Scientific Research Publishing

Journal of Information Security, 2022, 13, 294-311
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Knowledge Management Strategy for Handling Cyber Attacks in E-Commerce with Computer Security Incident Response Team (CSIRT)

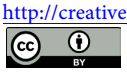
Fauziyah Fauziyah[1], Zhaosun Wang[1], Gabriel Joy[2]

[1]School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing, China
[2]Faculty of Economics and Business, University of Indonesia, Depok, Indonesia
Email: B20190694@xs.ustb.edu.cn, zhswang@sohu.com, joygabriel.21@ui.ac.id

How to cite this paper: Fauziyah, F., Wang, Z.S. and Joy, G. (2022) Knowledge Management Strategy for Handling Cyber Attacks in E-Commerce with Computer Security Incident Response Team (CSIRT). *Journal of Information Security*, **13**, 294-311.
https://doi.org/10.4236/jis.2022.134016

Received: August 6, 2022
Accepted: September 20, 2022
Published: September 23, 2022

Copyright © 2022 by author(s) and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/



Open Access

Abstract

Electronic Commerce (E-Commerce) was created to help expand the market share network through the internet without the boundaries of space and time. However, behind all the benefits obtained, E-Commerce also raises the issue of consumer concerns about the responsibility for personal data that has been recorded and collected by E-Commerce companies. The personal data is in the form of consumer identity names, passwords, debit and credit card numbers, conversations in email, as well as information related to consumer requests. In Indonesia, cyber attacks have occurred several times against 3 major E-Commerce companies in Indonesia. In 2019, users' personal data in the form of email addresses, telephone numbers, and residential addresses were sold on the deep web at Bukalapak and Tokopedia. Even though E-Commerce affected by the cyber attack already has a Computer Security Incident Response Team (CSIRT) by recruiting various security engineers, both defense and attack, this system still has a weakness, namely that the CSIRT operates in the aspect of handling and experimenting with defense, not yet on how to store data and prepare for forensics. CSIRT will do the same thing again, and so on. This is called an iterative procedure, one day the attack will come back and only be done with technical handling. Previous research has succeeded in revealing that organizations that have Knowledge Management (KM), the organization has succeeded in reducing costs up to four times from the original without using KM in the cyber security operations. The author provides a solution to create a knowledge management strategy for handling cyber incidents in CSIRT E-Commerce in Indonesia. This research resulted in 4 KM Processes and 2 KM Enablers which were then translated into concrete actions. The KM Processes are Knowledge Creation, Knowledge Storing, Knowledge

Sharing, and Knowledge Utilizing. While the KM Enabler is Technology Infrastructure and People Competency.

Keywords

Knowledge Management, Cyber Security, Computer Security Incident Response Team (CSIRT)

1. Introduction

Advances in technology are increasingly sophisticated today. This accelerates the globalization process. The speed of information that occurs strengthens the joints of life. The speed of information circulation is directly proportional to the speed of the economy, so all technologies-adaptive countries will feel the economic impact on each sector [1].

The retail industry is also affected by technological advances. Retail is no longer a supporting aspect of the economic structure of society [2]. The fulfillment of human needs is supported by the progress of the retail industry. The effect of this progress is an increase in the GDP of a country. In Indonesia, the retail industry contributes significantly to GDP, which is worth 10% [3].

Technology is a solution to various problems in the retail world. One of the problems in the retail world is scalability, which is doubling the retail system starting from the supply chain to selling from one place to another. Currently, the retail industry can abandon the brick-and-mortar form with solutions to build virtual spaces for retail systems. The retail business requires substantial costs, in relation to its operations, and supply chain is quite long, so digitization is the best solution today. The retail business is currently able to withstand all emergency conditions, even in an area that is being hit by war, or during a pandemic, online-based retail businesses are able to survive and even become a solution. This system is built in the form of a website or mobile application; even now it can be done through social media. This system is called E-Commerce. Thus, a retail brand can accelerate its scalability which of course has an impact on increasing revenue and extending to the economic structure. Retailers that involve their activities in a virtual space through a website, are able to sell up to five times more products than retailers that only rely on manual sales systems or directly in offline stores [4].

However, behind all the benefits, E-Commerce also raises the issue of consumer concerns about responsibility for personal data that has been recorded and collected by an E-Commerce. The personal data is in the form of consumer identity names, passwords, debit and credit card numbers, conversations in email, as well as information related to consumer requests. Several cases regarding the leakage of personal data that have occurred on E-Commerce in Indonesia are various. In 2019, there was a case of leakage of personal data from the largest E-Commerce company in Indonesia. The personal data sold in the form of email

addresses, telephone numbers, and residential addresses were sold at a price of 234 US dollars [5]. Also in the same year, E-Commerce Bukalapak also experienced a data leak; as many as 13 million users' personal data were stolen by professional hackers known as gnostic players. The stolen data consisted of emails, usernames, shopping details, IP addresses, and account passwords. In response to this, Bukalapak has confirmed that there was indeed a hacking attempt, but that no important data such as usernames, passwords, financial or other personal information were managed by the hackers [6].

The case of leakage of personal data from this E-Commerce company will continue until 2020. In 2020, to be precise, in May, Tokopedia's E-Commerce experienced another leak of personal data [7]. Personal data sold includes e-mail address, username, gender, location, user's full name, mobile number, and password. However, the company claims that the user's information remains protected. In addition, Bhinneka.com in the same month and year, Bhinneka.com user data has been sold on 1.2 million users. Cases of this kind are still happening, as evidenced in September 2020, the E-Commerce curator, ShopBack, admitted to finding illegal access to the user data system. Although important information is still safe, ShopBack still recommends users to change their passwords for account security.

