Jurnal Pendidikan dan Konseling
Volume 4 Nomor 5 Tahun 2022
E-ISSN: 2685-936X dan P-ISSN: 2685-9351
Universitas Pahlawan Tuanku Tambusai

Improving Computer Security Incident Response Team: Establishment & Operation

Mohammad Rabbani[1], Benfano Soewito[2]
[1,2] BINUS Graduate Program – Master of Computer Science,
Bina Nusantara University, Jakarta, Indonesia
Email : mohammad.rabbani@binus.ac.id[1], bsoewito@binus.edu[2]

Abstrak

Computer Security Incident Response Team (CSIRT) dibentuk sebagai tindakan pencegahan untuk melindungi organisasi dari ancaman siber yang dapat berdampak negatif pada proses bisnisnya, terutama ketika suatu organisasi sangat mengandalkan Teknologi Informasi (TI) untuk mendukung aktivitas bisnisnya. Dengan CSIRT, organisasi dapat merespons dan mengurangi ancaman siber secara sistematis untuk meminimalkan gangguan apa pun yang disebabkan oleh ancaman tersebut. Saat menerapkan CSIRT, ada dua pertanyaan umum, pertama, "Apa yang kita lindungi dengan CSIRT?", Kedua, "Bagaimana kita tahu jika CSIRT kita beroperasi dengan benar?". Untuk memastikan CSIRT mapan & dioperasikan dengan baik, pengukuran perlu dilakukan sebelum & sesudah pembuatan CSIRT.
Kata Kunci: *Aset, Klasifikasi Aset, Ancaman Siber, Postur Keamanan, Tim Merah.*

Abstract

Computer Security Incident Response Team (CSIRT) are established as a countermeasure to protect organisations from cyberthreat that can lead to negative impact on their business process, especially when an 3195rganization are heavily rely on Information Technology (IT) to support their business activities. With CSIRT, organisations can respond and mitigate cyberthreat systematically to minimize any disruption caused by the threat. When deploying a CSIRT, there are two common question, first, “What do we protect with CSIRT?”, second, “How do we know if our CSIRT operate correctly?”. To ensure CSIRT well established & operated, a measurement need to be conducted prior to & subsequent to creation of CSIRT.
Keywords: *Asset, Asset Classification, Cyberthreat, Security Posture, Red Teaming.*

PENDAHULUAN

Nowdays, IT become a heart of enterprise to run their business from complicated things such as the use of web applications to support transaction processes with customers, to simple things such as using email to communicate between internal employees. Thus, the more protocols used, the greater the attack surface will be. Attack surface is a path used by cybercriminals to attack systems within the company and cause a disruption. Specific industries such as financial services is experiencing an increasing volume of cyberattack by 50% in 2020 [1]. Those cyber attack are caused by many various

of type of threats (such as trojan, malware, botnet and etc) and caused various impact to the system (such as unauthorized access, lost of data, performance degradation and etc) [2][3].

This can be challenge for an organization's security posture to ensure protection to their interests and keep all business activity running normally.

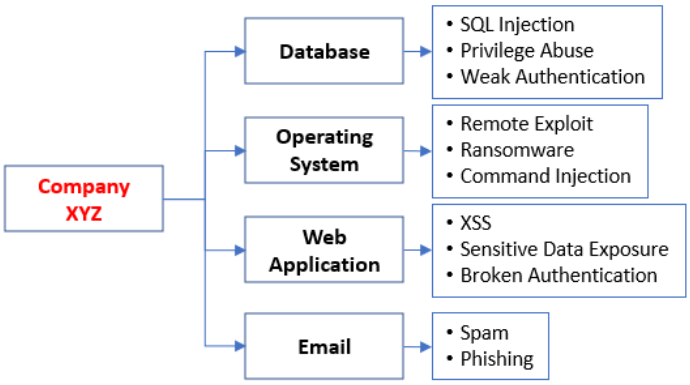

Figure – 1 : Example of Attack Surface

Information security is defined as a state of well-being of information and infrastructure in which the possibility of theft, tampering, and disruption of information and services is kept low or tolerable [4].

