Asian Journal of Social and Humanities
https://ajosh.org/

Analysis of Knowledge Management Strategies for Handling Cyber Attacks with the Computer Security Incident Response Team (CSIRT) in the Indonesian Aviation Sector

Lingga Dwiaji[1*], Agung Mulyo Widodo[2], Gerry Firmansyah[3], Budi Tjahyono[4]
Universitas Esa Unggul, Indonesia
E-mail: Lingga.dwiaji@gmail.com

*Correspondence: Lingga.dwiaji@gmail.com

KEYWORDS
Knowledge Management, Cyber Attack, CSIRT.

ABSTRACT

Cyber attacks are a genuine threat that has emerged due to the evolution of a more dynamic and complex global strategic environment. In Indonesia, several cyber attacks target various government infrastructure sectors. The National Cyber and Crypto Agency (BSSN) predicts Indonesia will face approximately 370.02 million cyber attacks in 2022. The majority of cyber attacks target the government administration sector. The National Cyber and Crypto Agency (BSSN) officially formed a Computer Security Incident Response Team (CSIRT) to tackle the rampant cybercrime cases. CSIRT is an organisation or team that provides services and support to prevent, handle, and respond to computer security incidents. The current CSIRT does not have a data storage process and forensic preparation. CSIRT will repeat the procedure, and so on. This is a repeating procedure; the attack will occur once, and only a technical problem will arise. Therefore, the research entitled "Analysis of Knowledge Management Strategies for Handling Cyber Attacks with the Computer Security Incident Response Team (CSIRT)" is expected to implement this Knowledge Management Strategy to manage existing knowledge so that it can make it easier for the CSIRT team to handle cyber attacks that occur.

Introduction

The rapid development of technology today has resulted in the high development of cybercrime (Sari, 2018). The National Cyber and Crypto Agency (BSSN) noted that Indonesia experienced 370.02 million cyber attacks in 2022 (Firmansyah & Yuswanto, 2022). This figure climbed by 38.72% over the previous year when 266.74 million cyber attacks were documented in the country since the second quarter (July-December). In 2023, there will be an average of 3.727 million daily attacks. BSSN identified five areas frequently associated with cyber security incidents: government, health, banking, information and communications technology, and transportation (Mahendra & Pinatih, 2023).

To tackle the increasing number of cybercrime cases occurring, by Presidential Regulation Number 18 of 2020 concerning RPJMN 2020-2024, the National Cyber and Crypto Agency (BSSN) officially formed a Computer Security Incident Response Team (CSIRT). CSIRT is an organisation or team that provides specialised services and support to prevent, address, and respond to computer security incidents (Islami, 2018). BSSN directs each industrial sector to have its own CSIRT and coordinate with BSSN regarding cyber attack information so that it can detect it as quickly as possible and prevent further incidents from occurring, one of which is in the aviation transportation sector (Kristiyono, 2015).

According to (Alfikri & Ahmad, 2022), Implementation of the Policy for Establishing a Cyber Incident Response Team to Support Information Security in the Government Sector shows that although the target for establishing CSIRT in the government sector in 2024 has reached 52%, the target for establishing CSIRT in the government sector in 2024 has reached 52%. CSIRT in the government sector in 2024 will reach 52%. Implementing BSSN Regulation No.10 of 2020 is still not optimal regarding policy content and implementation context. The main obstacle was a lack of information security awareness; CSIRT in this sector still had problems, including a lack of understanding of handling and testing defence and storing and preparing data. When the attack reappeared, CSIRT did not have summary data on cyber attack procedures, whether this attack had occurred before, or how to handle each attack (Solehudin et al., 2023). Therefore, procedures for handling cyber attacks became ineffective. To drive better platform security performance in the future, organisations need to manage knowledge regarding reporting and handling cyber incidents that have occurred (Kaburuan, 2022).