This phenomenon and cases of data leakage were created due to changes in people's behavior through online shopping which experienced a significant increase. The various phenomena and cases bring their own impact on E-Commerce users, especially on personal data. The personal data of E-Commerce users is often threatened and misused by irresponsible parties. This is a separate concern for users in using E-Commerce. Thus, the security aspect for processing data needs to be focused on E-Commerce companies [8].

The solution offered to E-Commerce companies today is to handle it by a cyber team which is often called the Computer Security Incident Response Team (CSIRT). CSIRT is an organization or team that provides services and support to a defined constituency for preventing, handling, and responding to computer security incidents [9]. Attacks and defenses against cyber-attacks are centralized in one team so that attack and defense methodologies can be synchronized. Several E-Commerce sites in Indonesia already have CSIRT by recruiting various security engineers, both defense and attack.

However, CSIRT still has its drawbacks. Based on interviews with security experts, several E-Commerce companies who already have CSIRT stated that they are still in the aspects of handling and experimenting with defense, not yet on how to store data and prepare for forensics. When the attack reappears, the CSIRT will do the same thing again, and so on. Thus, there is an iterative procedure, in which one day the attack will come back and only be carried out with technical handling.

In order to improve the performance of better platform security in the future, organizations need to manage knowledge regarding reporting and handling cyber incident that have occurred [7]. From the perspective of cognitive theory,

knowledge is divided into two categories, namely explicit knowledge and tacit knowledge [9]. Explicit knowledge is knowledge that can be expressed by symbols, stored in literature, and easily stored, communicated, and shared. Meanwhile, tacit knowledge is knowledge rooted in one's experience, highly personalized and difficult to format, usually exchanged and shared through direct and face-to-face contact. Mutual conversion and mutual benefit can be realized between explicit knowledge and tacit knowledge. That is, explicit knowledge can be converted into tacit knowledge and tacit knowledge can also be converted into explicit knowledge. This transformation is called the developmental spiral of knowledge creation. As for studying the process of knowledge conversion and creation, the most famous model is the SECI model proposed by Nonaka in 1991.

Cyber incidents in E-Commerce are becoming a critical issue. On average, for every 1 critical incident that occurs to a user, there will be a loss of 20,000 users. These critical incidents are incidents that can result in inaccessibility of the platform or when user data is stolen. Every 1 number of cyber incidents that occur to users creates a loss of 10% of revenue. The loss is potentially higher because E-Commerce is an industry that is still growing in Indonesia, so customer trust is the number one issue [10].

So that this repetitive procedure does not continue to occur, a Knowledge Management (KM) is needed to manage knowledge related to cyber-attacks and defenses [11]. All forms of attacks that occur are then carried out in forensic preparations so that there are no repeated incidents. In organizations that have KM, the organization has succeeded in reducing costs up to four times from the original without using KM in the cyber security operations. Therefore, we will discuss the application of Knowledge Management in CSIRT in E-Commerce, especially in Indonesia.

2. Theoretical Background

2.1. Knowledge

Knowledge is dynamic created through social interactions between individuals [12]. Knowledge is divided tacit that rooted in individual's mind and it is a result of values, beliefs, life experiences, emotions, procedures, actions and routines; and explicit it is easy to transmit since it is already systematized in data, formula, manual, books, specifications, along with others.

2.2. Knowledge Management

Knowledge Management (KM) is the effort to manage organizations' workforce through information and communication technologies or creation of a corporate culture that focuses on social processes that facilitate the sharing between individuals, aiming to reach a sustainable source of advantage [13].

This understanding is defined as a collection of tools, techniques, and strategies for retaining, analyzing, organizing, enhancing, and sharing insights and

experiences. Such understanding and experience are built on knowledge, whether embodied in an individual or embedded in the real processes and applications of an organization. In addition, KM is undertaken to enhance the ability of organizations to learn from the environment and to incorporate knowledge into business processes and decision making.

2.3. Knowledge Management Strategy

Knowledge Management Strategy (KMS) is the effort to manage organizations' workforce through information and communication technologies or creation of a corporate culture that focuses on social processes that facilitate the sharing between individuals, aiming to reach a sustainable source of advantage [7].

This understanding is described as a collection of tools, techniques, and strategies to maintain, analyze, organize, enhance, and share understanding and experiences. Such understanding and experience are built on knowledge, whether embodied in an individual or embedded in the real processes and applications of an organization. In addition, KM is undertaken to enhance the ability of organizations to learn from the environment and to incorporate knowledge into business processes and decision making.

Knowledge Management (KM) is doing something needed to produce a maximum result using the existing knowledge resource [14]. Knowledge Management Systems (KMS) are systems that support mechanisms and processes in knowledge management [14]. Knowledge management, according to Becerra, has an impact on people by increasing their ability to learn, improve member adaptability, and increase job satisfaction. Then it has an impact on the process carried out by the company or organization by increasing the effectiveness of the project, efficiency, and the level of innovation in the ongoing process [15].

2.4. Cyber

Cyber is a space where communities are connected to each other using a network to carry out various daily activities [16]. The term cyber relates to all aspects of computing, including storing data, protecting data, accessing data, processing data, transmitting data and connecting data. Also, cyber can defined as the space for data and information sharing towards the communities without the time and nation barrier [17].