There are 3 elements of information security :

1. *Confidentiality :* Confidentiality is the assurance that the information is accessible only to those who are authorized to have access. It plays a major role in securing sensitive information from unauthorized access [4].
2. *Integrity* : Integrity is the trustworthiness of data or resources in the prevention of improper and unauthorized changes [4].
3. *Availability* : Availability is the assurance that the systems responsible for delivering, storing, and processing information are accessible when required by authorized users [4].

Those 3 elements are something that must be considered when protecting an asset. An asset is an entity from which the economic owner can derive a benefit or series of benefits in future accounting periods by holding or using the entity over a period of time, or from which the economic owner has derived a benefit in past periods and is still receiving a benefit in the current period. Because it represents a stock of future benefits, an asset can be regarded as a store of value [5].

Based on their form, assets can be divided into two groups, that is tangible and non-tangible assets. Tangible assets are physical and measurable assets that are used in a company's operations. Assets like property, plant, and equipment, are tangible assets. Tangible assets form the backbone of a company's business by providing the means by which companies produce their goods and services. Tangible assets can be damaged by naturally occurring incidences since they are physical assets [6]. On the other hand, intangible assets are type of assets that can be defined as an identifiable non-monetary asset without physical substance [7]. The value of intangible asset can be are fluctuates and often changes over time.

In context of Information Technology (IT), assets can be simply divided into software and hardware such as computing device, IT network, IT circuit and etc [8]. Each of assets has a specific owner depending how organisastion structure of enterprise defined. IT Assets,

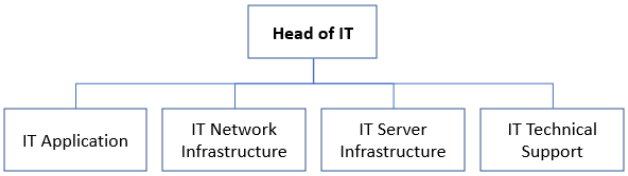

Figure – 2 : Example of IT Organization Structure

TABLE I

EXAMPLE OF GENERAL IT ASSETS CLASSIFICATION ON ENTERPRISE

Common IT Assets	
System Owner	**Assets**
IT Network Infrastructure	Router
	Switch
	IP Phone
	VM Server
	Baremetal Server
	Workstation
	Laptop
	Email Server
IT Server Infrastructure	VM Server
	Baremetal Server
IT Technical Support	Workstation
	Laptop
	Email Server
IT Application	Ticketing System
	Internal Portal
	Internet Banking
	Mobile Banking System

By knowing the detail of asset classification and how many assets there are, it will create better understanding the necessity of building CSIRT, so enterprise can create a result-driven approached to counter cyberthreats [9]. Infact, knowing organisastion's assets is essential and governed by Information Security Management Systems (ISMS) framework on specific control [10].

It is important to keeping all these assets secure and accessible at anytime, failing to do so may lead to potential loss that can harm an organization, for example productivity loss (i.e loss of revenue), reputation loss (i.e loss of market share) and etc [11], but at the same time it doesn't make any sense to invest countermeasure mechanism to protect assets beyond the value of the assets themselves.

By developing CSIRT, an enterprise can expect a better "peace of mind" when running their business while so many cyberthreat are evolving. CSIRT is a continuous work that require people, process and technology to operate, therefore CSIRT operation need to evaluated regularly to ensure their effectiveness to do detection for any possible threats as early as possible [12].

METODE

On this paper, the methodology will start with establishment phase which is done before creating a CSIRT. This phase consist of multiple steps such as CIA rating, assess potential impact and lastly create asset classification of the system. Those first 3 steps is required to identify asset criticality. The last step on this methodology is operation phase, which is done after CSIRT is operating. This phase consist of two steps, started with cyber attack simulation and summarize findings & recommendation. This last phase is executed to find any gaps that may adhere while CSIRT is operating.