So that this repetitive procedure does not continue to occur, Knowledge Management (KM) is needed to manage knowledge related to cyber-attacks and defence. All attacks are then carried out with good handling preparations so that repeated incidents do not occur (HUTAURUK, 2023). Therefore, in the research entitled Analysis of Knowledge Management Strategies for Handling Cyber Attacks with the Computer Security Incident Response Team (CSIRT) in the Indonesian Aviation Sector. It is envisaged that deploying this knowledge management system will enable the management of existing knowledge, allowing the CSIRT team to handle cyber threats in the transportation industry more efficiently, especially air transportation.

Table 1
Previous Study

Nama Penulis	Research Title	Research Result
Mariami Gonashvili (2019).	Knowledge management for incident response teams	Analysing the application of KM in assisting the incident response team at Masaryk University, Czechia

Mooi, R. D., & Botha, R. A. (2016)	A Management Model for Building a Computer Security Incident Response Capability	Development of the KM CSIRT model to form a Computer Security Incident Response Team (CSIRT) with the ITIL framework
Fauziyah Fauziyah1, Zhaosun Wang1, Gabriel Joy2 (2022)	Knowledge Management Strategy for Handling Cyber Attacks in E-Commerce with Computer Security Incident Response Team (CSIRT) ISSN Online: 2153-1242	analysing the implementation of Knowledge Management strategies in helping handle cyber attacks carried out by the CSIRT E-Commerce team
Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, Repchick, K. M., Tetrick, L. E. (2015)	Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research	Research on Improving the Effectiveness of Cyber Incident Response Teams Using Team-Based Research
Muhammad Haidar; Yudho Giri Sucahyo; Teddy Sukardi; Arfive Gandhi (2021)	Analysis of Csirt Services in Facing Cyber Security Challenges in Indonesia	Analyse how CSIRT Services handles cybersecurity
Fernandes, (Fernandes et al., 2021), Adaíl, Santos, Leonel; Rabadã, Carlos. European Conference on Cyber Warfare and Security (2021)	A Strategy for Implementing an Incident Response Plan	Discusses the challenges of implementing the CSIRT team's strategic plan in handling cyber incidents
Orissa Octaria, Dr. Ermatita, M. Kom (2017)	Analisis Knowledge Management System dengan Metode Inukshuk	Implementation of Knowledge Management using the Inshulk Model Framework

Prabaswari, Muhamad (Prabaswari et al., n.d.)	Evaluasi Implementasi Kebijakan Pembentukan Tim Tanggap Insiden Siber pada Sektor Pemerintah https://doi.org/10.21787/mp.6.1.2022.1-13	Discusses the results of the evaluation of CSIRT implementation in the government sector

Research Methods

The research method used is qualitative research, namely the Case Study Method. With an analysis method using Fishbone problem analysis (cause and effect), GAP as is & To be Condition analysis and Value chain analysis to form a knowledge management strategy analysis.

Results and Discussions

Problem Analysis with Fishbone Diagrams

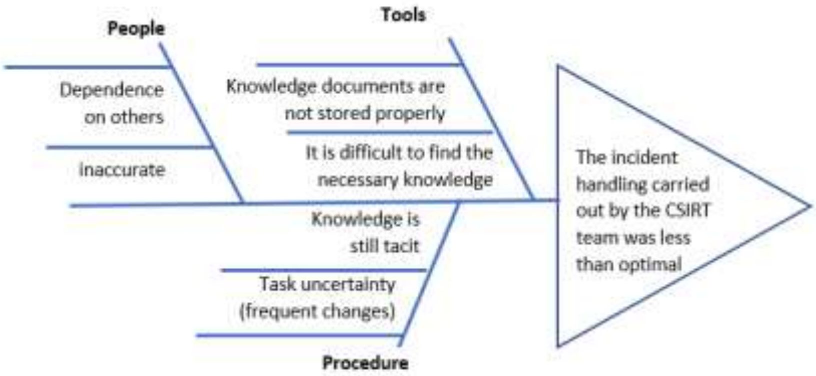

People
Dependence on others
Inaccurate
Tools
Knowledge documents are not stored properly
It is difficult to find the necessary knowledge
Knowledge is still tacit
Task uncertainty (frequent changes)
Procedure
The incident handling carried out by the CSIRT team was less than optimal

