# Paper 77

## Detecting Insider Attack from Behavioral and Organizational Approach

*Sazqi Harashta*

ICMEM

The 7th International Conference on Management in Emerging Markets

*Abstract* - **With alteration in many activities to digital procedures comes vulnerability. Cyber-attack risk keeps increasing for individuals and businesses. One of the attacks that could occur inside companies or organizations is an "Insider Attack". Due to the complexity of human factors, this issue is mainly dealt with and discussed in previous studies through a technical approach. This research aims to find the correlation between the possibility of insider attacks with behavioural and organizational factors. To evaluate the difference in practice between different business sectors in Indonesia. The data were collected through semi-structured interviews with people from diverse work backgrounds conducted online. The interview was recorded and transcribed manually. The data analysis was done using tables to help the coding and correlating variable process. This research is supposed to determine the most impactful factor based on people's views. Possible gaps were found between theories and what happened in the practice of the company or organization. This research outcome intends to give information to future research and serve as a reference to businesses and organizations about current development and gaps in a business environment.**

*Keywords* - **Digitalization Risk, Cyber Security, Cyber attack, Insider Attack, Behavioural and Organizational Factors, Gaps, Prediction, Prevention.**

## I. INTRODUCTION

This research was done to address and answer four questions related to cyber-security. First, the focus will be discussing the interaction between organizations or businesses towards cyber-attack, specifically the "Insider attack". Second, the exchange will consist of prevention and action were taken in facing cyber issues through a socio-technical perspective; as mentioned in a few past research [6, 13-14], the balance between technical and non-technical approaches is needed to achieve the desired result in facing this issue. Third, the approach will focus on the organizational and behavioural aspects as suggested by past research by Geitzer in 2018, where future research in this aspect, especially the relationship between factors, needs to be addressed [14]. Fourth, the improvement of technology is impacting many sectors, especially businesses. It is common for companies to strive for opportunities without proper precautions and adequate security measures [34].

This research aims to put past research theories into Indonesia's work environments. Data safety is crucial in the banking and communication sector [36]. This research will focus on "Insider Attack" prevention and control through a non-technical approach. Several efforts have addressed cybercrime problems across government, industry, and academia [25, 38]. As a result, companies specializing in cyber security are emerging with increasing demand. To know how the organization or company approaches the problem, the interview will discuss the employee or staff's experience with the past issue and the impact the work environment has gone through. With the semi-structural discussion, this research aims to understand the responses and reactions that the interviewees delivered [9]. The semi-structured interview has the advantage of being reasonably objective while still allowing a more detailed knowledge of the respondent's thoughts and reasons than a mailed questionnaire would allow. In-depth opinions are best obtained through a one-on-one interview [7].

Insider threat utilizes privileged access to compromise the confidentiality, integrity, or availability of the organization's information, systems, or infrastructure categorized as malicious insiders [17, 37-38]. The second threat is an unintentional, or non-malicious, insider, who is thought to be the most prevalent [6, 10]. Phishing is a cyber-attack where the suspect uses impersonation methods to gain information or data from the victims. Phishing attacks a company's vulnerabilities in their network, including their employee. Phishing can be caused by an insider attack, whether malicious or non-malicious [17]. Human error is inevitable, and it would take a while to detect an attack, but that does not mean the risk could not be reduced ([17, 25-26, 31].

The technical approach is more commonly used to tackle the cyber issue [2, 4-5]. A socio-technical approach is needed to balance the solution despite solving some parts of the issue. Since 1980 suggested, a socio-technical method based on multi-perspective concepts to aid in evaluating new and existing technologies in the 1980s. Research discussing the socio-technical or behaviour-related approach [3, 13-14, 25] is emerging, and some have come up with frameworks or ontology to set boundaries in their research.

Vulnerability can be caused by the company or organization's negligence; the more data and security breaches occur, the more resources organizations

spend to prevent them. A digital economy is described as economic activities that are based on, rely on, and develop from the use of technology. This caused changes in how businesses operate, for example, transaction process, consumer engagement, and communication with stakeholders. The increase in cyber threats that occurred in 2020-2021 experienced an increase of 6.15% [29]. Despite the increasing number of insider attacks and cyber-attack in Indonesia, there is still limited research that addresses the issue specifically in this country and sectors [18-19].

Because of the risk of invading employee privacy, leaking crucial organizational information, or sacrificing a competitive advantage unintentionally, organizations and teams are hesitant to release this information, making it challenging to gain information regarding actual practice [10]. Nevertheless, the awareness of the importance of this topic seems to have not spread evenly due to different knowledge limits in each country and how policy or law works in that country [29]. Some organizations have reported similar cases, but some might be reluctant to do so since this issue could affect the company's reputation and credibility and shows vulnerability inside the company [10, 16]. Furthermore, most businesses were bureaucratic, with positions defined and organized hierarchically [3]. Therefore, there are gaps in opinion between generations and different Hierarchies inside the organization [13, 15, 25].

As the main country subject in this research, Indonesia shows those gaps. According to CNBC Indonesia, Cyber Attacks caused Indonesian Banks to lose around IDR 246 billion in 2021 ([36]). Insider threats accounted for 58% of reported security incidents [17, 20]. Based on CNN Indonesia, in 2020, Indonesia experienced Phishing attacks on as much as 7.6 % of the population, categorized as moderate [18]. News and articles about cyber-attack in Indonesia keep increasing, yet the knowledge development on this matter did not grow as fast as the issue. Research that explicitly discusses this country is limited, and rather than giving a solution, most of it only aims to review the case [1, 4, 29, 30, 36]. In business matters, employees experience the issue and the effect they need to adapt to while working rather than have a common understanding from the beginning of the work mentioned by [3] relating to training implementation inside an organization.

