ANALYSIS OF CSIRT SERVICES IN FACING CYBER SECURITY CHALLENGES IN INDONESIA

Muhammad Haidar
Faculty of Computer Science
University of Indonesia
Jakarta, Indonesia
muhammad.haidar92@ui.ac.id

Yudho Giri Sucahyo
Faculty of Computer Science
University of Indonesia
Jakarta, Indonesia
yudho@cs.ui.ac.id

Teddy Sukardi
Chairman
Ikatan Konsultan Teknologi Informasi Indonesia
Bogor, Indonesia
tedsuka@indo.net.id

Arfive Gandhi
Faculty of Computer Science
University of Indonesia
Jakarta, Indonesia
arfive.gandhi@ui.ac.id

2021 4th International Conference on Information and Communications Technology (ICOIACT) | 978-1-6654-3394-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICOIACT53268.2021.9563925

***Abstract*— Along with the rapid development of information technology and supporting several aspects of life, the increase in the use of information technology is directly proportional to the risk of cyber security so that it can cause losses in the form of data theft, data loss/damage, and obstruction of information flow. In handling information technology security. CSIRT (Computer Security Incident Response Team) is an organization or team responsible for receiving, reviewing, and responding to cyber security incident reports and activities. However, since CSIRT was established, the current CSIRT service in Indonesia has not changed much from when it was first launched, only technology and some cyber security attack and defense techniques have changed but the management principles are considered to remain the same. This study aims to analyze the role and services of CSIRT in Indonesia to deal with the threat of cyber-attacks using the Carnegie Mellon University (CMU) framework. The results of this study are recommendations by mapping the results of research against the FIRST framework so that 10 recommendations can be obtained for the implementation of CSIRT services in Indonesia.**

Keywords*— *Incident Response; CSIRT; Carnegie Mellon University Framework; Cyber security

I. INTRODUCTION

The increase in the use of information technology is directly proportional to the risk of cyber security. The progress and dependence of society on information technology creates vulnerabilities when there are attacks on information systems and infrastructure. Such information attacks can cause losses in the form of data theft, data loss/damage, and delays in the flow of information. So that in the current era, it cannot be denied that cyber security attacks are a serious threat that can cause harm to national interests and even the occurrence of instability in a country [1].

According to the Indonesian Internet Service Providers Association (APJII), the penetration of internet users / information technology in Indonesia in the second quarter of 2020 has reached 73.7 percent of the total population of 266.9 million people, which means that there are around 196.7 million people in Indonesia who have used access internet [2]. According to the general chairman of APJII, that the increase in the number of internet users is due to several factors such as broadband infrastructure in Indonesia supported by the Palapa Ring, increasingly massive digital transformation due to distance learning policies and WFH (Work from Home) due to the COVID-19 virus pandemic since March 2020.

The year 2020 itself is the year where people are required to use internet technology as the COVID-19 virus pandemic does not allow people to have direct interaction to each other, so that internet technology is used by the public to interact through cyberspace. Based on the results of Pusopskamsinas BSSN monitoring of Indonesian traffic anomalies in 2020 (1 January 2020 to 31 December 2020) it was found that there were 495,337,202 traffic anomalies that occurred in 2020 [3]. According to data from the report (e-Governance Academy Foundation, 2021), Indonesia currently ranks 77th for the National Cyber security Index. Indonesia's position is lagging behind other ASEAN countries such as Singapore, Malaysia, the Philippines and Thailand [4],

In handling information technology security, there is an Information Security Index (KAMI) which is an application that is used as a tool to assess and evaluate the level of readiness (Completeness and Maturity) of the application of information security based on the criteria of SNI ISO/IEC 27001. One of the factors that determine the value of the US index of 4.1 is information security governance, which has a definition of policies and measures to deal with information security incidents involving violations of law (criminal and civil).

Fig 1. Traffic Anomaly Graph [3]

CSIRT (Computer Security Incident Response Team) is an organization or team responsible for receiving, reviewing and responding to cyber security incident reports and activities. CSIRT itself can be analogized as a fire department, where the fire department has an emergency number that can be contacted if someone finds indications of a fire. Likewise, CSIRTs should have contacts who can be contacted and ready to respond when needed [5].

