value, as their usage patterns are relatively stable. Therefore, the information asset value is given a higher weight in the risk assessment. For data, the impact can fluctuate depending on timing and usage patterns, making items like the number of users and usage frequency more critical. As a result, these items are assigned higher weights in the assessment. The total weight assigned to all assessment items is always set to 1.

The calculations are based on log records collected over a certain period. If there is a large volume of log records, the computation can be costly. Additionally, since usage patterns are unlikely to change drastically in real-time, we plan to update the calculations outside of business hours. Given the time required for these computations, the information resource risk assessment is updated periodically, such as daily.

F. Insider Threat Risk Assessment

The insider threat risk assessment module performs an insider threat risk assessment based on the scores of the member risk assessment and the information resource risk assessment by the two categories of insider threats. If judged as an potential insider threat, it sends the combination of members, and information resources to the operation monitoring module.

Insider threat risk scores for system and data are defined as follows:

$$R_{\text{system\_insider\_i,j}} = R_{\text{system\_member\_i}} \times R_{\text{resource\_j}} \quad (0 \leq R_{\text{system\_insider\_i,j}} \leq 1) \tag{8}$$

$$R_{\text{data\_insider\_i,j}} = R_{\text{data\_member\_i}} \times R_{\text{resource\_j}} \quad (0 \leq R_{\text{data\_insider\_i,j}} \leq 1) \tag{9}$$

Note that $R_{\text{resource\_j}}$ in $R_{\text{system\_insider\_i,j}}$ refers to the system's information resource risk assessment, while $R_{\text{resource\_j}}$ in $R_{\text{data\_insider\_i,j}}$ refers to the data's information resource risk assessment.

If the insider threat risk score $R_{\text{system\_insider\_i,j}}$ or $R_{\text{data\_insider\_i,j}}$ exceeds the threshold $T_{\text{system\_insider}}$ or $T_{\text{data\_insider}}$, it is considered as an insider threat and becomes a monitoring target. These thresholds are set by the proposed system, based on the number of operations that are detected.

G. Operation Monitoring

The operation monitoring module identifies operations to be monitored based on members, and information resources received from the insider threat assessment module. Specifically, it identifies the operations necessary for the member to achieve the sabotage activity of the threat categories for the information resource in the sabotage activity operation path. The sabotage activity operation path database stores the operation paths required to carry out sabotage activities. It is created based on the company's own cases as well as domestic and international examples, and is organized into two categories of insider threats.

An example of the sabotage activity operation path data for file data is shown in Figure 3. The number of operation steps required to achieve the sabotage activity is indicated by s. Operation $s = 1$, when executed, immediately completes the sabotage activity on the information resource. Operation $s \geq 2$ represents a preparatory operation to affect the target. After this operation is performed, the next operation $s = 1$ completes the sabotage activity. The higher the number in s, the more operation steps are required before the sabotage activity is accomplished.

The operation monitoring module obtains the authorization information of each member from the directory service. From this information, the module identifies the next operation on the path that is necessary to achieve the sabotage activity.

The operation monitoring module identifies the operations $s = 1, 2$ to be monitored and sends target operations to the detection and action module. Therefore, if a high-risk member plans sabotage activities step-by-step starting from step 3 or higher, the proposed system can prevent the sabotage activities

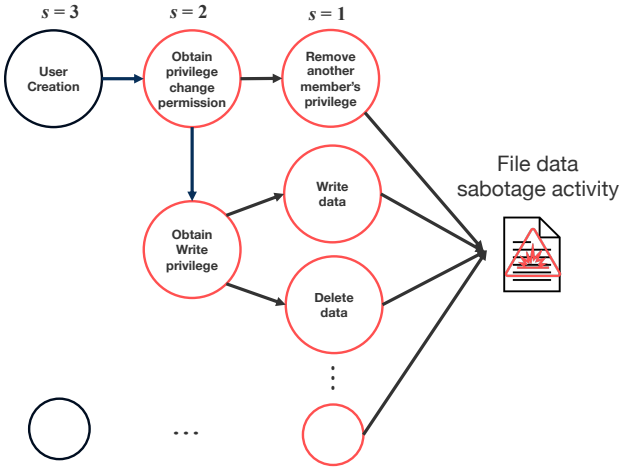

Figure 3. Example of Operation Path for Achieving Objectives.

at $s = 2$. On the other hand, if a high-risk member suddenly executes $s = 1$ operations to carry out sabotage activities, the system quickly rolls back the completed operations to minimize the damage. The contaminated data by operations that cannot be rolled back, such as deletion, tampering, and encryption, is replaced using backup data.