Researchers are overwhelmed by various possibilities in assessing human behaviour, which is why theoretical frameworks are made to set guidelines and boundaries in analyzing [2, 10, 12, 13, 15, 31]. This research adapts some of the frameworks, some are simplified due to time constraints, and the framework is re-assessed from the interview [9]. Assessing employee behaviour did not fall too far from discussing employee performance [3]. The surest way to determine employee behaviour is through their performance indicator [10]. However, the research that correlates performance appraisal and cyber-attack is limited; most studies discuss this topic separately, While the performance appraisal research focuses on improving employee performance and assessing employee wellbeing [20, 35]. In this research, both topics are related to the issue, that is, insider attacks, which include cyber security and employee behaviour and performance [17, 19, 12].

The framework was constructed for advanced and detailed research that would be too complicated to elaborate on each factor in a limited time. Therefore, only a few factors are going to be discussed. The SOFIT framework is used as a foundation while the factor is adapted to the sample target. In individual factors, motivation, competence, ability, acceptance of roles, resources, and work environment are the factors that will be discussed, while organizational; security practices, communications, management systems, and work planning aspects will be addressed [23]. As a result, researchers and companies will be able to index incidents and better understand prevalent attack vectors based on human behaviour ([31]) [35].

Security awareness for employees can reduce cyber risks by up to 70%. Performance appraisals positively affect employee performance [3, 10]. Integrity affects employee loyalty. Many organizational and behavioural approaches are made [20, 24]. Due to an overemphasis on more immediate reasons, which tend to focus on investigating accidents, mishaps, and other failures, potential organizational contributing elements may go unnoticed. For example, falling for a phishing email could be dismissed as a "human error" and attributed entirely to the user [5, 24, 32, 33]. However, other more systemic concerns, such as insufficient or poor training, overwork, poor team management, corporate regulations, company enforcement of policies, and management systems and practices, could all be at play [23]. In practice, even the most prepared policies and standard operating procedures have human error as their weakness.

# II. METHODOLOGY

## Introduction

The study for this paper will be focused on previous frameworks and conclusions. As a result, this research will be based on secondary and primary data. The use of secondary data is because of the relative speed and low cost. The use of preliminary data will be used in this study as well. It is, however, employed as an addendum or supplementary material for the research to support the leading theory from the material gained from past research. This research data will focus on qualitative methods.

The case study will be used to build the conceptual and theoretical frameworks. Through in-depth interviewing, sympathetic understanding, and suspending or bracketing preconceptions about the topics under discussion, the researcher strives to acquire data on the perceptions of local participants from the inside [21, 27].

One of the essential characteristics of well-gathered qualitative data is that it focuses on naturally occurring, ordinary events in natural contexts, giving us a good sense of what "real life" is like [28]. The goal of the interview is to support available theories and to gain perspective from the direct discussion. Data will be gathered through in-depth interviews. The qualitative technique differs from the quantitative method in that hypotheses are formed through questions and narrative descriptions rather than hypothesis testing in qualitative research [22].

The tools used in the data analysis will be Data Matrix / Conceptually clustered matrix and other programs like Microsoft Word and Excel to organize the textual data gained from the interview. The method used to analyze is the combination between content and narrative analysis. The codes are determined manually according to the research questions and objectives. Identifying similar expressions, correlations between variables, patterns, themes, categories, distinct differences between subgroups, and common sequences by sorting and filtering these coded data [28]. The pattern in a narrative method shown in the result will be used to analyze the gaps and interconnectedness between participants in answering each question. The matrix in the form of a table will help to gain a better overview of the interview and compare responses; this will help monitor any anomaly and consistency inside the response. Conceptually clustered matrices are extremely useful when certain prominent concepts or themes emerge from the initial investigation [27].

## Research Settings and Participant

In this research, the participants will be taken according to their expertise and divided into four categories. Participants come from an educational background or working/were working in that field. The interview is semi-structural; therefore, the interviewees can adapt the question. The questions are formed according to the research objectives. The participant's name will be anonymous to respect the participant's consent. For this research, the participants' names will be coded based on their working field and numbered as in (participant 1, participant 2).

PP = People Performance
OHR = Organizational and Human Resource
CS = Cyber Security
BT = Banking and Telecommunication

| Background Category | Objective | Number of Participant |
|---|---|---|
| People and Performance | aims to understand the ways to approach employees and to support the goal of this research which is to give suggestions for a performance appraisal system | 2 |
| Organizational and Human Resource | The goal is to gain insight for the strategy from organization environment. This research is not only aiming for technical solution but also to build a strategy in behavioural approach. | 2 |
| Cyber Security | The focus of this research is to analyse a cyber security related issue. Therefore, to identify the risk and issue possibilities that might occur for the business and to understand the theoretical and practical experience in the field | 2 |
| Banking and Telecommunication | to interview employee and ex-employee from this field to see whether there are gaps between periods. Hierarchy inside the company also will be used as analysis thus the participant position varies. Interviewing this field also aims to analyse the policy or procedure improvement and awareness inside the field from employee perspective. | 3 |

Fig. 1. Interview participant classification

## Theoritical Framework

Employee motivations for conducting a harmful attack are diverse and complex, making them difficult to assess. We used work-related stress levels to measure motives in our framework. For example, we looked at authorized users' attitudes toward the workplace, employee support from their line manager or coworkers, coworker relationships, and employee understanding of the organization's security policy [11]. Employee age and gender also have an impact on motivation levels. Because individuals are anticipated to realize their intents should an opportunity exist, opportunities determine the possibility of authorized users executing a malicious insider threat [13].

