# A Study on Evaluation Items and Indicators for Ensuring Cyber Resilience

Sooyon Seo[1], Jaeho Hwang[1], Minseok Hur[1], Dongmin Kim[2], Sechan Lee[3], and Moohong Min[4]

[1] Department of Immersive Media Engineering, Sungkyunkwan University, Seoul, Republic of Korea
{sooyon1119, ashiereki, alexhur3535}@skku.edu
[2] Department of Data Science, Sungkyunkwan University, Seoul, Republic of Korea
ehdals5744@g.skku.edu
[3] Department of Computer Education, Sungkyunkwan University, Seoul, Republic of Korea
chan1031@g.skku.edu
[4] Department of Computer Education/Social Innovation Convergence Program, Sungkyunkwan University, Seoul, Republic of Korea
iceo@skku.edu

**Abstract**

This study focuses on developing evaluation items and indicators to enhance cyber resilience. As cyberattacks become increasingly sophisticated and frequent, ensuring system resilience beyond traditional security measures is essential for organizations. The study analyzes the fundamental components of cyber resilience, along with global examples and frameworks, to propose step-by-step evaluation items for policy formulation, priority identification, threat anticipation, system resistance, rapid recovery, and continuous learning and evolving. This approach provides a foundation for organizations to ensure business continuity and effectively respond to cyber threats.

**Keywords**: Cyber Resilience, Evaluation Items, Evaluation Indicators

## 1 Introduction

Cyberspace, composed of various hardware and software within computer networks, has rapidly expanded in connectivity and openness, leading to an exponentially complex structure. This complexity introduces numerous security vulnerabilities that can be easily exploited by malicious attackers. The recent advancements in innovative technologies such as artificial intelligence and the expansion of digital asset transactions have further escalated cyberattacks.

Cyberattacks occur across various domains and in multiple forms, leading to diverse research areas. For instance, studies have been conducted on Distributed Denial of Service (DDOS) attacks in networks and wireless networks[26, 28], False Data Injection Attacks (FDIA) in power systems and smart grids[13, 18], ransomware attacks in finance[12], zero-day attacks in software development[27], black hole & grey hole attacks in healthcare[24], and actuator or authentication & availability attacks in manufacturing[17, 14].

However, as cyberattacks become increasingly sophisticated and frequent, it is practically impossible to completely block and prevent these threats. Therefore, it is crucial for organizations not only to develop the capability to respond to these threats but also to ensure system survivability and rapid recovery post-attack. This is where the importance of cyber resilience comes into play. Cyber resilience goes beyond merely strengthening system security; it encompasses the ability to maintain business continuity by responding swiftly, minimizing damage, and recovering quickly when a cyberattack occurs.

The 2017 WannaCry ransomware attack crippled hundreds of organizations worldwide, including the UK's National Health Service (NHS)[25]. The lack of cyber resilience led to prolonged recovery times due to inadequate backup systems and recovery plans, resulting in significant operational disruptions and economic losses[7]. In contrast, organizations with strong cyber resilience strategies, such as the global shipping group Maersk, were able to recover their entire IT infrastructure within 10 days following a similar attack by the NotPetya ransomware[1]. This demonstrates the necessity for organizations to strengthen their cyber resilience in preparation for potential cyberattacks.

Given its critical role in organizational survival, this study aims to propose evaluation items and indicators for ensuring cyber resilience. The research will begin by exploring the definition of cyber resilience and examining the policy trends of leading countries. It will then analyze the components that need to be considered for developing cyber resilience evaluation items and assess the frameworks of global institutions. Based on this analysis, the study will present new evaluation items and indicators for cyber resilience.

# 2 Background

## 2.1 Cyber Resilience

The concept of cyber resilience integrates the traditional notion of resilience, commonly used in ecological, biological, and sociological contexts, into the realm of cyberspace. It was developed to address various elements that pose threats in cyberspace. The increasing frequency of cyber incidents and rapid technological changes have highlighted the necessity for cyber resilience, prompting various organizations to define the term[11].

In this study, we adopt the definition provided by the National Institute of Standards and Technology (NIST), which defines cyber resilience as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources[23]." This definition serves as the foundation for our research on evaluating and enhancing cyber resilience.

