Review of Security Principles and Security Functions in Critical Information Infrastructure Protection

Prasetyo Adi Wibowo Putro*, Dana Indra Sensuse

Faculty of Computer Science, Universitas Indonesia, Depok 16424, Indonesia

Corresponding Author Email: prasetyo.adi01@ui.ac.id

https://doi.org/10.18280/ijsse.120406

Received: 18 May 2021
Accepted: 26 June 2022

Keywords: critical information infrastructure, protection, security principle, security function

ABSTRACT

There is quite a lot of research on Critical Information Infrastructure Protection (CIIP), but what threats and vulnerabilities are considered in the security principle offered is unknown. Likewise, the security functions provided have not been measured. This study is a review of CIIP using the Kitchenham framework. From 31 scientific publications and 5 CIIP standards, it was found that there were 13 threats and 16 vulnerabilities were categorized into three security principles. As a result of measuring security functions on CIIP, we found that only 23% provide all security functions.

1. INTRODUCTION

Critical Infrastructure (CI) defines critical infrastructure as essential human-made assets related to energy, communication, and water supply that support continuity and welfare [1]. In order to maintain the continuity of a CI, we must identify and secure the Critical Information Infrastructure (CII) in it [2]. CII is defined differently by several countries [3, 4], but the similarity of these definitions is that this infrastructure is related to CI, the leading security asset. Cybersecurity guidelines define CII as a system provided or operated by CI providers [5]. It is very important to be protecting CII because CI management already uses an electronic system so that CI services depend on CII security.

Currently, many countries have identified existing CII services and categorized them into several sectors [3]. There are five sectors: finance, energy, transportation, water, and food. In addition, some countries add to the defense, technology, and government sectors, but other policies incorporate these fields into other sectors [6]. Several countries have also made CII safeguard policies that consider national risks [7]. However, many have recently identified the CII sector based on national risk and let the CII Protection to the CII service operators according to existing information security standards [8].

Information security standards are different for vital infrastructure than for general infrastructure [9]. Information security standards, better known as Information Security Management Systems (ISMS), focus on business objectives with a custom domain to business processes. Meanwhile, CII Protection (CIIP) security functions, focused on Preventive, Detective, Corrective, Deterrent, Recovery, and Compensation [10].

Some information security incidents occurred on the CII, although national security policies were in place. For example, in September 2020, a hospital in Germany whose database was attacked was forced to refuse emergency patients, resulting in the death of a woman who did not make it to the nearest hospital twenty miles away [11]. Great Britain was also affected by the Ransomware WannaCry attack on many hospitals, resulting in inaccessible medical data and national service providers having to cancel more than 19,000 medical appointments [12]. The two attacks against CI above occurred because CIIP was carried out only by implementing ISMS at the operator level. Therefore, CIIP must pay more attention to threats and impacts on continuity and national welfare [7].

Several international CIIP standards provide a comparison with other standards to show their connectivity capabilities [4, 13]. Review on national standards was also conducted on the CIIP national policy as a form of evaluation in strengthening. In 2009, 20 national and five inter-country CIIP policies were reviewed [3]. The result shows similarity between the CIIP security principles and the CI strategic sectors. Despite the international CIIP standard, there is still a large CIIP gap between developed and developing countries [14]. CI with inadequate protection and unstructured protection often becomes a zombie to carry out attacks. [15].

Strengthening CIIP can also be done using research results. There is quite a lot of research on CIIP published on three reputable scientific journals in information infrastructure [16]. A review of critical information infrastructure has also been carried out specifically on the security assessment method for industrial control systems [17]. Similar research specifically reviews the measurement of risk in strategic industries [18]. However, based on the reviews conducted [19], research on CIIP has not met Reliability, Availability, Maintainability, and Safety/Security parameters (RAMS). As a part of information security, it is also necessary to know whether CIIP have the same security principles with information security.

The Security Principle is a must-have trait in information security [20]. These traits can be lost due to threats or vulnerabilities. Therefore, information security principles are often used to classify threats and vulnerabilities. Common security principles namely confidentiality, integrity, and availability [10]. No one is more important than the other in these three principles. In fact, this principle can be added by other properties according to the needs of the organization.