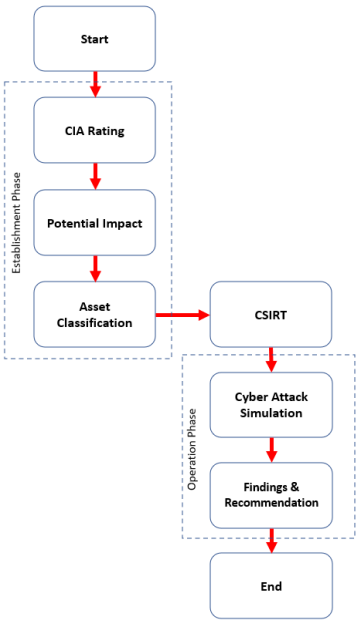

Figure – 3 : Methodology

HASIL DAN PEMBAHASAN

Establishment Phase – CIA Rating

CIA rating is conducted to measure how specific system is behaving in terms of Confidentiality (i.e it carrying sensitive data), Integrity (i.e data are protected from unauthorized changes) and Availability (i.e system must be always accessible). This can vary greatly for every organization (depending type of industries and size), several parameter and rating are should be defined to do severity-based asset classification. This method can be done by creating sets of question for each parameter (Confidentiality, Integrity, Availability), and each question are defined with certain value, for example :

a. 1 = Insignificant
b. 2 = Low
c. 3 = Medium
d. 4 = High
e. 5 = Critical

Each rating of value will be detailed again with more description for better understanding. Example of CIA Rating are detailed below :

TABLE III

EXAMPLE OF CONFIDENTIALITY RATING

Confidentiality Rating		
Component	**Sub-component**	**Description**
Organisation Information (ID = Q1)	Type of Information that stored or processed on the system	Insignificant, if this type of data are rated as public data (information open to the general public, where the security level is minimal) Low, if this type of data are rated as official use only (restricted to who have a legitimate purpose for accessing such data and must be guarded due to proprietary, ethical, or privacy considerations.) Medium, if this type of data are rated as propietary (for authorized personnel only) High, if this type of data are rated as confidential (information are protected by statutes, regulations, organisations policies or contractual agreements) Critical, if this type of data are rated as highly confidential (highly sensitive information whose access is restricted to selected, authorized employees and must be protected all time)

TABLE IIIII

EXAMPLE OF INTEGRITY RATING

Integrity Rating		
Component	**Sub-component**	**Description**
System of Change (ID = I1)	Estimation of system changes performed annualy	Insignificant, if there are no changes need on the system Low, if the number of changes are less than 5 changes. Medium, if the number of changes are between 5 – 9 changes. High, if the number of changes are between 10 – 25 changes. Critical, if the number of changes are more than 25 changes

TABLE IVV

EXAMPLE OF AVAILABILITY RATING

Availability Rating		
Component	**Sub-component**	**Description**
Time Sensitivity (ID = I1)	Specific time needed by the application to run properly	Low, if the application need batch/real-time processing and serving for internal purposes with no Service Level Agreement (SLA) offered by this application Medium, if the application need batch processing and serving for external purposes with Service Level Agreement (SLA) offered by this application

	Critical, if the application need real-time processing and serving for external purposes with Service Level Agreement (SLA) offered by this application

Establishment Phase – Potential Impact

Potential impact is a probaility of risk that may occurred when system are degraded (caused by cyberthreat). This can vary greatly for every organization (depending type of industries and size), several parameter and rating are should be defined to do severity-based asset classification. As previously discussed on CIA rating, this method is also done by creating sets of question for each parameter (i.e Financial Loss, Reputation Loss, etc), and each question are defined with certain value, for example :

TABLE V

EXAMPLE OF POTENTIAL LOSS IMPACT RATING

Potential Loss Impact		
Component	Sub-component	Description
Financial Loss (ID = PL1)	Potential Loss Revenue per day	Low, actual or potential revenue value loss per day is less than $5.000 Medium, actual or potential revenue value loss per day is between $5.000 - $10.000 High, actual or potential revenue value loss per day is between $10.000 - $50.000 Critical, actual or potential revenue value loss per day is more than $50.000

Establishment Phase – Asset Classification

The last method on establishment phase is to do asset classification based on result of last two steps (CIA rating & potential impact), this method categorized the system based on several category that have specific characteristics for each of them :