2.5. Cyber Attack

Cyber attack is a type of offensive maneuver used by countries, individuals, groups, or organizations that target computer information systems, infrastructure, computer net-works, and/or personal computer devices by various means of malicious actions that usually come from anonymous sources that steal, change, or destroy specified targets by hacking vulnerable systems [18]. In other words, a cyber attack is defined as an attack to disrupt, disable, destroy, or control the computing environment or to access controlled information. It must be countered by de-

signing an efficient defense framework that is challenging with respect to a network's complexity, widespread sophisticated attacks, attackers' ability, and the diversity of security appliances [19].

2.6. Handling the Cyber Attack

Cyber attack handling is a type of offensive maneuver used by countries, individuals, groups, or organizations that target computer information systems, infrastructure, computer networks, and/or personal computer devices by various means of malicious actions that usually come from anonymous sources who steal, modify, or destroy specified targets by hacking vulnerable systems [14]. In other words, a cyber attack is defined as an attack to disrupt, disable, destroy, or control the computing environment or to access controlled information.

2.7. E-Commerce

E-Commerce is one of the most important digital channels of transaction. Persons, enterprises, and governments can participate in E-Commerce transactions. Different models of E-Commerce have been developed based on different application scenarios. Ranging from E-Commerce Business to Business (B2B), E-Commerce Business to Consumer (B2C), to E-Commerce Consumer to Consumer (C2C) [20]. E-Commerce in general can be interpreted as transactions of buying and selling performed electronically through internet media [21]. In addition, E-Commerce can also be interpreted as a business process using electronic technology that connects companies, consumers and the community in the form of E-Commerce electronic transactions and the electronic exchange or sale of goods, services and information.

2.8. Handling the Cyber Attack in E-Commerce

E-Commerce is one of the most important channels of transaction. Persons, enterprises, and governments all participate in E-Commerce transactions. Different models of E-Commerce have been developed based on different application scenarios. E-Commerce in general can be interpreted as buying and selling transactions electronically through internet media. In addition, E-Commerce can also be interpreted as a business process using electronic technology that connects companies, consumers and the community in the form of E-Commerce electronic transactions and the electronic exchange or sale of goods, services and information [22].

2.9. Computer Security

Computer Security is defined as a computer-based discipline, which involves technology, people, information and processes, with the goal of securing operations against unauthorized access or attack [4]. This practice aims to protect systems, networks, and programs from digital attacks. These attacks are usually aimed at accessing, altering, or destroying sensitive information; extort money

from users; or interfere with normal business processes.

Cybersecurity principles should take into account the technical level that pertains to the information technology itself, the formal level that concerns organizational bureaucracy and the use of information, and the informal level that refers to organization subcultures. In this context, cybersecurity is defined in a more flexible manner as "a well-informed sense of assurance that information risks and information security controls are in balance" [23].

2.10. Incident

Incident is represented as a sequence of activities; each activity indicates the execution of an action in the smart space. Incident activities may be malicious because they exploit a specific vulnerability, and/or may be legitimate (e.g. enter a room, connect to a network). Using the tool, incidents can refer to components and actions defined for one or more smart building models [16]. In other words, a cyber incident is one or a series of events that disrupt or threaten the operation of the Electronic System.

2.11. Incident Response

Incident response is intended to respond automatically to incidents by attuning the attack damage and countermeasure costs [3]. Cybersecurity Incident Handling is an attempt to detect, report, assess, handle and respond to and study cybersecurity incidents. Cybersecurity Incident Response is an attempt made to mitigate, repair and or restore an Electronic System to a normal condition. Meanwhile, a cybersecurity culture refers to the procedures laid down by an organization to all its employees, directing their course of action in all situations related to data integrity, whenever in the line of duty [20].

2.12. Computer Security Incident Response Team (CSIRT)

Computer Security Incident Response Team (CSIRT) is well known in the information security domain. It has recently received renewed interest for novel areas of application like cloud computing (with its unique information security challenges) and in developing countries catching up with the Internet bandwagon [21]. There is a relevant data component for the incident response procedures that include threat intelligence and other information from various sources [5]. CSIRT business requirements and services are introduced, before exploring the relationships between the areas using argumentation [8].

3. Research Methodology

The explanation of the research design, research steps, data processing methods, and research instruments is explained in this chapter. All sections are arranged referring to the Research Question and the theoretical framework that has been described in the previous chapter [24] (**Figure 1**).