BSSN is a government institution of the Republic of Indonesia which was established in 2017 where BSSN has the task of implementing cyber security effectively and efficiently by utilizing, developing, and consolidating all elements related to cyber security. determined by the Head of the National Cyber & Crypto Agency in decision no. 56 of 2018 as one of the services that carries out the mission of building, coordinating, collaborating, and operating systems for mitigation, critical management, response and recovery to cyber security incidents. Currently, 17 registered CSIRT organizations have been registered with the Gov-CSIRT Indonesia in Government agencies, both the Central Government and Regional Governments [6] . On the one hand, there is also ID-SIRTII which is a CSIRT body under the auspices of the BSSN which has the task of being a coordination center for CSIRT in Indonesia.

According to the author's interview with Chairman of the Indonesian Information Technology Consultant Association (IKTII), since CSIRT was established 20 years ago, the current CSIRT service in Indonesia seems has not changed much from when it was first launched, only technology and some cyber security attack and defense techniques have changed. The management principles are considered to remain the same.

Based on the facts described in the interviews and the author's findings, it was found that the role of cyber incidents should play a role in dealing with and responding to cyber threat information security incidents. Therefore, it is necessary to analyze the role of CSIRT services in facing the existing cyber security challenges so that the results of the research can be used as a reference for compiling recommendations for implementing CSIRT in Indonesia.

II. Literature Review

A. Cyber security

According to ISO/IEC 27032, cyber security is defined as the preservation or effort to maintain the confidentiality, integrity, and availability of information in cyberspace. Cyberspace according to the Minister of Defense Regulation number 82 of 2014 is a space where communities are connected to each other using networks (such as the internet) to carry out various daily activities.

The three elements of the CIA (Confidentiality, Integrity and Availability) are a framework / model designed as a standard regarding information security in an organization. Confidentiality is an attempt to ensure that information cannot be accessed by unauthorized persons. Integrity is an effort to ensure that information cannot be changed without the authorization given. While the availability (availability) is an effort that information must always be available whenever needed.

B. Computer Security Incident Response Team (CSIRT)

Initialization of CSIRT began in 1988, when an "internet worm" incident occurred which resulted in most systems on the network at that time being compromised and unusable. The recommendation from this incident is that a single point of contact is needed for internet security issues. So, at that time a CERT (Computer Emergency Response Team) was formed [5].

According to Carnegie Mellon University (CMU), CSIRT (Computer Security Incident Response Team) is an organization or team that is responsible for receiving, reviewing and responding to reports and activities of cyber security incidents.

In the Carnegie Mellon Software Engineering Institute document, CSIRT services can be categorized into 3 categories [7]

- Reactive services
- Proactive services
- Security Quality Management Services

Fig 2 CSIRT Services [8]

C. FIRST Framework

FIRST is a global forum for incident response and cyber security teams. Currently FIRST has more than 500 members spread across Africa, America, Asia, Europe, and Oceania.

FIRST's CSIRT Framework is a high-level document that describes in a structured manner the set of cyber security services and related functions that may be provided by the Computer Security Incident Response Team (CSIRT) and other teams that provide incident management related services.

According to (FIRST, 2019), the CSIRT service framework is based on the relationship between 4 key elements including [9]:

a) Service Areas

Service area is a group of services related to aspects with the aim of helping to organize services. In the service areas there are Information security incident management, vulnerability management, situational awareness, knowledge transfer, and information security event management.

b) Services

A service is a recognizable and coherent set of functions that is oriented towards a specific result. Services are defined with the following template:

• Description: which describes the nature of the service

• Purpose: which explains the purpose of the service

• Outcomes: which describe measurable service outcomes

c) Functions

Functions is an activity or series of activities that aim to fulfill certain service objectives. Any functionality may be shared and used in the context of multiple services.

d) Sub-Functions

Sub-Functions are activities or series of activities that aim to fulfill certain goals. Each sub-function may be shared and used in the context of multiple functions and/or services. Sub-functions can be performed optionally or required for one of the functions and/or service.