The expertise and ability of an employee to carry out/ enable various types of security breaches are referred to as capability ([14]). Insiders have privileged access to the organization's data assets (perhaps for extended periods), which might provide these authorized users with the capacity to learn about and understand the security mechanisms in place. For example, employee access rights to intellectual property and job knowledge were used to assess capability levels (Elmrabit et al., 2019; Walker et al., 2018).

Another factor discussed was Hierarchy, which in this research will be used to find gaps in the response between the participants. People who live in groups

and organizations, like most of us, and social scientists who study groups and organizations know that your role influences your perspective on life. A role is a complicated mix of expectations and behaviours that define what you should do as a specific type of actor in a given situation. A role-ordered matrix group summarises and contrasts different people's role perceptions on certain themes or concerns, allowing the researcher to compare and contrast them. For example, bosses are generally blind to their employees' frustrations, partly because they are removed from them and because subordinates frequently suppress unpleasant news when reporting upward [27].

## Conceptual Framework

Additional constructs can be added to the currently available ontology, which has caught important constructs from the literature. In this research, more studies on organizational variables that expose a company to heightened insider threat risk would help to specify further the lower-level leaf nodes and instances [19]. When informed by ontology relationships, models that use estimates of threat values for individual indicators can be used to anticipate threats in scenarios involving collections of indicators [10, 13-14, 25, 32].

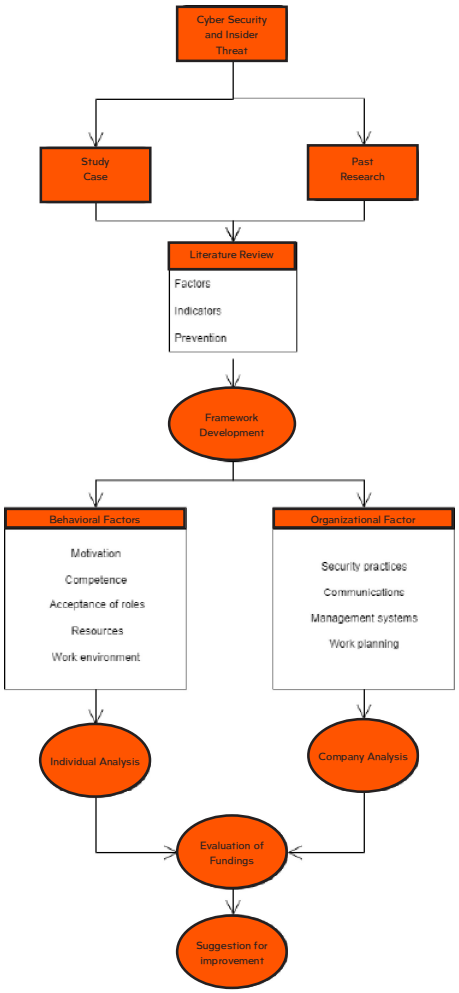


Fig. 2. Conceptual Framework

## Validity and Reliability

The phenomenon can be studied in its natural setting and meaningful, relevant theory generated from the understanding gained through observing actual practice. Although some researcher argues that validity and reliability are needed in qualitative research, in this research, this section will help explain the attempt by the researcher to avoid biases and miss interpretation of the data collected. The reliability can be seen from the consistency in the answer, which will be presented in a graph projected from the researcher's administered questionnaire based on the participant's responses. Furthermore, the question can measure the generability of this research addressed to the interviewer. In the semi-structured interview, the main question asked is the same for all the participants despite the difference in their field of work background. The participant gave an opinion based on their experiences, showing that findings can be applied to another context, setting or group.

# III. RESULTS

## Overview of Finding

Below are the findings of this research which will be elaborated on.

1. There is a correlation between employee well-being and the working environment
2. It is possible to predict possible attacks from the employee performance
3. Employees are aware of possible attack
4. Only half of the participants have experienced cyber security education provided by their workplace
5. The gap of knowledge in cyber security is more prominent when comparing between working fields rather than comparing from working period inside the same industry
6. Country's policy and the firm have an essential role in giving guidance related to working place practice that correlated to the awareness of security
7. Most of the participants experienced or witnessed a cyber attack
8. Some of the cyber attacks the participants experienced or witnessed took place in their workplace
9. Most of the participant agrees that a performance appraisal system help improve employee spirit and well-being whilst monitoring the possible attack

10. Hierarchy affected how the employee express their concern and discomfort [16]

Sometimes experiences were not obtained due to rejection of learning; one of them can be described as a silo mentality where there is reluctance in sharing and gaining information within a company [8]. Every participant is familiar with the term "Cyber-attack". They gained knowledge regarding cyber security from outside and inside their workplace but mainly express learning this topic outside of the work environment.