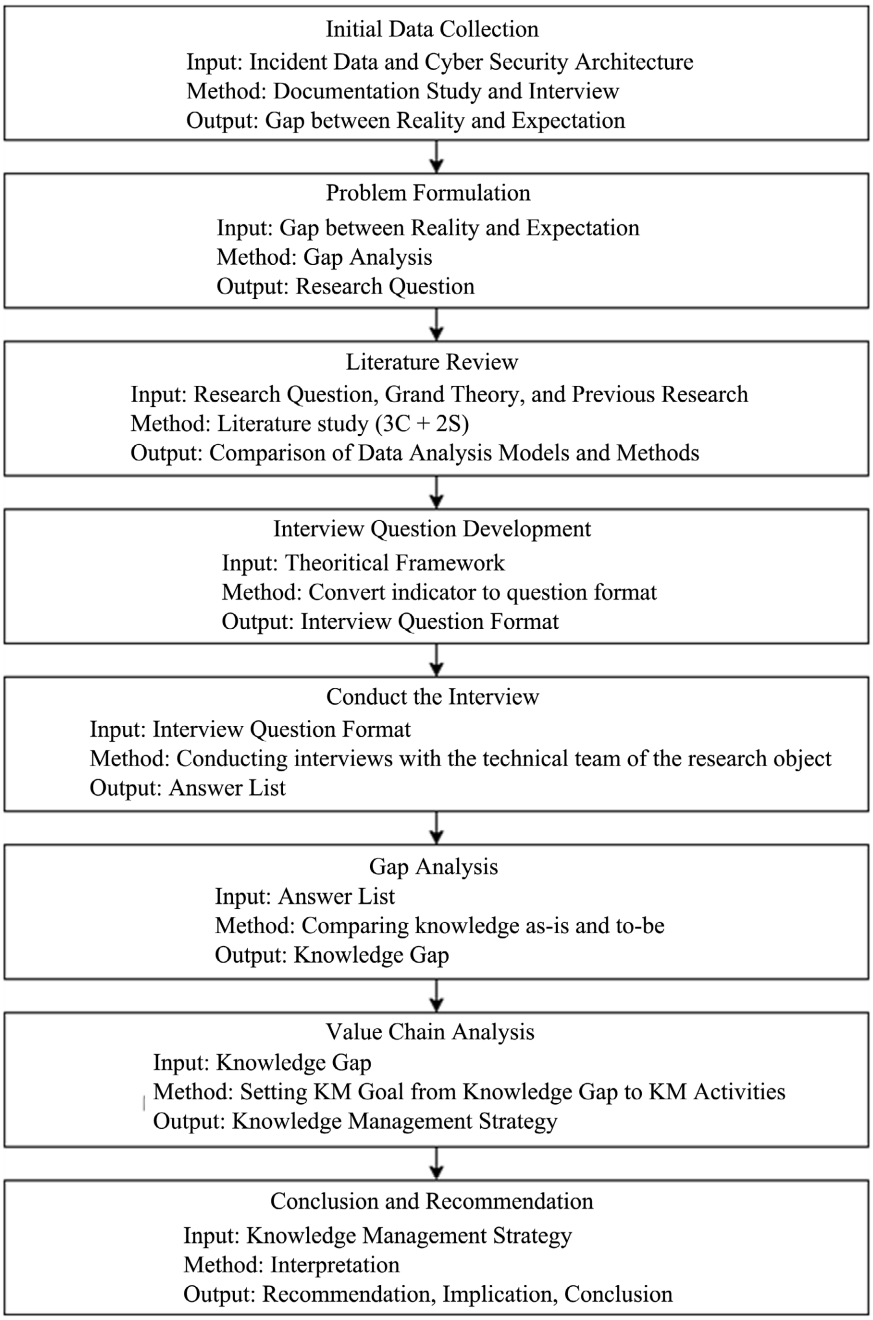


Figure 1. Research methodology.

3.1. Research Design

This research is conducted on several E-Commerce companies in Indonesia. This study aims to answer the Research Question in order to provide practical and concrete benefits for the object of research. Therefore, in the form of applied research.

3.2. Data Collection Method

In terms of data sources, this study uses primary and secondary data. Primary

data comes from the object, namely the technical team of the research object through interviews. As for the secondary data obtained from Incident Data and Cyber Security Architecture of each research object.

In order to collect empirical data, we used purposive sampling techniques which are used in qualitative research, and may be defined as selecting interviewees based on specific goals that are associated with answering research questions [15]. In particular, considering the fact our research gathers specific knowledge from individuals that have particular expertise, the adopted sampling technique falls into the assumptions of expert sampling. The expert for this interview is the cyber security engineer of some E-Commerce companies in Indonesia.

3.3. Data Analysis Method

This study uses a gap analysis technique to analyze the data (with Microsoft Word). Gap analysis is used to determine what steps need to be taken to move from current conditions to future conditions [16]. Gap analysis can also be interpreted as a comparison of actual performance (as-is) with potential performance (to-be). The output of the gap analysis is a knowledge gap that can be made in the form of a KM Value Chain to describe the strategy in a coherent manner. Therefore, gap analysis is a strategy that is more suitable to be implemented for organizations that are still in simple form, such as CSIRT.

After conducting a gap analysis, the authors mapped each interview data into a diagram that resulted in the strategy being implemented. Then, the strategy is detailed into the KM Value Chain. From the KM Value Chain, a strategy will be printed in the form of how the E-Commerce CSIRT can achieve the to-be condition.

3.4. Interview Questions List

The interview questions list as follows:

1) What are your duties as a Security Engineer?

2) How many people do you supervise?

3) How is the end to end Cyber Security process in your company?

4) Who are the parties involved in the end to end Cyber Security process in your company?

5) What do you think about the current Cyber Security team and end-to-end process at the company?

6) What is your opinion regarding the current Cyber Security team and end-to-end process at the company?

7) What is your input for your company's team, processes, management, and products for the future?

4. Result and Discussion

4.1. Gap Analysis

The gap analysis strategy is made by looking at the determinants between exist-

ing conditions and to be conditions. Based on the data collected by the author comprehensively, it produces 4 things, namely as is condition, to be condition, gap, and proposed strategy. This strategy is mapped out in Figure 2.

4.1.1. As Is Condition

As shown in Figure 2, the author found things that became the initial conditions in the process of handling cyber attacks in E-Commerce with CSIRT, namely:

1) Repeat handling of the same cyber incident.

Based on interviews from informants, the current condition is the repetition of the same reporting and incident handling procedures. This creates time inefficiency for the cyber security, software development, and QA teams because this process is repetitive.

2) Recurring cyber incident happened.

The next thing that the author found was that the CSIRT member found the same incident over and over again. The impact is that the focus on developing features incrementally is disrupted due to a divided focus on resolving these incidents.

4.1.2. To Be Condition

Then, as shown in Figure 2, the author suggests the desired conditions in the process of handling cyber attacks in E-Commerce with CSIRT, namely:

1) The same cyber incident can be directly reported and handled.