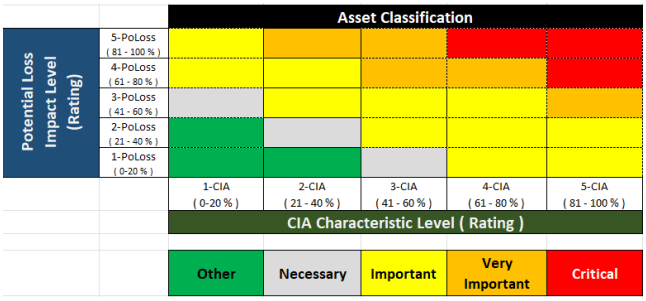

Figure – 4 : Asset Classification Chart

TABLE VI

EXAMPLE OF ASSET CATEGORY CLASSIFICATION

Asset Category	Maximum Tolerable Downtime	Recovery Time Objective	Uptime Ratio per year
Critical	Equal or less than 4 hours	Equal or less than 2 hours	Minimum 99,5%
Very Important	Greater than 4 hours & less than or equal 12 hours	Greater than 2 hours & less than or equal 6 hours	Minimum 99,0%
Important	Greater than 12 hours & less than or equal 24 hours	Greater than 6 hours & less than or equal 12 hours	Minimum 97%
Necessary	Greater than 24hours & less than or equal 48 hours	Greater than 12 hours & less than or equal 24 hours	Minimum 95%
Others	Greater than 48 hours	Greater than 24 hours	Minimum 90%

Operation Phase – Cyber Attack Simulation

This type of security testing is also known as red teaming. Red team is a group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture, their objective is to improve enterprise cybersecurity by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders [15]. Unlike the other form of security testing, Red teaming intend to kept secret from everyone not involved in their organization for their duration, and aim at testing the defense and detection capabilities of the organization [16]. Red teaming can uncover organization's risk by doing various test that can be fully customized based on organization's need, most common ways that red teams assessors go beyond the test such as social engineering, network service exploitation, application exploitation and many more [17].

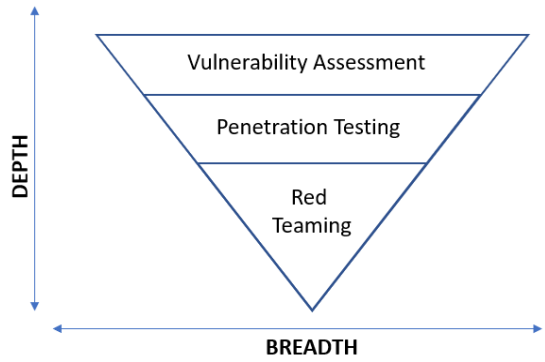

Figure – 5 : Security Testing Method

Despite the various objective that can be defined as a goal for red teaming operation, most of the time the methodology remain the same, it using Cyber Kill Chain framework developed by Lockheed Martin [18].

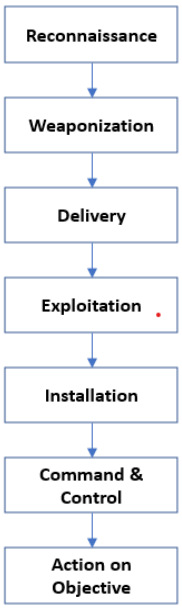

Figure – 6 : Cyber Kill Chain Framework

Cyber Kill Chain is a framework that explains how attackers move through networks to identify vulnerabilities that they can then exploit, this sequential steps consist of 7 steps :

1. *Reconnaissance*

   Reconnaissance is the first stage in the Cyber Kill Chain and involves researching potential targets before carrying out any penetration testing. The reconnaissance stage may include identifying potential targets, finding their vulnerabilities, discovering which third parties are connected to them (and what data they can access), and exploring existing entry points as well as finding new ones [19].

2. *Weaponization*

   In the weaponization stage, all of the attacker's preparatory work culminates in the creation of malware to be used against an identified target. Weaponization can include creating new types of malware or modifying existing tools to use in a cyberattack [19].

3. *Delivery*

   In the delivery stage, cyberweapons and other Cyber Kill Chain tools are used to infiltrate a target's network and reach users. Delivery may involve sending phishing emails containing malware attachments with subject lines that prompt users to click through [19].

4. *Exploitation*

   Exploitation is the stage that follows delivery and weaponization. In the exploitation step of the Cyber Kill Chain, attackers take advantage of the vulnerabilities they have discovered in previous stages to further infiltrate a target's network and achieve their objectives [19].