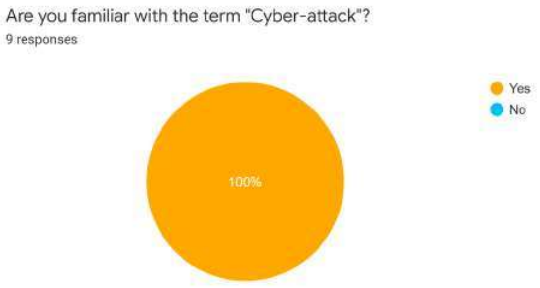


Fig. 3. Cyber security awareness pie chart result

Despite the awareness the length of knowledge and familiarity for cyber security context seems to vary. The awareness is affected by the working field and the company main operation [32].

## Code: Cyber Security Awareness

**Participant: OHR 1**

> *Yes, I am aware that the company is at risk of cyberattack, especially since the company also revolve around technologies and software. The company itself haven't really executed any training and given the employee much knowledge about it.*

**Participant: PP 1**

> *Yes, the risk is high especially with digitalization keeps developing at such a fast tempo and the company are also operates with digital software.*

According to samples in this research, we can conclude that the issue is not the lack of awareness in the country [29] but the extent of people's knowledge about cyber security, mainly affected by their field of work.For example, participants that work in the banking and cyber security field have more experience and knowledge regarding the systems implemented for the company to ensure cyber security. This is shown by the amount of system implementation in the company.

## Code: Cyber Security Experience and Knowledge

**Participant: BT 2**

> *Important document like collateral document are protected by separate department called the custody department. There is a vault to store the documents. When a department or and employee need to use or borrow some documents there are some safety measure that needed to be oblige to, for example it is mandatory to have a permission letter and to register. Which even with that much rules there are still some cases where the documents is lost. Sometimes it was caused by "unmatched" document registration. Human error in operational risk will always present.*

The participant from the banking sector can give a detailed description of the rules implemented and provide examples of possible issues and cases. While the participant in the other field showed knowledge that was informed formally by the company only, not all aspects related to their work.

**Participant: OHR 2**

> *Yes, during our internship, we were given a link tree, which contained a booklet that contained information about the company, facilities, do's and don'ts for interns, floor plans, and company rules. There is also a COVID 19 SOPEmployees are encouraged to study and know the structure and rules of the company. Yes there are restrictions for the use of zoom, whatsapp. Right now I haven't taken care of the external part so I only know about the internal system.*

This is not to compare which field of work is better, rather this compparison can show the priority of companies. This can also visualised where the cyber security topic stay in the company priorities.

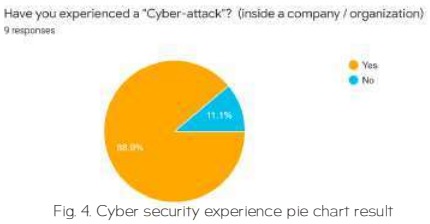


Fig. 4. Cyber security experience pie chart result

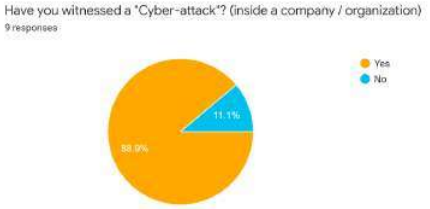


Fig. 5. Cyber security experience pie chart result 2

Only the minority of the participant that have not experience a cyber-attack. And one of that participant responds with the possibility of the issue might happened but the participant have not heard about it.

## Code: Cyber Security Experience and Knowledge

**Participant: OHR 2**

> *I haven't heard any case related to this but maybe it happened before. If it's a case that not related to cyber, I have heard a few cases. It does harm the company but rather than directly about the cyber attack it's more to a case that could have been detected if the cyber system in the company is already implemented correctly. For example procurement of goods manipulation, if only our cyber system was used accordingly this case should have been detected sooner.*

With this we can conclude that majority of participant as an individual or an employee have experienced a cyber attack [3, 13, 18]. From past research it is shown that majorit of people have experienced or witnessed cyber attack but people are still unfamiliar with the term or have limited knowledge about the issue.

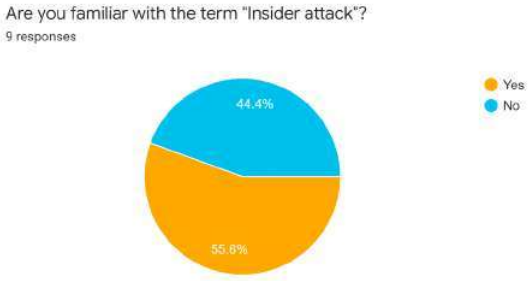


Fig. 6. Cyber security familiatiry pie chart result

While for the term "Insider Attack". Participant shown more unfamiliarity with the term. After a brief explaining some participant turns out to be familiar with the topic but not with the term [14]. This will be evident in the graph below where most of participant have experience the attack and all of the paricipant have witnessed the attack inside their company.

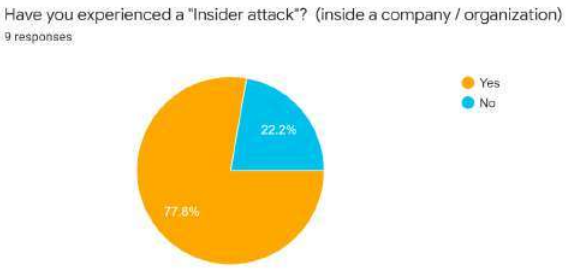


Fig. 7. Insider attack experience pie chart result

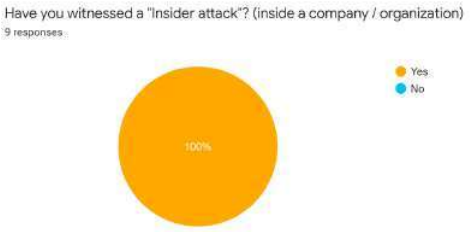


Fig. 8. Insider attack experience pie chart result 2

All participant have experience insider attack. Despite the experienced some some also convey their lack of knowledge about the topics. Some participant convey their concern regarding the lack of thoughts their company put in the matter [35].