If an incident can be identified that has been handled, then the procedure carried out is complete. The process for reporting and resolving from the beginning is time-consuming because the same incident that is repeatedly reported and handled is a waste of time and money.

2) No recurring cyber incident.

The impact of incidents that appear repeatedly causes repeated efforts so that it creates a waste of time and money. This is certainly contrary to the company's goal of seeing costs based on the given value. The company wants to focus more on incremental feature development due to the volatile market situation.

4.1.3. Gap

Based on the initial conditions and the desired conditions, there are things that become gaps in the process of handling cyber attacks in E-Commerce with CSIRT, namely:

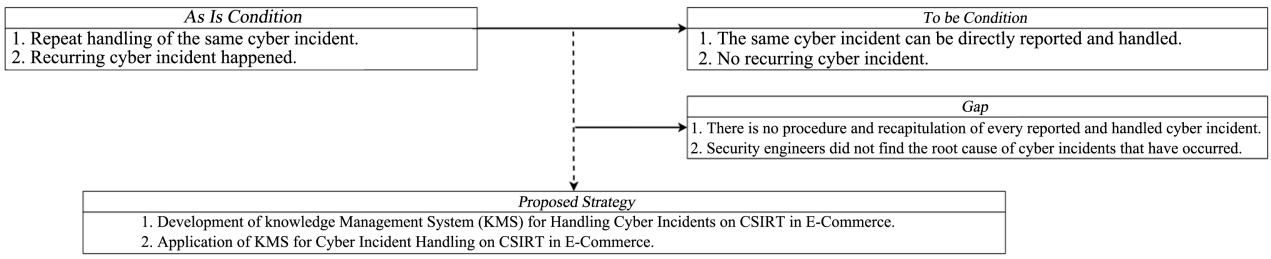


Figure 2. Gap analysis.

1) There is no procedure and recapitulation of every reported and handled cyber incident.

The repetition of the same incident reporting and handling procedures is caused by the absence of procedures and recapitulation of each reported and handled incident. This makes incident handling knowledge missing from the organization. The absence of data on each process of handling cyber incidents causes inaccurate information and actions taken. Then, the organization does not have preventive measures to deal with future uncertainties, such as the emergence of incidents in the future. In the worst case, failed products actually fail to be released to end-users which can cause a company's business to stop.

2) Security engineers did not find the root cause of the cyber incident that had occurred.

Repeated incidents occur because the security engineer only "treats the symptoms". This action is like seeing the tip of the iceberg. A thorough study is needed in order to see an incident as a unit. By having a comprehensive perspective, the security engineer can break the chain of incidents by solving the root cause of the incidents. Decisions taken are enriched with historical incident data and track record of software development.

4.1.4. Proposed Strategy

The author found two things that became the initial conditions in the process of handling cyber attacks in E-Commerce with CSIRT, namely:

1) Development of Knowledge Management System (KMS) for handling cyber incident on CSIRT in E-Commerce [25].

In overcoming the gap that occurs, it is a best practice system to manage all company knowledge both sourced from internal and external companies as well as the tacit knowledge of all experts. KMS is a strategy for managing knowledge in a structured and effective manner in storing, searching, and sharing knowledge for organizations [16]. Knowledge that has been managed is then disseminated back to HR experts. Human resource knowledge is an important company asset that must be managed effectively in order to provide added value to the company. By developing knowledge management, organizations can anticipate future possibilities and can eliminate repetitive processes for handling and reporting cyber incidents.

2) Application of KMS for cyber incident handling on CSIRT in E-Commerce.

The KMS built in Point 1 should be implemented by involving all stakeholders in software development and QA. Involvement aims to speed up the flow of information within the company and make the process of educating experts easier [16]. Then, the next effect is the cost efficiency of improving the quality and knowledge of human resources and in anticipation of the loss of company key personnel which causes the loss of company knowledge. The real effect on users is that it can help deal with problems faster which will have an impact on customer satisfaction.

4.2. Knowledge Management Value Chain

The results of primary and secondary data which are then elaborated with the results of the gap analysis create a KM Value Chain.

In Table 1, all KM Processes and KM Enablers have been described in detail. Therefore, the KM Value Chain created is as follows (Figure 3).

4.3. Discussion

As shown in Figure 3, the author summarizes the actions that can be taken based on the 4 KM Processes and 2 KM Enablers described above. Here is the description.

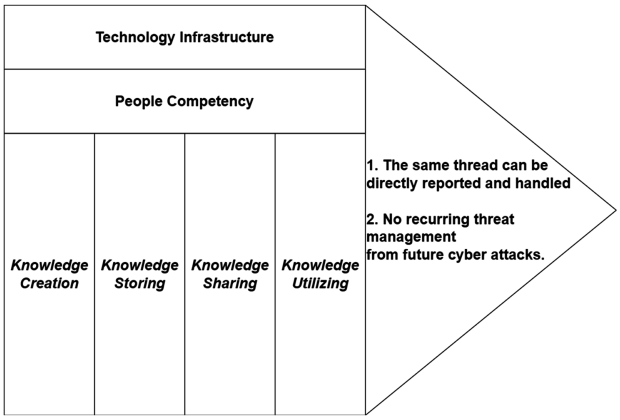


Figure 3. KM value chain.

Table 1. KM process and enabler.