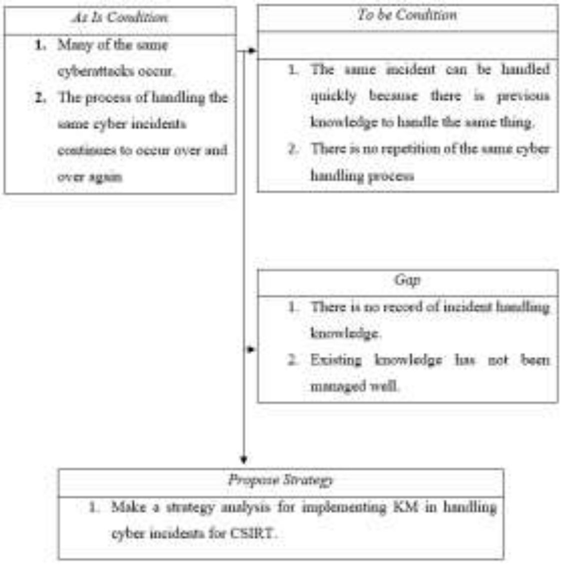
Figure 1 Analysis Fishbone

Table 2
Problem analysis

Problem analysis	The root of the Problem
The CSIRT team had difficulty finding solutions when encountering problems and had to ask other or experienced teams.	Solution knowledge is still in tacit form.
The CSIRT team often carries out repeated analyses of incidents that have occurred before.	There is no record of incident handling knowledge.
Knowledge and information on handling incidents is difficult to find and unstructured.	Existing knowledge is not managed well.

Every problem experienced by the CSIRT Team in handling incidents that were less than optimal was caused by several problems, such as repeated analysis and problem-solving of incidents that had occurred before, as well as knowledge and incident reports that the CSIRT Team does not manage.

GAP Analysis As Is & Becoming Condition



As Is Condition

1. Many of the same cyberattacks occur.
2. The process of handling the same cyber incidents continues to occur over and over again

To be Condition

1. The same incident can be handled quickly because there is previous knowledge to handle the same thing.
2. There is no repetition of the same cyber handling process

Gap

1. There is no record of incident handling knowledge.
2. Existing knowledge has not been managed well.

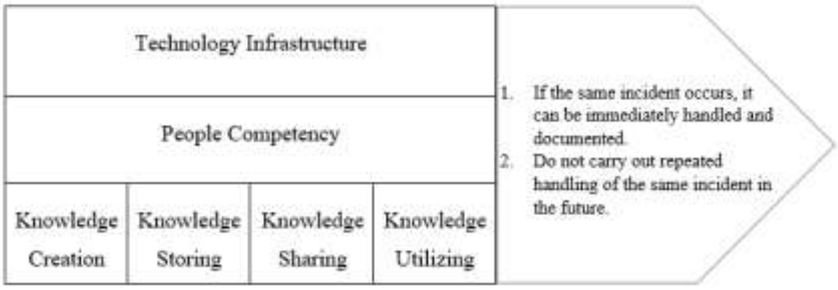
Propose Strategy

1. Make a strategy analysis for implementing KM in handling cyber incidents for CSIRT.

Figure 2
Analysis As Is & Becoming Condition

Knowledge Management Recommendations

The results of the data gap analysis will then be explained with the results of the analysis using Value Chain. This analysis will be described in the following table:



1. If the same incident occurs, it can be immediately handled and documented.
2. Do not carry out repeated handling of the same incident in the future.