## Code: Cyber Security Risk Awareness

**Participant: OHR 2**

> *Yes, the risk is high especially with digitalization keeps developing at such a fast tempo and the company are also operates with digital software. Unfortunately, the company I'm working at still haven't put a lot of thought into the issue. The company's focus just has not yet reached that to that point but slowly the company seems to try to dig more into this topic.*

Some participant elaborate their experience during the attack and how was the issue impacting the working environment.

**Participant: CS 1**

> *Obviously accidental ones do happen. And I and I when I worked for a holiday park, I worked with a lady who accidentally sent. The medical record, medical, financial and personal details of nine employees to a custom. There was a lot that was going on, like salary information, bank account details, any issues they'd had with in met with their medical history. And she just she just left. It's really hard position for them because that's a major GDPR violation. And it was a total accident.*

In this case the participant witnessed a non-malicious attack. We can see that the impact is significant for the company and the woman in the story despite the issue occur unintentionally.

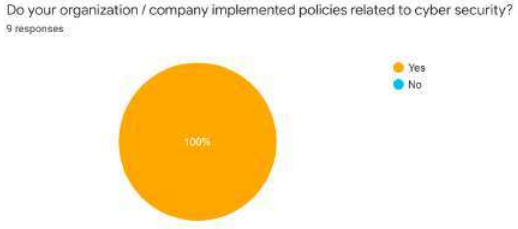


Fig. 9. Cyber security in organization pie chart result

All the participant respond is positive, the company they are working and worked for implemented policies and procedures related to the cyber security [18, 35]. Whether it is for prevention or countermeasures when the issue takes place. The rules vary on the field of work [34]. The more important data security the more detailed and rigid the policies are [36]. For example, one of the participant from the banking field convey the reason they resigned was because of the overwhelming amount of rules that implemented in the company. But they show their understanding and supported the policies.

> *But the official policies and rules inside banking industry are already detailed and rigid, which actually became one of the reasons people might be quitting. That includes me, i understand the importance and realy appreciate it but for me personally after working in this sector for quite sometimes it was tiring and mentaly weighing.*

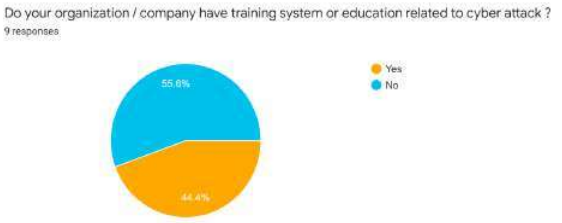


Fig. 10. Cyber security in organization pie chart result 2

Most participant have no experience training relating to cyber security in their working place. Some participant said that the company is using 3rd party like hiring people outside of the company to deal with the issue.

**Participant: CS 2**

> *Yes, and don't do training, but just hire a professional (example: build a firewall)*

Some participant said that training is not their company's main concern. Thus, the company just implement policies and rules. Training might take time and cost some mony whis is why some company opine that training is not part of their priority but some company put training as one of their future planning [14, 20, 35]

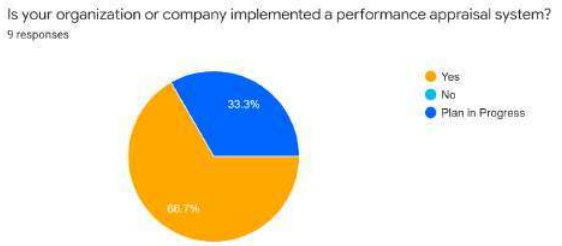


Fig. 11. Performance appraisal in organization pie chart result

Some participant workplaces implemented a performance appraisal system, which according to the participant the system affects the working performance inside the company [3, 10]. The main feature was mentioned by several participants in the KPI and the report delivered to the employee. The KPI is believed to be an essential tool for an objective indicator of employee performance. The KPI help the company monitor the operation targets. The report, which is usually delivered in a descriptive manner accompanied by average scoring, allows the employee to understand their strengths and weaknesses, which can be a significant introspection for the future. Participant conveys feelings of appreciation for the report, which increases motivation.

**Participant: PP 1**

> *Yes, there are some performance appraisal strategies in preparation. With this new system, hopefully, the contribution of each employee can be appreciated. The physical, spirit, and thoughts of each employee should be appreciated. With this, we also hope that we can monitor what is it that the employees are lacking and provide support for that. Employees that didn't perform well hopefully can be seen and be given a warning in the future.*

Although some participant convey that the company they have been working in did not implemented a performance appraisal system. Is not that the company do not have the system, it just the system is still on planning process and have not yet been implemented. The main caused to this issue is the company current focus to the project which caused a delay in developing the system and the company workload. Some participant convey their concern for this delay.