This research is a literature review of scientific articles and
standards in CIIP based on information security principles and functions. The results of this review are expected to provide information on security principles and security functions that have so far been considered problematic. Threats and vulnerabilities are looked at for each literature and then grouped according to information security principles. Threats, vulnerabilities, and security functions in each literature, is used to describe relationship between security principles and security functions in CIIP.

This article will be organized as follows: Chapter 1 will explain the motivation, problems, and research contributions. The review methodology will be explained in Chapter 2. Chapter 3 will explain the results from each literature and discuss the findings in Chapter 4. In the end, Chapter 5 will answer the research questions, limitations, and further research.

2. METHODOLOGY

Review in this study used Kitchenam’s Systematic Literature Review (SLR) protocol [21]. SLR is a literature study method that identifies, assesses, and interprets findings on a research topic to answer predetermined research questions [22]. Although The Kitchenham protocol has not provided methods for synthesizing/analyzing findings, this protocol is considered ideal for describing security functions and classifying threats and vulnerabilities into security principles [23].

2.1 Specify research questions

To answer the research problem as previously described, two research questions were made as follow:

RQ1: What is the security principle of Critical Information Infrastructure?

RQ2: Is the security model that fulfills the Critical Information Infrastructure Security function?

2.2 Develop review protocol

The preparation of the research protocol began by compiling the research aspects and describing them into Population, Intervention, Comparison Outcomes, and Context (PICOC) as in Table 1. Based on the PICOC aspects, the SLR protocol was compiled as in Table 2. Five publication databases were selected according to the availability of accessing the full articles on those databases. Search string are arranged based on the PICOC aspect and added with the * character to accommodate variations in word writing in the search sentence. Because information security is a dynamic technology suited to the newest attacks and vulnerabilities, the publication was selected from international conference proceedings and journals with an index of Q1 to Q3 from 2016 until 2020.

<table>
<thead>
<tr>
<th>Table 1. PICOC aspect of the research</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aspect</td>
</tr>
<tr>
<td>Population</td>
</tr>
<tr>
<td>Intervention</td>
</tr>
<tr>
<td>Comparison</td>
</tr>
<tr>
<td>Outcome</td>
</tr>
<tr>
<td>Context</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 2. SLR protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rules</td>
</tr>
<tr>
<td>Keywords</td>
</tr>
<tr>
<td>Database</td>
</tr>
<tr>
<td>Search string</td>
</tr>
<tr>
<td>Inclusion Criteria</td>
</tr>
<tr>
<td>Exclusion Criteria</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

2.3 Validate SLR protocol

The SLR protocol in Table 2 is the validated protocol that used in this study. Protocol validation was carried out through discussion between the authors and consultation with those familiar with CCIP. At this validation stage, the SLR protocol was revised twice. The protocol was first tested in the IEEE Xplore database to determine search sentences according to the scope of the search results. Furthermore, the Complete protocol was made, and the literature obtained was consulted, and the latest version of the SLR protocol was obtained from the second improvement.

3. RESULT

The SLR results are a series of identifying relevant research
processes to extract required data. The selected literature is obtained from the identification stage of relevant research to assess the quality of the research, as shown in Figure 2. These results will be extracted and become the basis for synthesis.

3.1 Identify relevant research

This stage is carried out by searching based on the search sentences that have been compiled. The search sentence must be adjusted for searches on the Science Direct database because it cannot process star characters (*).

3.2 Select primary study

A selection is carried out at this stage based on inclusive exclusive criteria, as listed in Table 2. This stage also eliminates the duplication of publications because they appear in several databases. The primary study was selected by looking at the publication metadata, including abstracts and references. Snowball analysis was also conducted to identify new literature based on references. The results of the Snowball analysis continued to use the same inclusive and exclusive criteria as the SLR protocol.

![Figure 2. Literature selection process](image)

3.3 Access study quality

The literature quality assessment is carried out based on the questions as in Table 3. Literature that is declared quality is literature that meets all the existing criteria. Based on the reference list in selected literature, five international standards for information security were identified. National policies on safeguards are not included in the primary literature because not all national policies on CIIP are published in full. Based on the SLR stages carried out, 36 pieces of literature consisting of 31 scientific articles and five international CIIP standards have been obtained.