Figure 3 KM Value Chain

Table 3
KM Value ChainKM Process and Enabler

No	Category	KM Activities	Descriptions
1	Primary	Knowledge Creation	Activities refer to developing new knowledge from data, information, or previous knowledge.
2	Primary	Knowledge Storing	Activities of storing and retrieving existing knowledge in various forms of component structures, knowledge, codification of knowledge, and storage of knowledge for organisational memory
3	Primary	Knowledge Sharing	Activities in which explicit or tacit knowledge is communicated to other individuals

4	Primary	Knowledge Utilizing	Activities that use actual knowledge that can be used to adjust strategic direction, solve new problems, and increase efficiency
5	Secondary	Technology Infrastructure	Support in the form of technology or tools to support organisational performance
6	Secondary	People Competency	The ability of individuals involved in the organisation to carry out their primary tasks

KM Process

The KM process consists of 4 parts: creating, storing, sharing, and utilising knowledge. The following activities must be carried out in each KM Process to handle cyber incidents at CSIRT in the local aviation sector.

Knowledge Creation

Knowledge creation is the activity most often defined as a KM strategy. This is consistent with the alignment of knowledge development in support of effective KM management. Nothing can be managed without information. True courage cannot be developed without an adequate knowledge-generating process. Therefore, the development of knowledge is the main activity in KM.

At this stage, each CSIRT team collects tacit and explicit knowledge. After that, the knowledge collected is classified by the level of existing knowledge or information, whether in the form of tacit or explicit knowledge. More detailed steps are as follows:

1) Classification of Application of Knowledge

At this stage, the existing knowledge and information are classified according to their level, whether in the form of tacit or explicit knowledge. Knowledge creation is applied using the SECI model (socialisation, externalisation, combination, and internalisation).

2) Create a Tree of Knowledge

The knowledge collected and classified is mapped into a decision tree model or knowledge tree. At this stage, a category type is created for each existing information as follows:

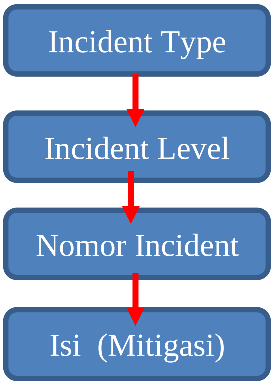


Figure 4. Knowledge Classification

Incident Type

Incident Type contains the initial Knowledge category. Knowledge categories include ATO (Account et al.), ransomware, Phishing, etc.

Incident Level

Incident Level is a subsection of Incident Type; incident level contains the classification of incident levels for each category, such as Low, Medium, High, and Critical. This level of determination refers to the severity of the cyber security risk.

Incident Number

This Incident Number refers to the classification of incident report documents where the number has been specified in the classification code name and predetermined number.

contents (Mitigation)

The content is detailed knowledge; this section contains mitigation steps to handle cyber incidents in text and document form. Here is an example of a knowledge tree that has been classified based on Incident Type, Level, Number, & Content:

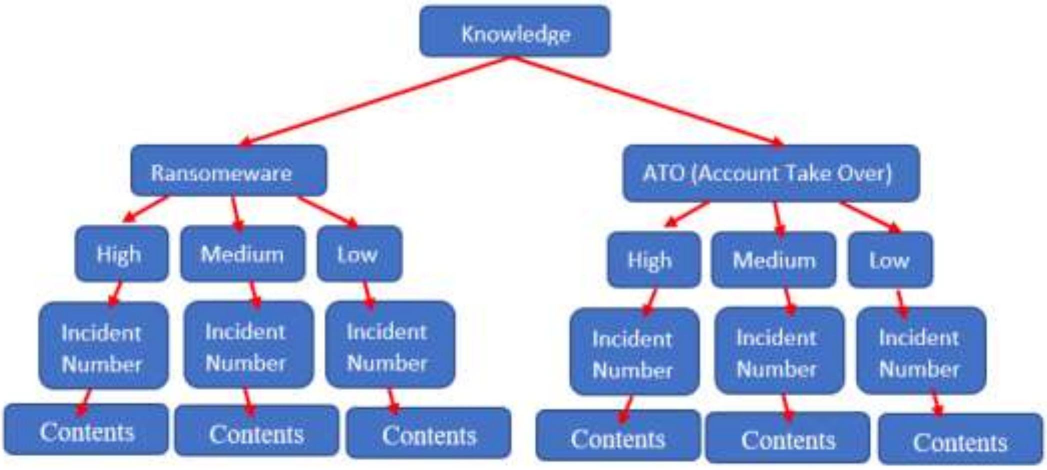


Figure 5 Knowledge Tree

Knowledge Storing

The second knowledge process defines knowledge storage as storing and retrieving knowledge in many forms, including component structures, knowledge, knowledge codification, and knowledge storage for organisational memory.

Any knowledge generated by the KM process must be processed first and then stored in a predetermined structure. After creating standard documentation at the Knowledge Creation level, the CSIRT team needs to define the structure of the database components.

The database component structure is a knowledge structure organised by tacit or explicit information that is then transformed into a structured form.

All documentation standards were divided into two parts. The first part is explicit: storing data containing incident data, incident points, incident impact, severity of the incident, tools used, and metadata of all existing processes. Then the second part is storing knowledge in tacit form, namely cyber incident handling activities. Tacit knowledge is then externalised into explicit knowledge. The two parts can be stored simultaneously in a structured form for easy processing.

Knowledge Sharing

The third KM process is Knowledge Sharing, which decides how knowledge will be transferred or communicated to individuals inside the organisation. People in organisations are the primary providers and consumers of knowledge management.

This activity focuses on developing skills in knowledge distribution. Because all knowledge is now explicit, the dissemination process can be streamlined. The knowledge recorded in the form of incident data, incident points, incident impact, incident severity, tools utilised, metadata, and activities from all existing processes is consolidated into a single knowledge base. The storage provided can be a single platform, making it easier for users to access this knowledge.

Knowledge Utilizing

KM is an appropriate concept in this activity since it involves knowledge. This is correct because the idea behind employing this concept is that it can aid with work and activities. By setting KM Goals, it is hoped that the knowledge transferred can be used to carry out Business Process Reengineering and Business Process Improvement on old business processes.

This KM Activity might be an application focusing on incident diagnosis and prevention. Occurrence diagnostics is a method that identifies the type of occurrence and the underlying causes. By having an incident diagnosis, the current KM Goal can be achieved, namely avoiding repeated incidents because the CSIRT team knows the root of the problem that causes the incident to occur. On the other hand, incident prevention is a development procedure to avoid events that might occur and can handle the same events that have been handled before. So, Incident Diagnostic and Incident Prevention provide benefits for companies because they can reduce costs due to cyber incidents by reducing work on handling cyber incidents and avoiding the risk of incidents occurring.

KM Enabler

KM Enablers consists of 2 parts: technological infrastructure and human resource competence. Each must carry out the following activities:

1) Technology Infrastructure

Technological infrastructure is essential as it can catalyse the KM process. We can cross space, time and language boundaries with good technological infrastructure. Apart from that, the use of technology can also reduce production costs when developing a KM system.

KM Infrastructure's contribution to this research comes in the form of advice for establishing an online knowledge base. Preparing reliable supporters can help support using knowledge bases as a medium for knowledge-sharing activities. Especially when adapting to change, the CSIRT team needs rapid development in managing knowledge. The knowledge exchange process can be faster and more effective because it is hosted online so that anyone and anywhere the CSIRT team can use and store knowledge, allowing the CSIRT team to use and store knowledge from anywhere. As a result, the organisational development process at local Indonesian aviation companies will improve, thereby increasing the organisation's worth.