## 2.2 Policy Trends in Major Countries Related to Cyber Resilience

### 2.2.1 United States

The U.S. cybersecurity policy is led by the President, with the Office of the National Cyber Director (ONCD) developing cybersecurity strategies and implementation plans under the supervision of the National Security Council (NSC), in collaboration with the Office of Management and Budget (OMB)[9]. The Office of Science and Technology Policy (OSTP) focuses on enhancing the international competitiveness of cybersecurity technologies and mitigating critical risks. The Cybersecurity and Infrastructure Security Agency (CISA) is responsible for cyber defense, critical infrastructure security, and resilience[6].

The U.S. government's cybersecurity policy is driven by the "Interim National Security Strategic Guidance" released on March 3, 2021, and further detailed in the "National Cybersecurity Strategy," which outlines specific requirements for policy development, implementation, and review to manage threats effectively[10]. A key focus is on ensuring rapid resilience in the event of failures within cybersecurity defenses. Research and development (R&D) priorities align with this direction, emphasizing resilient and secure communications, as well as the protection of critical infrastructure and sensitive networks from cyber and supply chain attacks[16].

In support of these national security-level cyber strategies, the U.S. administration, for the first time since the establishment of CISA in 2018, has introduced the "CISA Strategic Plan 2023-2025," which serves as a milestone in the agency's mission and the enhancement of national cybersecurity over the next three years.

### 2.2.2 European Union (EU)

The EU's cybersecurity policy is led by the President of the European Commission, who is responsible for making policy decisions. The European Union Agency for Cybersecurity (ENISA) develops a pan-European cybersecurity strategy based on these decisions. The European Cybersecurity Center (Computer Emergency Response Team-EU, CERT-EU) is tasked with responding to cyberattacks and ensuring the security and resilience of critical infrastructure[16, 19].

The EU emphasizes corporate and organizational cybersecurity accountability, product security, reliability, and cyber resilience[15]. In line with this, the EU has introduced the Cyber Resilience Act, which imposes cybersecurity obligations throughout the entire lifecycle of products with digital elements, including planning, design, development, production, delivery, and maintenance[5]. This legislative direction underscores the EU's focus on integrating cyber resilience as a core concept within its broader digital and cybersecurity policies.

### 2.2.3 Japan

Japan's cybersecurity policy is led by the Prime Minister, under whom the Cybersecurity Strategic Headquarters is established and operated. The National center of Incident readiness and Strategy for Cybersecurity (NISC) acts as the secretariat, supporting operations through the Government Security Operation Coordination team (GSOC) and the Cyber Incident Mobile Assistance Team (CIMAT). The Strategic Headquarters collaborates closely with the National Security Council (NSC) and the Digital Agency, which is advancing digital transformation policies[16, 3].

In 2021, Japan revised its cybersecurity strategy to simultaneously advance digital transformation and cybersecurity, ensuring overall safety and security in cyberspace while strengthening national security[2]. The updated strategy focuses on enhancing incident response systems, risk management, and protective infrastructure. It emphasizes the proactive and autonomous efforts of critical infrastructure operators in ensuring cybersecurity[8]. Additionally, Japan is expanding the concept of cyber resilience by assessing the risks posed by asset breaches during cyberattacks and introducing zero-trust-based authentication systems for high-risk cloud services.

## 3 Methodology

In this chapter, we examine the key components necessary for developing a systematic evaluation framework for cyber resilience and analyze the cyber resilience frameworks established by global institutions. The components include the goals, objectives, techniques, and implementation methods of cyber resilience. These components and international frameworks serve as critical reference points for establishing effective evaluation criteria and deriving actionable indicators for assessing cyber resilience.

## 3.1 Analysis of Cyber Resilience Components

### 3.1.1 Goals of Cyber Resilience

The goal of cyber resilience is to manage risks at the organizational, business process, and system levels while strengthening the organization's risk management strategy. This involves selecting factors that will be used to analyze threats related to cyber risks, prioritize and interpret strategies or missions, and set critical objectives at both the business process and system levels to achieve cyber resilience.