No	Category	KM Activities	Description
1	Primary	Knowledge Creation	Activities that refer to the development of new knowledge from data, information, or previous knowledge [26].
2	Primary	Knowledge Storing	Activities of storing and retrieving knowledge that are in various forms of component structures, knowledge, codification of knowledge, and storing knowledge for organizational memory [26].
3	Primary	Knowledge Sharing	Activities in which explicit or tacit knowledge is communicated to other individuals [26].
4	Primary	Knowledge Ulitizing	Activities that use actual knowledge that can be used to adjust strategic directions, solve new problems, and increase efficiency [26].
5	Secondary	Technology Infrastructure	The main support is in the form of technology to support organizational performance [27].
6	Secondary	People Competency	The ability of individuals involved in the organization in carrying out their main tasks [23].

4.3.1. KM Process

The KM Process consists of 4 parts, namely creating, storing, sharing, and utilizing knowledge. The following are activities that must be carried out in each KM Process for the process of handling cyber incident on CSIRT in E-Commerce:

1) Knowledge Creation

Knowledge Creation is an activity that is most often defined as a KM strategy [28]. This fact is consistent with the alignment of knowledge creation in supporting good KM management. Without knowledge, then of course nothing is managed. Without a good knowledge-making process, of course no true courage is created. Therefore, knowledge development is the main activity in KM.

In the activities carried out at E-Commerce companies, there is no procedure to manage software separately from the software development process. The procedure is a procedure where you can find, identify, create characteristics, set goals, select processes, execute, analyze, provide resolutions, and carry out packaging [23]. Packaging is localizing and studying incidents so that in the end the organization can form an incident prediction, a way to detect the emergence of incidents. Logically, this step is very beneficial because the organization can avoid the existing risks because it can know the incidents that will occur even before the incidents appear. The above procedure completely states that the incident is a component that needs to be detailed and handled with special techniques because incidents will arise and arise according to product development.

2) Knowledge Storing

In the second knowledge process, knowledge storing is defined as the process of storing and retrieving knowledge in various forms of component structures, knowledge, codification of knowledge, and storing knowledge for organizational memory [26]. The keywords that can be taken from this activity are storage, retrieval, and structure. These three keywords will represent what must be done, namely creating a knowledge database. This knowledge database means a system that stores all knowledge and it is possible for knowledge transactions to occur, namely the entry and exit of knowledge. That way, the stored knowledge can be useful and utilized continuously so that its value continues to grow.

From the six processes of managing reporting and handling cyber incidents in E-Commerce companies, any knowledge created from the KM Process first needs to be processed first and then stored into a defined structure. After creating standard documentation at the Knowledge Creation level, E-Commerce companies need to define the structure of the database components. The database component structure means that the knowledge structure is grouped in the form of tacit or explicit knowledge which is then made into a structured form [23]. From the six activities above, all documentation standards were converted into two parts. The first part is explicit, which stores data containing incident data, point of occurrence, impact of incidents, severity of incidents, tools used, and metadata of all existing processes. Then, the second part, which is storing knowledge in tacit form, is the activity of reporting and handling cyber inci-

dents. Tacit knowledge is then externalized into explicit knowledge. That way, these two parts can be stored simultaneously into a structured form for easy processing.

3) Knowledge Sharing

The third KM process is Knowledge Sharing, which determines how knowledge will be distributed or communicated to people within the organization. People in organizations are the main producers and consumers of KM [16]. That way, the organization must prepare the right form in disseminating knowledge. The right form of doing knowledge sharing will determine the level of absorption of that knowledge. If knowledge is not absorbed properly, then the organization does not benefit from KM so that KM fails to become an enabler of organizational development and growth [16].

In this activity, development is focused on ways to distribute knowledge. Since all knowledge has now become explicit knowledge, the dissemination process can be directed into one form. Knowledge that has been stored is incident data, point of occurrence, impact of incidents, severity of incidents, tools used, metadata, and activities of all existing processes made into a knowledge base. In accordance with the opinion of [28], this form was chosen because everything is technical knowledge so that users with a technical background are more adaptive in accessing that knowledge. Therefore, the storage made can be in the form of a single platform which will also make it easier for users to access the knowledge.

4) Knowledge Utilizing

In this activity, the use of knowledge makes KM an appropriate concept. Appropriate in this case because what is intended for the use of this concept can really help work and activities [16]. By setting the KM Goal, every process that is set must meet these targets. It is hoped that the transferred knowledge can be used to carry out Business Process Reengineering, Business Process Opportunity, Business Process Automation, and Business Process Improvement to legacy business processes.

The form of application that can be done to reflect this KM Activity is to make incident diagnostics and incident prevention. Incident diagnostics is a procedure to identify the type of incident and understand the underlying cause [16]. With the incident diagnostics, the current KM Goal can be achieved, namely avoiding repeated incidents because the team already knows the root cause of the previous incident. On the other hand, incident prevention is the development of procedures to avoid incidents that may occur and can handle the same incidents that have been handled before [16]. As a result, incident diagnostic and incident prevention give E-Commerce companies an advantage because it can reduce costs due to cyber incidents by reducing the work of handling cyber incidents and avoiding the risk of an incident.

4.3.2. KM Enablers

KM Enablers consists of 2 parts, namely technology infrastructure and people competency. The following are the activities that must be performed on each

KM Enablers:

1) Technology Infrastructure

Technology infrastructure is important as something that can be a catalyst for the KM Process. With a good technology infrastructure, we can cross the boundaries of space, time, and language. In addition, the use of technology also reduces the cost of production when developing a KM system [16]. When viewed in more detail, information technology is an important pillar in KM development, especially in technology companies. Obviously, technology companies must have qualified technology and the speed to update each new science. With a good technology infrastructure, it is hoped that the organization can go further with the implementation of the KM system.