2) People's Competency

Human resource competency is a critical component for everyone involved in the firm. Each person's competency is evaluated based on their ability to perform their primary job. With the proper people in the right roles, the company should be able to achieve its objectives effortlessly.

At this stage, local Indonesian aviation companies, primarily the Information Security division, must conduct competency training for each CSIRT team based on the team's responsibility. There is a need for a cyber competence-specific SOP document that will help to execute a more structured and effective human resource competency procedure.

Knowledge Base Design

At this stage, the results of the KM value chain analysis above make recommendations for designing a knowledge base to manage various knowledge related to cyber handling for the CSIRT team.

Use Case Diagram

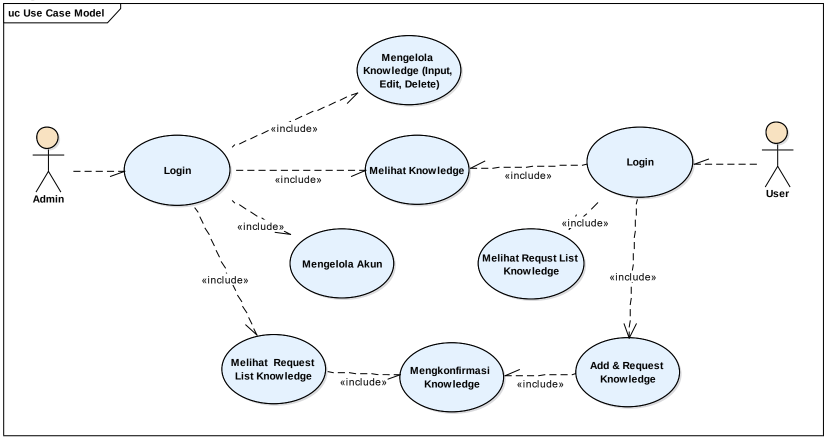


Figure 4 Usecase Diagram

In the use case diagram above, the admin has several activities such as viewing knowledge, inputting knowledge, editing knowledge, deleting knowledge, managing accounts, viewing the knowledge request list and confirming the addition of knowledge from users. The admin can carry out all of these activities by logging in first. In contrast, the user carries out several activities, such as viewing Knowledge, viewing the Knowledge Request list, and adding Knowledge, which the admin will later confirm before inputting it into the system; users can only do these activities after logging in first.