Various paths can be considered, and there may be unexpected paths on the sabotage activity operation path. Therefore, the proposed system cannot predict and monitor all possible paths. If a high-risk member reaches $s = 2$ despite having taken countermeasures on possible paths beforehand, it is necessary to identify the path taken up to that point and reflect that path in the sabotage activity operation path database. Additionally, it is necessary to infer paths that lead to $s = 1$ from that point and take measures, such as containing the impact of the attack.

Operations with $s \geq 3$ are used for member risk assessment as part of their behavioral information. When an operation that suggests advancing sabotage activities is performed, it affects the member's risk assessment. This allows for dynamic risk assessment of the members. The assessment of the operation on system and data by member i is defined as follows:

$$v_{y,\text{system\_operation\_member\_i}} = \frac{1}{2}\left(\frac{1}{s} \times D\right) \quad (0 \leq v_{y,\text{system\_operation\_member\_i}} \leq 1) \tag{10}$$

$$v_{y,\text{data\_operation\_member\_i}} = \frac{1}{2}\left(\frac{1}{s} \times D\right) \quad (0 \leq v_{y,\text{data\_operation\_member\_i}} \leq 1) \tag{11}$$

where s is the number of steps to achieve sabotage activity and D is the number of connected operations. Operations with many connected operations can significantly increase the number of possible achievement paths, thus increasing risk. These activities can be seen as actions leading to potential sabotage.

D is normalized to a value between 0 and 1 by dividing the number of links from the operation at step $s = n$ to the next

step $s = n - 1$ by the total number of such links connecting from all operations at step $s = n$. For the operation "obtain write privilege" in Figure 3, since theare are 2 links from $s = 2$ to $s = 1$, and and the total number of such links is 3, the value is $2/3$.

IV. Challenges in realizing implementation

National laws and organizational attitudes toward privacy and ethics vary, making it difficult to address all assessment items in this paper. In Japan, the Act of Protection of Personal Information (APPI) requires consent from members for the use of their personal information. Similarly, in Europe, the General Data Protection Regulation (GDPR) mandates strict data protection and privacy, while in the United States, laws like the California Consumer Privacy Act (CCPA) provide consumer privacy rights. Employee information is included in these regulations. On the other hand, some countries have security clearance to evaluate the eligibility of individuals who access security-related information. Considering the significant impact and actual damage by insider threats can cause, the need for systems to evaluate eligibility based on various information held by organizations is increasing. The need to explore criteria and methods that enable the effective use of information about members while balancing security and privacy is also crucial.

It is essential to detect the early signs of an attack, but insider threats may hide their activities. The system aims to prevent step-by-step sabotage activities, even if malicious actions are concealed. However, since some activities may evade detection, countermeasures are also needed for when sabotage activities are successfully executed.

The proposed system would replace contaminated data with backup data. However, replacing only part of the data may cause inconsistency issues with other data. This could potentially affect the overall system operation and data reliability. Additionally, if the extent of the contaminated data is unclear, it can be challenging to implement appropriate replacement procedures. This uncertainty complicates the process of ensuring data integrity. Therefore, further consideration is needed regarding the scope and methods of data replacement.

Due to the page limitation, the formulas used for assessment were written without in-depth analysis. They need to be defined more precisely when implementing our method.

V. Conclusion and Future Work

In this paper, we propose a countermeasure against insider threat regarding the psychological state of organizational members and the business impact of information resources. The method consists of the member risk assessment, the information resource risk assessment, and the insider threat risk assessment. If a high-risk member operates information resources, we detect the operations and take countermeasures.

Personality traits are innate and cannot be changed. However, other assessment items, such as emotions and human resources, are changeable, and organizations can actively intervene in these areas. For example, through EAP, organizations can address individual issues like dissatisfaction and reduce the risk of insider threats.

Due to varying legal, ethical, and privacy issues in different countries, not all assessment items can be used. Future research should investigate how reducing the number of assessment items affects the accuracy of risk assessment. Additionally, the formulas used for assessment also need clear explanation. The proposed system would replace contaminated data with backup data. However, replacing only parts of the data may cause inconsistency issues. If the extent of contamination is unclear, implementing appropriate replacement procedures is challenging. Therefore, further consideration is needed regarding the scope and methods of data replacement.

References

[1] Ponemon Institute, "2022 cost of insider threats global report", [retrieved: September, 2024], 2022, [Online]. Available: https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats.

[2] Harris Poll, "Vormetric insider threat report", [retrieved: September, 2024], 2015, [Online]. Available: https://enterprise-encryption.vormetric.com/rs/vormetric/images/CW_GlobalReport_2015_Insider_threat_Vormetric_Single_Pages_010915.pdf.