## Code: Behavioural Factors

**Participant: BT 3**

> *The first motivation, competence, work environment is very influential on motivation, ability, acceptance of roles, resources. If motivation is needed to work, competence must be possessed, when accepted in a company it means that we are considered to have the competence to work there. The work environment must be fun or comfortable to support work performance. Ability can be honed during work.*

**Participant: PP 2**

> *Competence is needed to do a task, without competence the result of the job might be not accordingly and not reach the satisfaction standart The environment is important, the*

*environment can improve motivation. If the environment is supportive, not giving too much pressure i think the motivation for the members to work well might be improve. Resource is impotant but without motivation resource might be useless. Role accepting is the least because i think that a person can have multiple skill that can help them adapt in many roles.*

Motivation and work environment have been the most discussed factors. The participant convey the importance of motivation accompanied by competence as individual factors to the performance. Competence is important to maintain the motivation, it is needed for the employee to be able to do their work to enjoy their work [3]. Without competence the employee could experience pressure and lacking in their performance. The environment is also related to the motivation, participants opine that with supportive work environment the motivation will increase and the performance will also increased [14, 16-17].

### Code: Organizational Factors

**Participant: BT 3**

*Good work planning and in accordance with the vision and mission of the people in the company (not just according to the leader) is very important. A management system is needed to set goals and to provide a foundation for the system. The way to support all of that is through communication, because that's why there is PR in a company. Not only by PR communications within the company must be carried out by each other to distribute information. The first security practice, employees must have knowledge of their own company to be able to work properly and according to the rules.*

**Participant: PP 2**

*Security practice, management system, work planning, communication. Communication is not the main issue in my case since everyone have their own job and platform, each of us doesn't really relate to each other task which means that communication was not that necessary for the working process. Security practice, it is the most importan because i think we do need the knowledge and awareness for the whole member because with that lacking it will caused vulnerability.*

The response for the organizational factors varies but participant shows agreement in the importance of all factor especially in work planning [2]. BT 1 is still working in this field currently and holding a higher up position. They shown a higher satisfaction towards the system. Whilst talking about the issue they convey the concern as minimum as possible. BT 2 was working in the same field and similar hierarchy but since this respondent is not bound to their work anymore they manage to convey more about the concern and the issue inside the company. The satisfaction in the working and the system is also lower.

### Code: Current System Satisfaction

**Participant: CS 2**

*So far, I feel that the regulations are in accordance with what is needed. Regulations already maintain systems and operations within the bank. In my opinion, regulations that regulate internal banks or external banks have facilitated the needs of banks. The existing rules already provide sufficient protection.*

**Participant: OHR 1**

*I think it would be nice to have a PA system. Maybe with this, every employee could prove their effort and the judgement will be accordingly rather than judgement and rewards based on "closeness" or how people present themselves to the higher-ups. With PA I think we could minimize the risk of freeloaders. With PA each individual will also have their own KPI so we can monitor each employees' workload.*

## IV. DISCUSSION

### Research questions answered

This research consists of 4 Research Question which developed to be the objective foundation of this research.

1. How can organizations detect cyber insider attacks?
2. How can cyber-attacks be prevented, what action can be taken by the organization?
3. What challenges do organizations face in detecting and preventing cyber-attacks?
4. What recommendations could be made to assist organizations regarding cyber-attacks going forward?

This section will use the findings from the analysis to answer the research questions. The answers to the first and second research questions will be related to one another. From the analysis and findings of this research, detection can be done by monitoring employee behaviour and performance in the company. The team leader or

teammates can watch each other through the project process. The interview participant opines that it is good to have peer evaluation at the end of each project. Other than appreciating the finished work, the member lacking in their target or performance can be evaluated and recommended for future projects. With the evaluation, the company will be more aware of what knowledge is needed for the future. The past report makes it easier to deal with and predict the attack. Experience can help the action taken faster [26, 31].

For Malicious attacks, performance appraisal or peer review can help the team to be more aware of the relationship between teammates and the working condition. Employees can have some issues with one another or maybe with the higher-ups, and this can leads to possible attack; for example, one of the interviewees said that one of her colleagues that has an issue with the other team conveyed her discomfort with person A and in the end, some arguments involved unnecessary department because of assumption. This resulted in the leak of the organization's internal issues and working process, which led to the department's image being scarred. Technical approaches can be used to protect the data and the system; some approaches are mentioned in [2, 4-5]. In this research, the direct approach analyzed is the behaviour approach. There are some methods in the past research that are already studied and can be developed to adapt to the company. From this research analysis, the approach suggested is leaning toward detecting employee behaviour as an individual that interacts with the environment.

The third question regarding the challenges is that an organization might face implementing a system that is aware of cyber security. The interview shown that most companies, especially those unrelated to cyber security, put their priorities on their project. This can cause negligence in the building of the prevention system. Some companies tackle this issue by using 3rd party firms, which can take less time and focus but might cause more caused. Participants also conveys their discomfort with too many policies, while the other participant counterfeits with that comment. The ability of each employee to accept the policies might vary this will takes time to adjust. Policies must be formed according to the company's needs [2, 35]. The company should give time to the employee to adjust to the system yet still set a limit for the adjustment to prevent a prolonged process that can cause vulnerabilities [28]. The other challenge is the need for the company to follow the improvement of technology since it might affect the competitive advantage.

Last will be what recommendations could be made to assist organizations regarding cyber attacks going forward?