Given that this study proposes evaluation items specifically for cyber resilience within the context of information technology, we have derived the goals of cyber resilience based on the "Developing Cyber-Resilient Systems" framework provided by NIST[23].

| Goal | Description |
|---|---|
| Anticipate | Strategies for anticipating threats in advance to shift to proactive cyber defense, including planning, preparation, changes, and identification. |
| Withstand | Strategies for enduring potential threats, even when not yet detected, such as absorption, substitution, and discarding. |
| Recover | Strategies for swiftly resuming critical functions after a cyberattack, including restoration, reconfiguration, and substitution. |
| Adapt | Strategies for improving and adapting vulnerabilities to prevent reoccurrence of attacks, including correction, reinforcement, and restructuring. |

Table 1: Goals of Cyber Resilience

### 3.1.2 Objectives of Cyber Resilience

The objectives of cyber resilience are about what must be achieved throughout the lifecycle that ensures the organization's mission and meets the needs of resilience-related participants. Based on this setting, we considered the following points while specifying the objectives based on the "Developing Cyber-Resilient Systems" framework provided by NIST[23]:

- What does each cyber resilience objective mean in the context of ensuring the organization's mission?
- Which cyber resilience objective is the most critical to the participants?
- To what extent can each objective be achieved?
- How quickly and cost-effectively can each objective be achieved?
- To what level of reliability can each objective be accomplished?

Taken all together, we derived the objectives of cyber resilience as shown in Table 2.

| Objective | Description |
|---|---|
| Prevent or Avoid | Eliminate the successful execution of threats or the realization of adverse conditions. |
| Prepare | Maintain a set of realistic actions to address anticipated threat activities. |
| Continue | Maximize the continuity and survivability of essential missions and business functions despite the presence of threats. |
| Constrain | Limit the damage from attacks. |
| Reconstitute | Restore as many missions or business functions as possible after an attack. |
| Understand | Maintain awareness of business dependencies and resource status concerning potential adversary attacks. |
| Transform | Modify missions or business functions and processes to handle and resolve threats more effectively. |
| Re-architect | Restructure to more effectively address environmental changes. |

Table 2: Objectives of Cyber Resilience

#### 3.1.3 Techniques and Approaches of Cyber Resilience

The techniques and approaches of cyber resilience provide the means by which a system can achieve the goals and objectives of cyber resilience. Cyber resilience techniques are a collection of practices and skills intended to deliver resilience-related functions, thereby helping to achieve one or more goals and objectives. Key techniques include:

- `Adaptive Response` – Implement flexible actions to manage risks.
- `Analytic Monitoring` – Monitor and analyze a wide range of characteristics and behaviors methodically.
- `Contextual Awareness` – Develop and maintain mission or business functions while considering threat events and actions.
- `Coordinated Protection` – Ensure protective mechanisms operate in an organized and effective manner.
- `Deception` – Confuse adversaries, hide critical assets, and expose manipulated assets.
- `Diversity` – Use heterogeneous elements to minimize events that exploit common vulnerabilities.
- `Dynamic Positioning` – Distribute and dynamically relocate functions and system resources.
- `Non-Persistence` – Create and maintain resources temporarily or as needed.
- `Privilege Restriction` – Limit privileges based on environmental factors and attributes of users and system elements.
- `Realignment` – Structure the use of systems and resources to meet mission and business needs, reduce current and anticipated risks, and adapt to changes in technical, operational, and threat environments.

- `Redundancy` – Provide multiple protected instances of critical resources.
- `Segmentation` – Define and separate system elements based on importance and reliability.
- `Substantiated Integrity` – Verify that critical system elements are not compromised.
- `Unpredictability` – Introduce random changes to prevent predictability.

## 3.2 Analysis of Cyber Resilience Frameworks by Global Institutions

### 3.2.1 CISA

CISA conducts security and resilience assessments for critical infrastructure in the United States. CISA provides a framework for infrastructure resilience planning, which helps to better understand threats to critical infrastructure, identify opportunities to enhance resilience, and guide policy and investment decisions[4]. This framework not only addresses ICT infrastructure but also extends to a broad range of national infrastructure, including government facilities, defense industrial bases, and transportation systems.

| Evaluation Items | Description |
|---|---|
| Foundation Establishment | Define resilience planning tasks, determine scope, and review resources. |
| Identification of Critical Infrastructure | Identify and assess critical infrastructure and dependencies. |
| Risk Assessment | Evaluate threats and vulnerabilities related to risks. |
| Action Development | Develop implementation plans to address risks and enhance resilience. |
| Implementation and Evaluation | Measure success based on the implementation of infrastructure resilience. |

Table 3: CISA Infrastructure Resilience Planning Framework

### 3.2.2 CPMI

The Committee on Payments and Market Infrastructures (CPMI), a committee under the Bank for International Settlements (BIS), released cyber resilience guidance in 2016 aimed at enhancing cyber resilience. This guidance is based on the Principles for Financial Market Infrastructures (PFMI) and provides detailed recommendations on measures to ensure operational resilience against cyberattacks and how to assess their effectiveness[22].