[3] E. T. Axelrad, P. J. Sticha, O. Brdiczka, and J. Shen, "A bayesian network model for predictiong insider threats", in *Proceeding of the IEEE symposium on Security and Privacy Workshops*, 2013, pp. 82–89.

[4] M. B. Ahmad, A. Akram, M. Asif, and S. Ur-Rehman, "Using genetic algorithm to minimize false alarms in insider threats detection of information misuse in windows environment", *Mathematical Problems in Engineering*, vol. 2014, pp. 1–12, 2014.

[5] D. M. Cappelli *et al.*, "Management and education of the risk of insider threat(merit): Mitigating the risk of sabotage to employers' information, systems, or network", Carnegie Mellon University Software Engineering Institute, Tech. Rep. no. CMU/SEI-2006-TN-041, 2008, CERT Technical Note.

[6] C. Gates *et al.*, "Detecting insider information theft using features from file access logs", in *Proceedings of the 19th European Symposium on Research in Computer Security*, 2014, pp. 383–400.

[7] F. Toffalini, I. Homoliak, A. Harilal, A. Binder, and M. Ochoa, "Detection of masqueraders based on graph partitioning of file system access events", in *Proceedings of the 39th IEEE Symposium on Security and Privacy Workshops*, 2018, pp. 217–227.

[8] F. L. Greitzer and D. A. Frincke, "Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation", *Insider Threats in Cyber Security. Advances in Information Security*, vol. 49, C. W. Probst, J. Hunker, D. Gollmann, and M. Bishop, Eds., pp. 1–12, 2010.

[9] F. L. Greitzer, L. J. Kangas, C. F. Noonan, A. C. Dalton, and R. E. Hohimer, "Identifying at-risk employees: Modeling psychological precursors of potential insider threat", in *Proceeding of the 45th Hawaii International Conference on System Sciences*, 2012, pp. 2392–2401.

[10] M. Kandias, A. Mylonas, N. Virvilis, M. Theoharidou, and D. Gritzalis, "An insider threat prediction model", in *Proceeding of the International conference on Trust, Privacy and Security in Digital Business*, 2010, pp. 26–37.

[11] M. Kandias, K. Galbogini, L. Mitrou, and D. Gritzalis, “Insiders trapped in the mirror reveal themselves in social media”, in *Proceeding of the International conference on Network and System Security*, 2013, pp. 220–235.

[12] M. Kandias, V. Stavrou, N. Bozovic, L. Mitrou, and D. Gritzalis, “Can we trust thie user? Predicting insider’s attitude via youtube usage profiling”, in *Proceeding of the 10th International conference on Ubiquious Intelligence & Computing and Automatic & Trusted Computing*, 2013, pp. 347–354.

[13] P. J. Taylor *et al.*, “Detecting insider threats through language change”, *Law and Human Behavior*, vol. 37, no. 4, pp. 267–275, 2013.

[14] A. P. Moore, D. M. Cappelli, and R. F. Trzeciak, “The “big picture" of insider IT sabotage across US critical insfrastructure”, *Insider Attack and Cyber Security, Advances in Information Security*, vol. 39, S. J. Stolfo *et al.*, Eds., 2008.

[15] A. Cummings, T. Lewellen, D. Mclntire, A. P. Moore, and R. Trzeciak, “Insider threat study: Illicit cyber activity involving fraud in the US financial services sector”, Carnegie Mellon University Software Engineering Institute, Tech. Rep. no. CMU/SEI-2012-SR-004, 2012, CERT Special Report.

[16] I. Homoliak, F. Toffalini, J. Guarnizo, Y. Elovici, and M. Ochoa, “Insight into insiders and IT: A survey of insider threat taxonomoies, analysis, modeling, and countermeasure”, *ACM Computing Surveys*, vol. 52, no. 2, pp. 1–40, 2019.

[17] M. Brown, “A global guide to background checks”, [retrieved: September, 2024], 2015, [Online]. Available: https://www.mayerbrown.com/files/uploads/Documents/PDFs/Employment/A-Global-Guide-Background-Checks.pdf.

[18] T. A. Judge and J. E. Bono, “Five-factor model of personality and transformational leadership”, *Journal of Applied Psychology*, vol. 85, no. 5, pp. 751–765, 2000.

[19] A. K. Kirk and D. F. Brown, “Assistance programs: A review of the management of stress and wellbeing through workplace counselling and consulting”, *Australian Psychologist*, vol. 38, no. 2, pp. 138–143, 2000.

[20] S. G. Kassa, “It asset valuation, risk assessment and control implementation model”, *ISAKA Journal*, vol. 3, 2017.

[21] F. L. Greitzer, “Insider threats: It’s the human, stupid!”, in *Proceeding of the Northwest Cybersecurity Symposium*, 2019, pp. 1–8.