![Table 3. List of quality assessment questions](image)

3.4 Data extraction

Data extraction was carried out for 25 scientific articles that had passed the quality test and 5 CIIP standards. The 30 pieces of literature are grouped according to the strategic sectors discussed, referring to the division of 9 strategic sectors [8] as shown in Table 4. The nine strategic sectors are government, energy and mineral resources, transportation, finance and banking, health technology and telecommunications, defense, food, and strategic industries. After data extraction, six scientific articles were found that did not specifically describe the strategic sector under study. One generic sector is added for literature that does not explicitly mention the strategic sector understudy.

From the reviewed literature, we find that many threats are considered in CIIP. Each researcher uses their terminology. If we use terminology based on the literature obtained, the CIIP threats are mostly about Cyber-attacks [24-32]. This cyber-attack can be in the form of DDoS on the Power Grid [24], Web attack [31], or attack the point of Sale (POS) [30]. Apart from cyberattacks, there are also External attacks [33, 34], Insider Threat [35, 36], Unauthorized Access [37, 38], Targeted attacks [39, 40], Hybrid Threats [41], Hazardous Event [42], Nature Disasters [43], Social Engineering [44], Falsification Attacks [45], Breach Attack [46], Data Theft [47], and Data Tampering [48] commonly found in CIIP.

![Table 4. Data extraction](image)

If we quote directly from the literature, vulnerability also has many terms. Many CIIPs have Poor Interoperability vulnerabilities [24-28, 33, 55]. There is a lack of connection between CII managers, so it is necessary to control safeguards to avoid risks. Other vulnerabilities found in the literature are Misconfigured Security Control [32, 37, 47], Collaborative Systems [38, 52], Financial Vulnerability [30, 31], Operator Mistakes [35, 44], Lack Traceability [48, 54], Unsecure Framework [53], Internal Turmoil [34], Unresolved Risk [42], Unknown Machine Failure [43], Manual Negotiation of Access Control [49], IoT Interconnection [45], Insecure Communication Technology [46], No Defense In-Depth [36], Sensor Misconfiguration [29], and Design Vulnerability [39]. Meanwhile, to identify CIIP needs, the theory of six security functions is used, namely Preventive, Detective, Corrective, Deterrent, Recovery, and Compensation. The security function is also not fully accommodated in the literature reviewed. Only research in the government sector [26-28, 33], strategic industry [32], dan generic [8, 37, 56] found a security model with complete security functions. In addition, CIIP standards also accommodate all security functions.

4. DISCUSSION

4.1 Threat and vulnerability on critical information infrastructure protection

Several threats and vulnerabilities found in CIIP are similar,
such as cyber-attack, web attack, targeted attack, breach attack, and point of sale attack. Therefore, the classification of threats and vulnerabilities uses the Security Principles. Security principles are used to identify security issues discussed in the literature, namely confidentiality, necessity, and availability.

If each threat and vulnerability are grouped on the security principle, it turns out that the most threats and vulnerabilities are in availability, as shown in Table 5. A total of 35 of the 36-literature reviewed identified availability as a risk that needs to be considered for CIIP. In addition, 21 CIIP models were made by considering all Security Principles. In addition to this, the principle of confidentiality has not been much considered in creating the CIIP model. If we analyze further using Table 4 and Table 5, we find that the principle of confidentiality is not yet considered in the Energy and Natural Resources, Food, and Strategic Industries sectors. This happens because this sector prioritizes service availability so that other security principles, such as confidentiality, will adjust to availability needs.

To support the security function, all three security principles must be met. From the existing literature, there are 21 literatures that accommodate all security principles. The three security principles are only found in the literature [24-28, 30, 31, 33, 35, 37, 41, 42, 50-53]. Whereas for literature in the form of CIIP standards [4, 8, 13, 56], all of them have met the security principle. This means that it is expected that later 58.33% of the CIIP model can fulfill all security functions.