- Company can give more awareness for the employee about cyber-security through training.
- Develop a performance appraisal system to improve the employee performance and support their well-being
- Do not underestimate the attack scope, avoid developing a system after the issue happened
- Provide prevention and countermeasure that are suitable for the company instead of following the trends

# V. CONCLUSION

## Reflection

Knowledge, skill, and passion are essential to support research. However, the research process is also the time to learn and develop. At the beginning of composing this research, the researcher had some basic knowledge related to the topic; most of it was gained from the other module taken in the past or courses are taken based on interest. This basic knowledge then turns into good, which drove the researcher to do this research. Not only gaining new skills, but the process also broadens the researcher's network and public speaking confidence. The use of NVIVO in this research is not direct, but it helps with coding for the interview result.

Time management skills are needed with time constraints and other projects in progress. From the beginning until half of the process, the author experienced difficulties in ensuring that the research progress proceeded according to schedule. The schedule was organized in the timetable with the target set from the beginning, but in practice, challenges arose, whether technical, health, or wellbeing. With the amount of past research that needed to be reviewed, the time it took exceeded the estimated time. For this matter, the researcher learned that limiting the amount of research is probably required. This issue is also solved by using a literature review matrix which helps compare and review faster and tidier.

Reconnecting with people and being more confident in engaging in a conversation is also benefits the researcher gained. Moreover, doing in-depth interview help the researcher to understand and sympathize more. Since this research is related to the behavioural aspect, the researcher, who had a limited knowledge and experience in the psychological field, managed to gain more in this topic and develop an interest in this matter [14, 15]. Therefore, the researcher feels grateful for the experience

gained from this research despite the challenges that the researcher has to face in the process.

### Limitation and Managerial Implication

However, there are a few drawbacks that should be considered. Because qualitative data was created for a different purpose and audience, it's sometimes difficult to address research questions directly. The use of semi-structured interview help the researcher to gain a more prosperous point of few; however, this method of narrowing the interpretation, relating it to the topic and comparing the answer to other participant takes more time [7]. With limited time, the sample that could be interviewed was also limited. Conclusion and findings are easier to find since the sample is narrow, but it would be nice to have more samples for a richer result The method used is suitable for this research since this research aims to understand the behavioural aspect in depth rather than quantity [20]. The findings in this research are meant to give the owners and researchers possible topics and issue to discuss based on information gained directly from direct interaction with employees that can be addressed for future use [6]. The findings meant not to contradict or challenged textual theory, rather to find gaps between those theories and the practice [17, 21, 28].

Although, it is possible to gain information from a quantitative approach where a questionnaire can be used to gain common opinion. During the interview, data collected can be limited, and some questions might not be answered accordingly; respondents may not feel they could openly discuss their experiences [7, 16]. Some respondents believed they lacked the competence to make valuable solutions to the questions posed. With the simplified framework in this research to save time, the researcher would recommend for future research analyze broader scope [12]. The sample could also be added and taken from a more specific field. The sample can be arranged based on the hierarchy when the participants are enough. If possible, the interview can be accompanied by field observation since the pandemic is decreasing. The analysis can be improved by using a more detailed questionnaire that is interview-based

## ACKNOWLEDGMENT

The author like to deliver special appreciation to the interview participants and the University of Hull, who have greatly facilitated and assisted this research. In addition, the author would like to thank families, friends, and the supervisor of this research Dr Bridget Freer, for their support and guidance whilst writing this dissertation.

The author would also like to thank the ICMEM 2022 for the opportunity to present and share the ideas and findings of this research.

## REFERENCES

1. Asauri, Z.A.F., 2022. Pengungkapan Cyber Risk: Efeknya Terhadap Profitabilitas Perbankan Di Indonesia (Doctoral dissertation, STIE Indonesia Banking School).

2. Asgari, R. and Atani, R., 2013. A Framework to Defense Against Insider Attacks on Information Sources. SSRN Electronic Journal,.

3. Alkalha, Z., Al-Zu'bi, Z., Al-Dmour, H., Alshurideh, M. and Masa'deh, R., 2012. Investigating the effects of human resource policies on organizational performance: An empirical study on commercial banks operating in Jordan. European Journal of Economics, Finance and Administrative Sciences, 51(1), pp.44-64.

4. Arofah, N.R. and Priatnasari, Y., 2020. Internet Banking Dan Cyber Crime: Sebuah Studi Kasus Di Perbankan Nasional. Jurnal Pendidikan Akuntansi Indonesia, 18(2), pp.107-119. Bada, M. and Nurse, J.R., 2021. Profiling the Cybercriminal: A Systematic Review of Research. arXiv preprint arXiv:2105.02930.

5. Banday, M.T. and Qadri, J.A., 2011. Phishing-A growing threat to e-commerce. arXiv preprint arXiv:1112.5732.

6. Cappelli, D.M., Moore, A.P. and Trzeciak, R.F., 2012. The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud). Addison-Wesley.

7. Carruthers, J., 1990. A Rationale for the Use of Semistructured Interviews. Journal of Educational Administration.

8. Cilliers, F. and Greyvenstein, H., 2012. The impact of silo mentality on team identity: An organisational case study. SA Journal of Industrial Psychology, 38(2), pp.1-9.

9. Codó, E., 2008. Interviews and questionnaires. The Blackwell guide to research methods in bilingualism and multilingualism, pp.158-176. [10] J. P. Wilkinson, "Nonlinear resonant circuit devices (Patent style)," U.S. Patent 3 624 12, July 16, 1990.

10. Costa, D.L., Collins, M.L., Perl, S.J., Albrethsen, M.J., Silowash, G.J. and Spooner, D.L., 2014. An ontology for insider threat indicators development and applications. CARNEGIEMELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

11. Dunn Cavelty, M. and Wenger, A., 2020. Cyber

security meets security politics: Complex technology, fragmented politics, and networked science. Contemporary Security Policy, 41(1), pp.5-32.