5. *Installation*

   In this step, cybercriminals may install cyberweapons and malware using Trojan horses, backdoors, or command-line interfaces [19].

6. *Command & Control*

   In the C2 stage of the Cyber Kill Chain, cybercriminals communicate with the malware they've installed onto a target's network to instruct cyberweapons or tools to carry out their objectives [19].

7. *Action on Objectives*

After cybercriminals have developed cyberweapons, installed them onto a target's network, and taken control of their target's network, they begin the final stage of the Cyber Kill Chain: carrying out their cyberattack objectives. While cybercriminals' objectives vary depending on the type of cyberattack, some examples include weaponizing a botnet to interrupt services with a Distributed Denial of Service (DDoS) attack, distributing malware to steal sensitive data from a target organization, and using ransomware as a cyber extortion tool [19].

Various tools are involved depending what steps are currently executed, such as reconnaisance steps will using Shodan, Nmap, Crt.sh to discover potential target, and delivery steps using GoPhish, and so many more [20]. To prepare Red Teaming operation, following information should be defined : *Define red teaming objectives* This objective can be customized depeneding to what systems that they are trying to evaluate, for example if they want to see how secure their active directory systems, then the objective can be defined to take over privilege account belonged to Administrator or Domain Admin group. *Define red teaming entry points* Entry points are also can be customized, whether the attacker came from outside the network such as trying to breach via published wireless SSID, or do social engineering by using phishing email.

Operation Phase – Findings & Recommendations

Systematic approach such as post-incident review are need to be taken to improve overall performance of incident response team [21]. One of them is to generate findings & recommendation after incident happened. Since red teaming are a specific security testing activity, findings and recommendation will be limited to any system that related to the path of attack kill chain related to the defined objective. Therefore, to achieve effectiveness of overall system, the recommendation must also be implemented to other system with the same concept. To be efficiently implemented, recommendation should be divided into two category :

Short-term plan

This type of recommendation has the following characteristics :

a. Require small amount of time (for example less than 3 months)
b. Can used current resource to do the recommendations
c. This type of recommendation is aimed to remediate the findings as soon as possible
d. Most of the time are considered as temporary solution or corrective action

Long-term plan

This type of recommendation has the following characteristics :

a. Require large amount of time (for example multi-years project)
b. New investment required to implement the recommendations
c. This type of recommendation is aimed to create a systematic solution to remediate the findings
d. Most of the time are considered as permanent solution or preventive action

RESULT AND DISCUSSION

Both CIA rating and Potential Loss Impact are must be done to categorize the asset based on Asset Classification Chart. Following example are the results both asset classification based on CIA rating and Potential Loss Impact :

TABLE VII

ASSET X CLASSIFICATION BASED ON CIA RATING

Type of Rating	ID	Value	Sub Rating	CIA Rating
Confidentiality	C1	5	93%	80%
	C2	5		
	C2	4		
Integrity	I1	5	87%	
	I2	4		
	I3	4		
Availability	A1	3	60%	
	A2	3		
	A3	3		

TABLE VVII

ASSET X CLASSIFICATION BASED ON CIA RATING

Type of Rating	ID	Value	Potential Loss Impact
Potential Loss Impact	PL1	5	100%
	PL2	5	
	PL3	5	
	PL4	5	

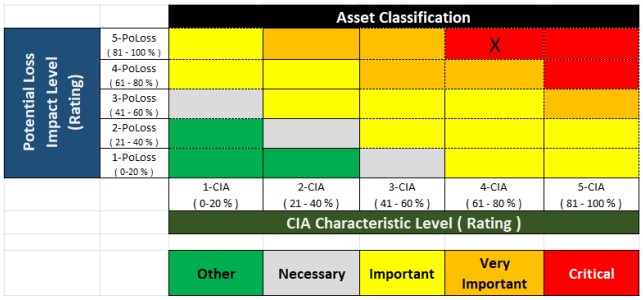

Figure – 7 : Asset Classification Chart for Asset X

TABLE VIX

EXAMPLE OF SCOPE CYBER ATTACK SIMULATION (RED TEAMING)