The form of support from KM Infrastructure in this research is to develop an online knowledge base. Knowledge base as a medium for Knowledge Sharing activities can be supported by preparing reliable supports. Especially when it comes to adapting to changes, E-Commerce companies really need rapid development in managing knowledge. The knowledge exchange process can be faster and better because it is hosted online so that anyone and anywhere on E-Commerce companies can use and store knowledge. In addition, with the E-Commerce company profile located in 3 cities, knowledge synchronization between developers and QA engineers in the three cities can run together. As a result, the organizational development process at E-Commerce companies is getting better and can increase the value of the organization itself [29].

2) People Competency

People's competency is a central point for everyone involved in E-Commerce companies. Everyone's competence is assessed based on their ability to carry out their main tasks [23]. With the support of the right people in the right positions, it is hoped that the organization can achieve its goals easily. In addition, according to the opinion of [14], people are one of the points that are used to measure the competitive level of an organization.

As a technology company, finding the right people, especially in the world of software development, is a challenge E-Commerce companies. Technology companies in Indonesia recruit developers from other companies in Indonesia and are then lured higher salaries due to a lack of supply of competent experts in the field of software development [30]. With this gap, the law of economics also occurs, as a result, companies can lose money due to production costs that are far proportional to the selling price. Therefore, E-Commerce company management decided to develop internal talent in dealing with this.

5. Conclusions

The author finds that there are two gaps between the current condition and the expected condition of E-Commerce. The two gaps are the same thread to be directly reported and handled and no recurring threat management from future cyber attacks. The organization lacks data and procedures for reporting and handling

cyber incidents which makes it minimally directive to make changes for the better. Thus, this condition leads to time and cost losses experienced by E-Commerce because of the focus on strengthening other cyber security [31].

The authors conducted a gap analysis and mapping of the value chain 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 Knowledge Creation, Knowledge Storing, Knowledge Sharing, and Knowledge Utilizing. The KM Enablers are Technology Infrastructure and People 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 directly reported and handled and that there are no repeated cyber incidents in the management and reporting of cyber incidents can be achieved [32].

Concrete actions that can be taken based on the 4 KM Processes and 2 KM Enablers described above are recording standardized knowledge on data, metadata, activities, and tools to create knowledge in the process of managing and reporting cyber incidents. Then, define the structure of the database components to store the knowledge and store the knowledge in a tacit form of all activities in the process. Then, the knowledge is distributed through the knowledge base. Finally, knowledge is made in the form of cyber incident diagnostics and cyber incident prevention.

The next research can examine the KM strategy to create a model in which knowledge can be input from external organizations.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Nugroho, A., Takahashi, M. and Masaya, I. (2021) Village Fund Asymmetric Information in Disaster Management: Evidence from Village Level in Banda Aceh City. *IOP Conference Series*: *Earth and Environmental Science*, **630**, Article ID: 012011. https://doi.org/10.1088/1755-1315/630/1/012011

[2] Sunitha, C.K., and Gnanadhas, E. (2014) Online Shopping—An Overview. *B-DIGEST*, **6**, 16-22.

[3] Reddy, K.V.S., Rajesh, B. and Rao, N.V. (2017) India - Retailing - Destination. 2017 *IEEE 7th International Advance Computing Conference* (*IACC*), Hyderabad, 5-7 January 2017, 939-942. https://doi.org/10.1109/IACC.2017.0191

[4] Deloitte (2014, January) From Bricks to Clicks: Generating Global Growth through eCommerce Expansion. Deloitte Development LLC, Hermitage.

[5] Harahap, D. A. (2018) Perilaku belanja online di indonesia: Studi kasus. *JRMSI*: *Jurnal Riset Manajemen Sains Indonesia*, **9**, 193-213.

[6] Hoisl, K., Stelzer, T. and Biala, S. (2015) Forecasting Technological Discontinuities in the ICT Industry. *Research Policy*, **44**, 522-532. https://doi.org/10.1016/j.respol.2014.10.004

[7] Alrimawi, F., Pasquale, L. and Nuseibeh, B. (2019) On the Automated Management

of Security Incidents in Smart Spaces. *IEEE Access*, **7**, 111513-111527. https://doi.org/10.1109/ACCESS.2019.2934221

[8] Mooi, R.D. and Botha, R.A. (2016) A Management Model for Building a Computer Security Incident Response Capability. *SAIEE Africa Research Journal*, **107**, 78-91. https://doi.org/10.23919/SAIEE.2016.8531544

[9] Nonaka, I. (1994) A Dynamic Theory of Organizational Knowledge Creation. *Organization Science*, **5**, 14-37. https://doi.org/10.1287/orsc.5.1.14

[10] Lin, T.C.W. (2016) Financial Weapons of War. *Minnesota Law Review*, **100**, 1377. Temple University Legal Studies Research Paper No. 2016-25. https://ssrn.com/abstract=2765010

[11] Alotaibi, F. and Alshehri, A. (2020) Gender Differences in Information Security Management. *Journal of Computer and Communications*, **8**, 53-60. https://doi.org/10.4236/jcc.2020.83006

[12] Pratomo, Y. (2020, May 3). Data 91 Juta Pengguna Tokopedia dan 7 Juta Merchant Dilaporkan Dijual di Dark Web. KOMPAS.Com. https://tekno.kompas.com/read/2020/05/03/10203107/data-91-juta-pengguna-tokopedia-dan-7-juta-merchant-dilaporkan-dijual-di-dark?page=all