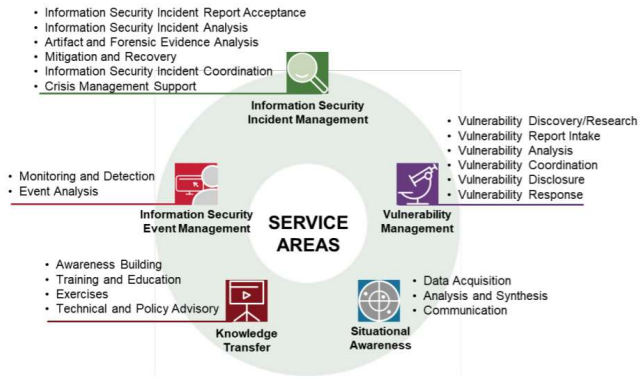

Fig 3 FIRST Framework *[9]*

D. ID-SIRTII

ID-SIRTII/CC provides assistance/assistance to improve security and security systems in strategic agencies/institutions (critical infrastructure) in Indonesia and becomes a coordination center (Coordination Center/CC) for each initiative at home and abroad as well as a single point of contact. Id-SIRTII/CC also conducts research and development in the field of information technology/information system security [3].

With the issuance of Presidential Decree 53 of 2017, the ID-SIRTII/CC function of the Ministry of Communications and Informatics shifted to BSSN. ID-SIRTII/CC is currently integrated in Pusopskamsinas (National Cyber security Operations Center).

BSSN is a government institution of the Republic of Indonesia which was established in 2017 where BSSN has the task of implementing cyber security effectively and efficiently by utilizing, developing, and consolidating all elements related to cyber security. determined by the Head of the National Cyber & Crypto Agency in decision no. 56 of 2018 as one of the services that carries out the mission of building, coordinating, collaborating, and operating systems for mitigation, critical management, response, and recovery to cyber security incidents [10] .

E. Gov-CSIRT

Gov-CSIRT Indonesia is the CSIRT sector of the Government of Indonesia. The organization was first set by the Head of the National Cyber and Crypto Agency in the Decree of the Head of the National Cyber and Crypto Agency Number 570 of 2018 dated December 20, 2018. Meanwhile, in 2019, Gov-CSIRT Indonesia was stipulated through the Decree of the Head of the Head of the Cyber and Crypto Agency [11]. State Code Number 199 of 2019 dated May 21, 2019 Gov-CSIRT Indonesia Constituencies of Gov-CSIRT Indonesia include all Local Governments and Central Governments and provide services that include incident response in the form of: incident triage; incident coordination; and incident resolution. Accompanied by proactive activities in the form of cyber security drill test; workshops or technical guidance; and assistance in establishing a government sector CSIRT [6]. Currently, 17 registered CSIRT organizations have been registered with the Gov-CSIRT Indonesia in Government agencies, both the Central Government and Regional Governments

III. Research Methodology

The conceptual framework in this study uses the CISRT framework methodology issued by Carnegie Mellon University (CMU) so that the conceptual framework for this research can be seen in the figure below.

The research begins by identifying the profile of cyber threats, especially in Indonesia, it can be seen the type of cyber security attack and the target of the attack. The profile of the cyber handling team in Indonesia was then identified so that a gap analysis could be carried out with the CSIRT framework issued by CMU. Information & data collection are done by obtaining primary data and secondary data.

The first stage is to identify the mission statement, position in the organization, relationships with other teams, and constituents on the cyber incident handling team in Indonesia. After that, the service and quality framework are carried out.