Admin Activity Menu

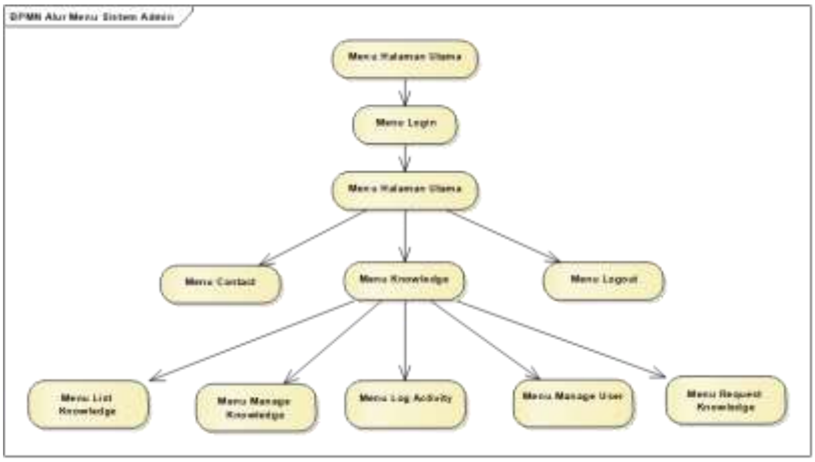


Figure 5. admin System Flow

User Activity Menu

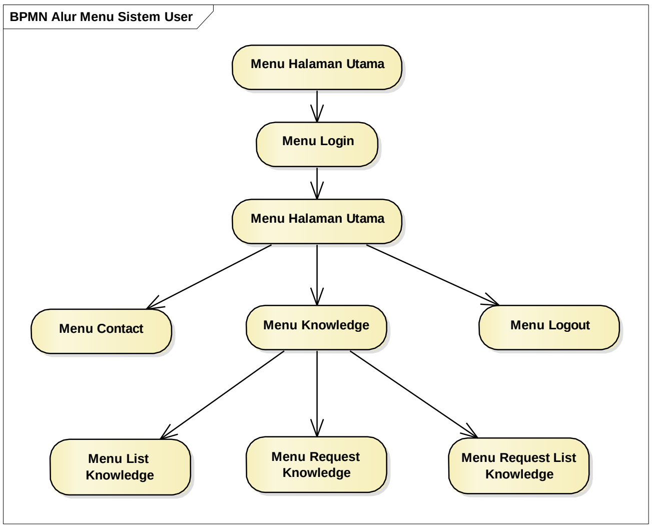


Figure 6. User System Flow

User Acceptent Testing

Apart from using black box testing, a User Acceptance Test (UAT) will be carried out at this testing stage. This test is carried out so that the system results match what the user wants.

Here are the testing stages:

This test uses a questionnaire to get the results. This test is used to assess the system in terms of system benefits, system appearance, and system feasibility.

The respondents' questionnaires will later be calculated using the Likert Scale method. The Likert scale measures a person or group's perception, attitude or opinion regarding social events or phenomena based on operational definitions that researchers have determined. When using the Likert scale, there are two forms of questions: positive questions to measure the positive scale and negative questions to measure the negative scale. Positive questions were scored 5, 4, 3, 2, and 1, while negative forms of questions were given scores of 1, 2, 3, 4, and 5.

Formula: T x Pn
Q: Total number of respondents who voted
Pn: Likert score number selection

In answering the questionnaire with calculations using the Likert scale, respondents answered on the microform by selecting one of the radio buttons on each question. The questionnaire that respondents have filled out is given a score for each answer, as shown in the table below:

Table 4
Assessment Weights

Statements	Score
Strongly agree	5
Agree	4
Less agree	3
Disagree	2
Strongly disagree	1

Table 5
UAT Results

No	Questions	Strongly agree	Agree	Less agree	Disagree	Strongly disagree
1	Does the system fulfil the need for CSIRT?	6	4	0	0	0
2	Are all expected features and functions of the system sound for CSIRT?	8	2	0	0	0
3	Is the appearance system easy for CSIRT to use?	3	7	0	0	0
4	is with exists system. This can help the CSIRT team look for the knowledge you need.	5	5	0	0	0
5	Ia system This can accessed When, or is there a limitation time specific?	1	7	2	0	0
Total		23	25	2	0	0

Based on the results of the calculation above, it can be concluded as follows:

1. P strongly agree: 23 * 5 = 115
2. P agree: 25 * 4 = 100
3. P less agree: 2 * 3 = 6
4. P disagree : 0 * 2 = 0
5. P strongly disagree : 0 * 1 = 0

Total Score = 221

After that, a search is carried out on the interpretation results by giving the highest score (Y) and the lowest score (X) with the following formula:
X = lowest Likert score * number of respondents * number of questions
X = 1*10*5 = 50
Y = highest Likert score * number of respondents * number of questions
u = 5 * 10 * 5 = 250

After determining the highest and lowest values, a search is conducted to find the interval and per cent interpretation using the method of finding the per cent score interval (I) with the following formula.
I = 100 / total Likert scores
I = 100/5
= 20

So, the distance interval from lowest to highest is 20. Here are the criteria for interpreting scores based on intervals.
A. Figure 0% - 19.99 = Strongly disagree
B. Figure 20% - 39.99% = Disagree
C. Figure 40% - 59.99% = Enough
D. Figure 60% - 79.99% = Agree
E. Number 80% - 100% = Strongly Agree