[13] Razzak, I., Xu, G. and Khan, M.K. (2022) Guest Editorial: Privacy-Preserving Federated Machine Learning Solutions for Enhanced Security of Critical Energy Infrastructures. *IEEE Transactions on Industrial Informatics*, **18**, 3449-3451. https://doi.org/10.1109/TII.2021.3128962

[14] Al Hafidz, M.U. and Sensuse, D.I. (2019) The Effect of Knowledge Management System on Software Development Process with Scrum. 2019 3*rd International Conference on Informatics and Computational Sciences* (*ICICoS*), Semarang, 29-30 October 2019, 1-6. https://doi.org/10.1109/ICICoS48119.2019.8982506

[15] Carayannis, E.G., Grigoroudis, E., Rehman, S.S. and Samarakoon, N. (2021) Ambidextrous Cybersecurity: The Seven Pillars (7Ps) of Cyber Resilience. *IEEE Transactions on Engineering Management*, **68**, 223-234. https://doi.org/10.1109/TEM.2019.2909909

[16] Ouriques, R.A.B., Wnuk, K., Gorschek, T. and Svensson, R.B. (2019) Knowledge Management Strategies and Processes in Agile Software Development: A Systematic Literature Review. *International Journal of Software Engineering and Knowledge Engineering*, **29**, 345-380. https://doi.org/10.1142/S0218194019500153

[17] Schlette, D., Caselli, M. and Pernul, G. (2021) A Comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective. *IEEE Communications Surveys & Tutorials*, **23**, 2525-2556. https://doi.org/10.1109/COMST.2021.3117338

[18] Shameli-Sendi, A., Louafi, H., He, W. and Cheriet, M. (2018) Dynamic Optimal Countermeasure Selection for Intrusion Response System. *IEEE Transactions on Dependable and Secure Computing*, **15**, 755-770. https://doi.org/10.1109/TDSC.2016.2615622

[19] Khan, S.W. (2019) Cyber Security Issues and Challenges in E-Commerce. *Proceedings of* 10*th International Conference on Digital Strategies for Organizational Success*, 5-7 January 2019, 1197-1204. https://doi.org/10.2139/ssrn.3323741

[20] Fawwaz, H.A.A. (2022) E-Commerce Transactions Regulation in Indonesia. *International Journal of Social Science and Human Research*, **5**, 674-679. https://doi.org/10.47191/ijsshr/v5-i2-38

[21] Ioannou, M., Stavrou, E. and Bada, M. (2019) Cybersecurity Culture in Computer Security Incident Response Teams: Investigating Difficulties in Communication and Coordination. 2019 *International Conference on Cyber Security and Protection of*

Digital Services (*Cyber Security*), Oxford, 3-4 June 2019, 1-4. https://doi.org/10.1109/CyberSecPODS.2019.8885240

[22] Wu, Y., Liu, Q., Liao, X., Ji, S., Wang, P., Wang, X., Wu, C. and Li, Z. (2021) Price TAG: Towards Semi-Automatically Discovery Tactics, Techniques and Procedures OF E-Commerce Cyber Threat Intelligence. *IEEE Transactions on Dependable and Secure Computing*. https://doi.org/10.1109/TDSC.2021.3120415

[23] Jinan, R. Hasibuan, S. (2019) Analysis of Knowledge Management Enabler in Knowledge Sharing on R&D Institution Capability. *International Journal of Engineering Research and Advanced Technology*, **5**, 36-42. https://doi.org/10.31695/IJERAT.2019.3495

[24] Etikan, I. and Bala, K. (2017) Combination of Probability Random Sampling Method with Non Probability Random Sampling Method (Sampling versus Sampling Methods). *Biometrics & Biostatistics International Journal*, **5**, 210-213. https://doi.org/10.15406/bbij.2017.05.00148

[25] Becerra-Fernandez, I. and Sabherwal, R. (2015) Knowledge Management Systems and Processes. 2nd Edition, Routledge, Taylor & Francis Group, New York.

[26] Ling, L.S. (2011) Defining Knowledge Management (KM) Activities from Information Communication Technologies (ICTs) Perspective. *IBIMA Publishing Journal of Organizational Knowledge Management*, **2011**, Article ID: 510976.

[27] Gupta, S., Sai Sabitha, A. and Punhani, R. (2019) Cyber Security Threat Intelligence Using Data Mining Techniques and Artificial Intelligence. *International Journal of Recent Technology and Engineering*, **8**, 6133-6140. https://doi.org/10.35940/ijrte.C5675.098319

[28] Herman (2018, November 24) Indonesia Kekurangan Ahli *Coding*. https://www.beritasatu.com/digital/524111/indonesia-kekurangan-ahli-coding

[29] Viswanathan, B. (2020, March) Knowledge Management in Start-Ups to Scale up through Innovations. *The International Journal of Analytical and Experimental Modal Analysis*, **12**, 2184-2195.

[30] Al-Dhaqm, A., Razak, S., Othman, S.H., Choo, K.-K.R., Glisson, W.B., Ali, A., *et al*. (2017) CDBFIP: Common Database Forensic Investigation Processes for Internet of Things. *IEEE Access*, **5**, 24401-24416. https://doi.org/10.1109/ACCESS.2017.2762693

[31] Kovačević, A., Putnik, N. and Tošković, O. (2020) Factors Related to Cyber Security Behavior. *IEEE Access*, **8**, 125140-125148. https://doi.org/10.1109/ACCESS.2020.3007867

[32] Catal, C., Ozcan, A., Donmez, E. and Kasif, A. (2022) Analysis of Cyber Security Knowledge Gaps Based on Cyber Security Body of Knowledge. *Education and Information Technologies*. https://doi.org/10.1007/s10639-022-11261-8