Objective	Entry Point	Evaluating
Attempt to access critical server & retrieve customer sensitive data	Published Wireless Infrastructure	SSID password policy (length, complexity) Network Segmentation Anti-malware

TABLE X

EXAMPLE OF STEPS OF CYBER ATTACK SIMULATION (RED TEAMING)

Cyber Kill Chain Steps	Results
Reconnaissance	Survey location, discover published SSID, host scanning
Weaponization	Capture Wifi credential using Evil Twin Attack
Delivery	Host Scanning
Exploitation	Wireless cracking, dump hash password using EternalBlue exploit
Installation	PHP backdoor
Command & Control	Create local admin user
Action on Objectives	Access critical server, dumping customer sensitive data

TABLE XI

EXAMPLE OF FINDING & RECOMMENDATION (SHORT-TERM PLAN)

Objective	Status	Recommendation
Attempt to access critical server & retrieve customer sensitive data	Objective Achieved	Implement strong password to all SSID Implement OS Hardening Implement Network Segmentation Implement Active Directory Policy

SIMPULAN

By implementing establishment phase and operation phase, CSIRT are expected to operate more properly in terms of protecting the asset and evaluating CSIRT operation as a whole. This paper are intended to achieve following benefit regarding to CSIRT operation, detail as follows : 1. Before CSIRT creation, system are categorized properly based on their criticality (CIA rating & Potential Loss Impact rating). By doing so, organisations can measure how CSIRT Service Level Agreement (SLA) must be define to assure protection on their asset. 2. After CSIRT creation, by doing cyber attack simulation, CSIRT effectiveness can be measured by deploying specific scenario based on current deployed services on CSIRT. After simulation is done, there are findings and recommendations that should be remediate to improve CSIRT operation.

DAFTAR PUSTAKA

NTT. 2021. Global Threat Intelligence Report
BSSN. (2020). Laporan Tahunan Hasil Monitoring Keamanan Siber.
BSSN. (2021). Laporan Tahunan Hasil Monitoring Keamanan Siber.
EC-Council. 2019. EC-Council Certified Incident Handler Version 2

Harrison, Anne. 2006. Definition of Economic Assets. Fourth meeting of the Advisory Expert Group on National Accounts
Murphy, Chris B. 2022. Tangible Assets vs. Intangible Assets: What's the Difference?. Investopedia
Australian Accounting Standards Board. 2004. Intangible Assets Web Site Costs
NIST. 2018. IT Asset Management. NIST SP 1800-5B
ENISA. 2020. How to Setup CSIRT and SOC
Candiwan. 2014. Analysis of ISO27001 Implementation for Enterprises and SMEs in Indonesia. Proceedings of the International Conference on Cyber- Crime Investigation and Cyber Security, Kuala Lumpur, Malaysia, 50-58.
The Open Group. 2013. Risk Taxonomy
Vielberth, M., Bohm, F., Fichtinger, I., & Pernul, G. (2020). Security Operations Center: A Systematic Study and Open Challenges. *IEEE Access*, 3.
Van der Kleij R, Kleinhuis G and Young H. 2017. Computer Security Incident Response TeamEffectiveness: A Needs Assessment.
M. Ioannou, E. Stavrou and M. Bada. 2019. Cybersecurity Culture in Computer Security Incident Response Teams: Investigating difficulties in communication and coordination. International Conference on Cyber Security and Protection of Digital Services (Cyber Security).
Committee on National Security Systems. 2015. Committee on National Security Systems (CNSS) Glossary. CNSSI No 4009
Kovačević, Ivan & Groš, Stjepan. 2020. Red Teams - Pentesters, APTs, or Neither. 1242-1249. 10.23919/MIPRO48935.2020.9245370.
Synopsys. 2022. https://www.synopsys.com/glossary/what-is-red-teaming.html
Lockheed Martin. 2015. Gaining The Advantage Applying Cyber Kill Chain® Methodology to Network Defense
EC-Council. 2022. https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/
Infosec. (2022). https://resources.infosecinstitute.com /topic/top-tools-for-red-teaming/
Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide (800-61 rev2). *National Institute of Standards and Technology*, 21-44.