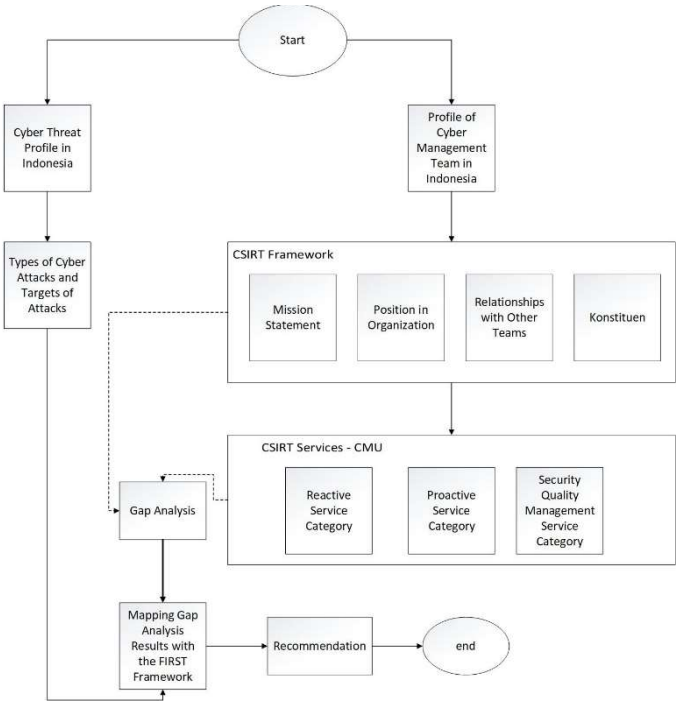

Fig 4 Conceptual Diagram

In the next stage, an analysis of the identification of CSIRT as-is services in Indonesia is carried out which is compared with the framework that has been issued by CMU. CSIRT service categories that are in accordance with the CMU framework include reactive services, proactive services, and service quality management services. After analyzing the existing services, a gap analysis was conducted on whether CSIRTs in Indonesia already had the services recommended by the CMU.

After that, recommendations will be made by mapping the identification results with the CSIRT service framework from FIRST and interviews conducted with expertise in the field of information security.

IV. Result

In this section, the two organizations (ID-SIRTII & Gov-CSIRT) will be analyzed using the CSIRT framework issued by CMU (Carnegie Mellon University) by reviewing the mission statement, constituents, parent organizations and how they relate to other CSIRTs.

A. Cyber security Threat Profile in Indonesia

`According to BSSN, the strategic objectives of the Indonesian Cyber security Strategy are to achieve cyber resilience, public service security, cyber law enforcement, cyber security culture and cyber security in the digital economy. Reported on the BSSN website, cyber security attacks in November 2020 reached 50,194,276 attacks [11]. Especially with the COVID-19 pandemic virus that is not only happening in the world but in Indonesia, which makes people aware of and use the internet for their daily needs. This condition creates an opportunity for hackers to take advantage of existing opportunities to launch cyber security attacks.

Cyber security attacks cases in Indonesia occur in almost all sectors in Indonesia. Several attacks occurred in the government, commercial and academic sectors. Some cases during 2020-2021 are: BPJS personal data leaks which are then traded to sellers in online forums in May 2021, Diponegoro University student data leak on January 2021, Alleged data leak of Kreditplus fintech and free sale on the internet in August 2020, Alleged leak of RedDoorz user data which includes name, e-mail, bcrypt password, profile photo, gender, and mobile phone number in November 2021, The alleged leak of a fintech platform user from Indonesia, Cermati, was reportedly hacked and sold freely in November 2021, Tokopedia & Bukalapak e-commerce user data leaked and reportedly sold on the dark web in May 2020, and Leaked Indonesian permanent voter data from the KPU was shared in the hacker community forum in May 2020

Not only national cases, according to the report (ID-SIRTII/CC, 2020) Indonesia has also been affected by global cyber security cases, such as Coronavirus Ransomware, Covidlock Malware, Border Gateway Protocol (BGP) hacking, vulnerabilities in Draytek Vigor router products, the existence of Remote Code Execution (RCE) on several versions of the Windows operating system product, the vulnerability to Arbitrary Code Execution on all Google Android operating systems, to the exploitation of the SolarWinds Orion Platform product.

B. Profile of Cyber Incident Handling Team in Indonesia

BSSN as a government agency engaged in information security and information security has the responsibility to realize national cyber security, protection, and sovereignty as well as to increase national economic growth. Within the BSSN itself, there are 3 CSIRT teams where ID-SIRTII (Indonesian Security Incident Response Team on Internet Infrastructure/Coordination Center) is the national CSIRT, Gov-CSIRT for government sector CSIRT and BSSN CSIRT for the BSSN Institution itself.