**Table 5. Security principle of critical information infrastructure protection**

<table>
<thead>
<tr>
<th>Security Principle</th>
<th>Related Literature</th>
<th>Sum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>[4, 8, 13, 24-28, 30, 31, 33-37, 41, 42, 47, 50-53, 56]</td>
<td>23</td>
</tr>
<tr>
<td>Integrity</td>
<td>[4, 8, 13, 24-29, 30-35, 37 39, 41-56]</td>
<td>33</td>
</tr>
<tr>
<td>Availability</td>
<td>[4, 8, 13, 24-34, 36-56]</td>
<td>35</td>
</tr>
</tbody>
</table>

**4.2 Security function on critical information infrastructure protection**

The existing CIIP model is more focused on the Preventive function. Based on the reviewed literature, as shown in Table 6, the Preventive security function is the most accommodated, followed by Compensation, which is also an alternative to the preventive function. This condition is quite reasonable considering that CII is a strategic sector where it is hoped that risks will never occur so that the function of prevention is prioritized. However, it is unfortunate that only nine pieces of literature, or 25% of the total literature, provide a complete Security Function.

**Table 6. Security function on critical information infrastructure protection**

<table>
<thead>
<tr>
<th>Security Function</th>
<th>Related Literature</th>
<th>Sum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preventive</td>
<td>[4, 8, 13, 25-38, 41, 43-56]</td>
<td>33</td>
</tr>
<tr>
<td>Detective</td>
<td>[4, 8, 13, 24, 26-33, 36, 37, 39, 40, 45-47, 53, 55, 56]</td>
<td>22</td>
</tr>
<tr>
<td>Corrective</td>
<td>[4, 8, 13, 26-28, 32, 33, 37, 45, 47, 55, 56]</td>
<td>13</td>
</tr>
<tr>
<td>Deterrent</td>
<td>[4, 8, 13, 26-28, 32, 36-38, 41, 47, 50-53, 56]</td>
<td>17</td>
</tr>
<tr>
<td>Recovery</td>
<td>[4, 8, 26-28, 32, 33, 37, 47, 55, 56]</td>
<td>11</td>
</tr>
</tbody>
</table>

The sum of security functions that CIIP accommodates is too small if we compare it with all of literature that meets security principles. For example, suppose 21 CIIP models fulfill all security principles. In that case, there should also be 21 security models that provide security functions because the principles of confidentiality, integrity, and availability should be sufficient to provide all security functions. Furthermore, the security controls used in CIIP, such as encryption, access control, digital signature, hash function, and detection systems, are not a type of security control that counter other security functions.

It turns out that the CIIP standard also has a security function gap. For example, the financial security standard (PCI DSS) does not accommodate the detective, corrective, and recovery functions. Likewise, the generic security standard (CIS) did not provide a recovery function. Nevertheless, it is possible to present these security functions because several scientific articles on the sector can provide this function.

Based on the identification of security principles and security functions, the relationship among can be described in Figure 3. Based on the literature review carried out, it turns out that confidentiality has no impact on the security function. Although no principle of confidentiality was considered, security function preventive [29, 32, 38, 43-46, 48, 49, 54, 55], detective [32, 39, 40, 45, 46, 55], corrective [32, 45, 55], deterrent [32, 38], recovery [32, 55] and compensation [29, 32, 38, 45, 46, 48, 54, 55] were found. This condition is different from Integrity which has correlation with corrective and recovery, and Availability with its correlation to all security function.

![Figure 3. Relationship between security principles and security functions](image)

**5. CONCLUSION**

There were 13 threats and 16 vulnerabilities considered for the CIIP model. If we classify the threats and vulnerabilities according to the Security Principle, we get it 58.33% of the security models have considered the principles of confidentiality, integrity, and availability. Although quite much of the security model considers the whole security principle, it turns out that only 25% of the CIIP security model fulfills the Critical Information Infrastructure Security function. Most security models still focus on the Preventive function, with availability as the primary security principle.
The relationship between security principles and security functions has also been identified based on the literature obtained. For further study, this relation offered can be reviewed with more literature or an information security perspective. For example, a new model that complements the standard can be proposed, which does not yet provide a complete security function. Further research can also be carried out by identifying model in CIIP.

ACKNOWLEDGMENT

I would like to thank Indonesia Endowment Fund for Education (LPDP) from the Ministry of Finance Republic Indonesia for granting the scholarship and supporting this research. This research was supported by E-Government and E-Business Laboratory, Faculty of Computer Science, Universitas Indonesia.

REFERENCES