12. Ebneyamini, S. and Sadeghi Moghadam, M.R., 2018. Toward developing a framework for conducting case study research. International journal of qualitative methods, 17(1), p.1609406918817954.

13. Elmrabit, N., Yang, S.H. and Yang, L., 2015, September. Insider threats in information security categories and approaches. In 2015 21st International Conference on Automation and Computing (ICAC) (pp. 1-6). IEEE.

14. Greitzer, F., Purl, J., Leong, Y.M. and Becker, D.S., 2018, May. Sofit: Sociotechnical and organizational factors for insider threat. In 2018 IEEE Security and Privacy Workshops (SPW) (pp. 197-206). IEEE.

15. Greitzer, F., Lee, J., Purl, J. and Zaidi, A., 2019. Design and Implementation of a Comprehensive Insider Threat Ontology. Procedia Computer Science, 153, pp.361-369

16. Gul, R., 2014. The relationship between reputation, customer satisfaction, trust, and loyalty. Journal of Public Administration and Governance, 4(3), pp.368-387.

17. Hashem, Y., Takabi, H., GhasemiGol, M. and Dantu, R., 2016. Inside the Mind of the Insider: Towards Insider Threat Detection Using Psychophysiological Signals. J. Internet Serv. Inf. Secur., 6(1), pp.20-36.

18. Ikhsan, M., 2020. BSSN Sebut Keamanan Siber RI 2020 Naik, Serangan Meningkat. [online] CNN Indonesia. Available at: [Accessed 5 May 2022].

19. Keeney, M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T. and Rogers, S., 2005. Insider threat study: Computer system sabotage in critical infrastructure sectors. National Threat Assessment Ctr Washington Dc.

20. Khan, N., J. Houghton, R. and Sharples, S., 2021. Understanding factors that influence unintentional insider threat: a framework to counteract unintentional risks. Cognition, Technology & Work.

21. Kitchenham, B., Pickard, L. & Pfleeger, S.L. 1995, "Case studies for method and tool evaluation", IEEE Software, vol. 12, no. 4, pp. 52-62.

22. Lareau, A., 2012. Using the terms" hypothesis" and" variable" for qualitative work: A critical reflection. Journal of Marriage and Family, 74(4), pp.671-677

23. Limba, T., Plėta, T., Agafonov, K. and Damkus, M., 2017. Cyber security management model for critical infrastructure. Entrepreneurship and Sustainability Issues, 4(4), pp.559-573.

24. Maasberg, Michele & Warren, John & Beebe, Nicole. (2015). The Dark Side of the Insider: Detecting the Insider Threat Through Examination of Dark Triad Personality Traits. 2015. 10.1109/HICSS.2015.423.

25. Nurse, J.R., Buckley, O., Legg, P.A., Goldsmith, M., Creese, S., Wright, G.R. and Whitty, M., 2014, May. Understanding insider threat: A framework for characterising attacks. In 2014 IEEE Security and Privacy Workshops (pp. 214-228). IEEE.

26. Magklaras, G.B. and Furnell, S.M., 2001. Insider threat prediction tool: Evaluating the probability of IT misuse. Computers & security, 21(1), pp.62-73.

27. Miles, M.B., Huberman, A.M. and Saldaña, J., 2018. Qualitative data analysis: A methods sourcebook. Sage publications.

28. Oplatka, I., 2018. Understanding Emotion in Educational and Service Organizations through Semi-Structured Interviews: Some Conceptual and Practical Insights. Qualitative Report, 23(6).

29. Parulian, S., Pratiwi, D.A. and Yustina, M.C., Studi Tentang Ancaman dan Solusi Serangan Siber di Indonesia. Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT), 1(2), pp.85-92

30. Rahmawati, C., 2020, November. Tantangan Dan Ancaman Keamanan Siber Indonesia Di Era Revolusi Industri 4.0. In Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO) (Vol. 2, pp. 299-306).

31. Schultz, E., 2002. A framework for understanding and predicting insider attacks. Computers & Security, 21(6), pp.526-531

32. Sikos, L.F., 2019. OWL ontologies in cybersecurity: conceptual modeling of cyberknowledge. In AI in Cybersecurity (pp. 1-17). Springer, Cham

33. Shaw, E.D. and Fischer, L.F., 2005. Ten tales of betrayal: The threat to corporate infrastructure by information technology insiders analysis and observations. DEFENSE PERSONNEL SECURITY RESEARCH CENTER MONTEREY CA.

34. Sundaram, A. and Radha, P., 2019. Social media security and privacy protection concerning youths.'How to

be safe, secure and social'. International Journal of Business Innovation and Research, 18(4), pp.453-471.

35. Wall, D., 2012. Enemies within: Redefining the insider threat in organizational security policy. Security Journal, 26(2), pp.107-124.

36. Wareza, M., 2021. Ini Serius! Serangan Siber Bikin Bank-bank RI Rugi Rp 246 M. [online] CNBC Indonesia. Available at: [Accessed 5 May 2022].

37. Whitehouse.gov. 2011. Executive Order 13587 -- Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information. [online] Available at: [Accessed 23 November 2021].

38. Wood, B., 2000. An insider threat model for adversary simulation. SRI International, Research on Mitigating the Insider Threat to Information Systems, 2, pp.1-3