After that, a search is carried out using the % index formula.
Index % = Total Score / Y * 100
The % index results for respondents are as follows.
Index% = 221/250 * 100
= 88%

Conclusion

From this research, after analysing the gaps between current and expected conditions, there are two gaps: the absence of reporting, direct handling, and the absence of management of repeated threats from cyber attacks in the future; after carrying out gap analysis and value chain mapping to form a KM strategy. The result is that there are 4 KM Processes and 2 KM Enablers in achieving the KM Goal. The KM processes are Creation, Storage, Knowledge Sharing, and Knowledge Utilization. Meanwhile, KM Enabler has a technological infrastructure and human resources competency. With all the components in the KM Value Chain, it is hoped that the two KM Goals, namely the same cyber incident, can be immediately reported and handled and that cyber incidents will not occur again in the management and reporting of cyber incidents. This Knowledge Management Strategy Analysis can help the local Indonesian Aviation Information Security Unit CSIRT team overcome and manage cyber incidents better.

References

Alfikri, M., & Ahmad, I. (2022). Evaluasi Implementasi Kebijakan Pembentukan Tim Tanggap Insiden Siber pada Sektor Pemerintah. *Matra Pembaruan: Jurnal Inovasi Kebijakan*, *6*(1), 1–14. https://doi.org/10.21787/mp.6.1.2022.1-14

Fernandes, A., Oliveira, A., Santos, L., & Rabadã, C. (2021). A Strategy for Implementing an Incident Response Plan. *European Conference on Cyber Warfare and Security*, 120–XIV.

Firmansyah, M., & Yuswanto, A. (2022). Knowledge management for information security incident handling at the Security Operation Center of Jakarta Provincial Government. *Monas: Jurnal Inovasi Aparatur*, *4*(2), 441–452. https://doi.org/10.54849/monas.v4i2.102

HUTAURUK, O. G. (2023). *Penerapan Manajemen Risiko Cyber Security Di Atas Mv. Ever Ocean Untuk Mewujudkan Keamanan Teknologi Informasi Di Era Society 5.0*.

Islami, M. J. (2018). Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index. *Masyarakat Telematika Dan Informasi: Jurnal Penelitian Teknologi Informasi Dan Komunikasi*, *8*(2), 137–144.

Kaburuan, E. D. (2022). *Efektivitas Strategi Polri Dalam Pemberantasan Kejahatan Siber Melalui Asean Ministerial Meeting On Transnational Crime (AMMTC)*. Universitas Kristen Indonesia.

Kristiyono, J. (2015). Budaya internet: Perkembangan teknologi informasi dan komunikasi dalam mendukung penggunaan media di masyarakat. *Scriptura*, *5*(1), 23–30.

Mahendra, Y. C., & Pinatih, N. K. D. S. A. (2023). Strategi Penanganan Keamanan Siber (Cyber Security) Di Indonesia. *Jurnal Review Pendidikan Dan Pengajaran (JRPP)*, *6*(4), 1941–1949.

Prabaswari, P., Alfikri, M., & Ahmad, I. (n.d.). The Implementation of Policy for the Establishment of A Cyber Incident Response Team to Support Information Security in the Government Sector. *Matra Pembaruan*, *6*(1), 1–14. https://doi.org/10.21787/mp.6.1.2022.1-14

Sari, N. W. (2018). Kejahatan cyber dalam perkembangan teknologi informasi berbasis komputer. *Jurnal Surya Kencana Dua*, *5*(2), 577–593.

Solehudin, M. M., Deni, A., Kuswibowo, C., Erfina, S. P. I., Oktavianty, S. E., Biomi, A. A., Erg, M., Irmawati, S., Sudiyarti, M. S., & Anwar, H. M. (2023). *DIGITALISASI MANAJEMEN ORGANISASI*. Cendikia Mulia Mandiri.