C. Analysis Results of Indonesia's CSIRT Profile with CMU's version of the CSIRT Service

According to CMU, there are 3 types of services that CSIRT can provide to its constituents, namely reactive services, proactive services and security quality management services. The CSIRT services written in the RFC2350 ID-SIRTII document be checked and analyzed whether they already have the CSIRT services recommended by the CMU. This will involve Coding Analysis from the RFC 2350 document to the CMU Framework. The results of the identification in the table below show the services that are not available in each of the existing CSIRT teams. RFC 2350 document is used as the baseline as it provides information about CSIRT, its channels of communication, and its roles and responsibilities.

TABLE I. GAP ON CSIRT SERVICES ACCORDING CMU

Not available on ID-SIRTII / CC	Not available on Gov-CSIRT	Not available in both
A.B.2 Incident response on Site *A.B.3 Incident Response Support* *B.C. Security audit or Assessments* *C.A. Risk Analysis*	*A.D.3 Artifact Response Coordination* *B.B. Technology Watch* *B.E. Development of Security Tools* *B.F. Intrusion Detection Services* *C.B. Business Continuity & Disaster Recovery Planning*	*A.C.2 Vulnerability Response* *A.D.2 Artifact Response* *B.D. Configuration & Maintenance of Security Tools, Applications, & Infrastructures* *C.F. Product Evaluation or Certification*

D. Mapping of identification results with the FIRST Framework

Any services a CSIRT offers, it is important to understand which services are related to each other and what their interdependencies are. It is important for the CSIRT to define the interfaces between services and the associated information flow between services. It is important to identify which services:

• rely on information from, or provide information to, other services

• responsible for providing/requesting information to/from other services

• have a common need for a particular function or set of information

• transfer responsibilities that depend on information (e.g., for confidentiality, appropriate use) to other or external services (other CSIRTs, constituents)

In this section, mapping is carried out from the identification results with the Framework issued by FIRST. Where one part of the CSIRT service has a relationship with one another. The table below is the result of the mapping carried out on the results of the identification needed with the FIRST framework that are relevant to the services needed.

TABLE II. MAPPING CMU RESULTS TO FIRST FRAMEWORK

Gap Identification Results from CMU Checking	Relevant FIRST Framework services
A.B.2 Incident response on Site	*6.4.1 Function: Response plan establishment*
A.B.3 Incident Response Support	
A.D.2 Artifact Response	*6.3 Service: Artifact and forensic evidence analysis*
A.D.3 Artifact Response Coordination	
C.A. Risk Analysis	*9.4 Service: Technical and policy advisory*
C.B. Business Continuity & Disaster Recovery Planning	
B.C. Security audit or Assessments	
B.B. Technology Watch	*8.1 Service: Data acquisition*
B.E. Development of Security Tools	
B.D. Configuration & Maintenance of Security Tools, Applications, & Infrastructures	
A.C.2 Vulnerability Response	*7.6 Service: Vulnerability response*
B.F. Intrusion Detection Services	*5.1 Service: Monitoring and detection*
C.F. Product Evaluation or Certification	*9.3 Service: Exercises*

If the results of the identification of the services needed for each CSIRT team are returned, the table below will be obtained so that recommendations for CSIRT functions and services can be obtained for each service. Each of the organization has their own recommendation taken from FIRST Framework. The recommendation will also be a lesson learned, information and baseline for new CSIRT and any existing CSIRT in Indonesia.

TABLE III RECOMMENDATIONS FOR ID-SIRTII & GOVCSIRT

Required CSIRT Functions and Services Based on FIRST Framework	ID-SIRTII	Gov-CSIRT
6.4.1 Function: Response plan establishment	✓	
6.3 Service: Artifact and forensic evidence analysis	✓	✓
9.4 Service: Technical and policy advisory	✓	✓
8.1 Service: Data acquisition	✓	✓
7.6 Service: Vulnerability response		✓
5.1 Service: Monitoring and detection	✓	✓
9.3 Service: Exercises		✓

E. Recommendations for CSIRT in Indonesia.

As the CSIRT recommendations given to ID-SIRTII and Gov-CSIRT, it was found that in facing the threat of cyber-attacks, Indonesia cannot only rely on 1-2 CSIRTs so that it can be concluded that recommendations for the implementation of CSIRT in Indonesia can be in the form of CSIRT whether organization or sector must operate under a formal policy in order to have a strong legal basis, CSIRT needs to formulate in detail the services provided according to the needs of their constituents, not according to their current capabilities.

a) CSIRT needs to identify services that have not been provided directly by themselves and require assistance from other parties such as external experts or CSIRT above.

b) CSIRT needs to map out the HR competencies needed to support services.

c) CSIRT needs to identify the infrastructure equipment needed to provide services by prioritizing the use of open technology so that it is more free, independent and does not require a lot of cost.

d) CSIRT needs to formulate complete systems and procedures to ensure that operations can run well

e) A national or sector CSIRT should have a mechanism for collecting data on all incidents experienced by its constituents.

f) National or sector CSIRTs should have a knowledge sharing mechanism between CSIRTs so that all CSIRTs can benefit from the information, experience and solutions that already exist.

g) ID-SIRTII as National CSIRT / Country Coordinator should fill the vacancy in sectors that do not yet have their own CSIRT

h) Sectors which do not yet have a sectoral CSIRT in order to accelerate the availability of CSIRTs that can effectively run reactive, proactive service programs and quality management services.

V. Conclusion

In this study, it is concluded that BSSN as a government agency engaged in information security and information security has the responsibility of realizing national cyber security, protection, and sovereignty as well as increasing national economic growth where in BSSN itself has ID-SIRTII and Gov- CSIRT which oversees the CSIRT of the sectors below it. The establishment of every CSIRT must review the mission statement, constituents, parent organization and how it relates to other CSIRTs to have a solid basis for the establishment of a CSIRT and what services the CSIRT provides to its constituents. One thing to be concerned is that a team is considered a CSIRT if it has one or more incident handling services such as incident analysis, on-site incident response, incident response assistance, or incident response coordination. In practice, CSIRT can provide additional services in addition to the main service.

From the findings, that not all CSIRT services recommended by CMU have been implemented in the CSIRT organization in the study so that there is an opportunity for CSIRT to identify the services needed by its constituents and if they do not have these services to fill the void. In addition, one CSIRT service with other services is related to each other by relying on information from, or providing information to, other services, is responsible for providing/requesting information to/from other services, has a common need for certain functions or a certain set of information, transfer responsibility that relies on information (e.g., for confidentiality, appropriate use) to other or external services (other CSIRTs, constituents)

VI. Acknowledgement

This research was supported by PUTI Q2 grant “Digitalisation on Gig Worker: A Manifestation of digital Economy for Indonesia in Industry 4.0 Era” (NKB-1477/ UN2.RST/HKp.05.00/2020). We would express our gratitude to the Faculty of computer Science and directorate of Research and Community Engagement, Universitas Indonesia.

VII. References

[1] R. Gultom, Cyber Warfare, UNHAN Press, 2021.

[2] APJII, "APJII Rilis Hasil Survei Pengguna Internet Indonesia Terbaru," APJII, Jakarta, 2020.

[3] ID-SIRTII/CC, Laporan Tahunan Monitoring Keamanan Siber 2020, Pusat Operasi Keamanan Siber Nasional, 2020.

[4] e-Governance Academy Foundation, "National Cyber Security Index," April 2021. [Online]. Available: https://ncsi.ega.ee/.

[5] M. West Brown, D. Stikvoort and K. Peter Kossakowski, Handbook for Computer Security Incident Response Teams (CSIRTs), 2nd ed., 2003.

[6] BSSN, "GOV-CSIRT Indonesia," 2020. [Online]. Available: https://govcsirt.bssn.go.id/.

[7] Carnegie Mellon University, Organizational Models for Computer Security Incident Response Teams (CSIRTs), 2003.

[8] G. Kilcrece, K. Peter Kossakowski, R. Ruefle and M. Zajicek, Organizational Models for Computer Security Incident Response Teams (CSIRTs), Carnegie Mellon , 2003.

[9] FIRST, Computer Security Incident Response Team (CSIRT) Services Framework, 2019.

[10] BSSN, "TENTANG BSSN," BSSN, [Online]. Available: https://bssn.go.id/tugas-dan-fungsi-bssn/. [Accessed 3 July 2021].

[11] BSSN, Laporan Tahunan Gov-CSIRT, 2019: BSSN, 2019.