The governance framework is structured into five main management items and three supporting items, emphasizing the need for enhanced collaboration between financial authorities, financial institutions, IT firms, and investigative bodies. This framework is managed by a specialized cyber resilience evaluation group under CPMI, and it continues to evolve through regular evaluations, reviews, and confirmations by various countries[21].

| Evaluation Items | Description |
|---|---|
| Governance | Establishing a decision-making framework for cyber resilience. |
| Identification | Measuring risk levels through assessments of critical and external risks. |
| Protection | Ensuring confidentiality, integrity, availability, and protection measures are in place. |
| Detection | Rapidly identifying and detecting potential threat factors. |
| Response and Recovery | Restoring and resuming services based on business continuity planning. |
| Testing * | Assessing vulnerabilities based on scenarios for the five main items. |
| Situational Awareness * | Developing response measures for various attacks and sharing information with participants. |
| Learning and Evolving * | Promoting continuous improvement of preventive capabilities and the governance framework. |

** supporting items*

Table 4: CPMI Cyber Resilience Governance Framework

### 3.2.3 NIST

Since 2013, NIST has been developing and updating a framework for managing cybersecurity-related threats, which includes standards, guidelines, and best practices. NIST's framework is widely recognized as a benchmark for evaluating cybersecurity measures. It provides essential methodologies for protecting critical infrastructure and enhancing resilience.

The NIST cybersecurity framework consists of six primary evaluation items, which are further divided into 22 categories. These categories encompass a total of 106 subcategories, each detailing cybersecurity outcomes and security controls[20].

| Evaluation Items | Description |
|---|---|
| Govern | The organization's cybersecurity risk management strategy, expectations, and policy are established. |
| Identify | The organization's current cybersecurity risks are understood. |
| Protect | Measure risk levels through evaluations of critical and external risks. |
| Detect | Implement measures to ensure confidentiality, integrity, availability, and protection, along with detection mechanisms. |
| Respond | Swiftly identify and respond potential threat factors. |
| Recover | Restore and resume services based on business continuity planning. |

Table 5: NIST Cybersecurity Framework

# 4 Results

In this chapter, we propose fundamental evaluation items that allow governments, public institutions, and enterprises to systematically secure cyber resilience. By comparing and analyzing global institutions' cyber resilience frameworks, we aim to identify new evaluation items and present detailed indicators for these items. These indicators serve as practical criteria that organizations can apply to enhance their cyber resilience strategies effectively.

## 4.1 Development of Cyber Resilience Evaluation Items

To derive step-by-step evaluation items for cyber resilience, we conducted a comparative analysis of the evaluation items currently applied by global institutions. Based on this analysis, we identified the final evaluation items that meet the requirements for achieving the components of cyber resilience.

| Category | CISA | CPMI | NIST | **Evaluation Items** |
|---|---|---|---|---|
| Governance | | ✓ | ✓ | **Policy** |
| Foundation Establishment | ✓ | | | |
| Identification | ✓ | ✓ | ✓ | **Identification** |
| Risk Assessment | ✓ | | | |
| Detection | | ✓ | ✓ | **Anticipation** |
| Action Development | ✓ | | | |
| Testing | | ✓ | | **Resistance** |
| Protection | | ✓ | ✓ | |
| Response and Recovery | ✓ | ✓ | ✓ | **Recovery** |
| Situational Awareness | | ✓ | | |
| Learning and Evolving | | ✓ | | **Learning & Evolving** |
| Implementation and Evaluation | ✓ | | | |

Table 6: New Cyber Resilience Evaluation Items Derived from Comparative Analysis

The evaluation items for cyber resilience were structured into six stages: Policy, Identification, Anticipation, Resistance, Recovery, and Learning & Evolving. Each stage focuses on different aspects of strengthening and assessing cyber resilience, from recognizing its importance and planning to continuous improvement and response strategies.

The Policy stage focuses on recognizing the importance of cyber resilience and involves planning and evaluating strategies to strengthen it. The Identification stage prioritizes assets that need protection, distinguishing between critical operations and supporting information assets. The Anticipation stage presents proactive cyber defense methods to address external threats. Resistance relates to the inherent strength of systems to endure external threats. Recovery assesses the system's ability to restore functions quickly after a cyberattack. Lastly, Learning & Evolving reflects the ongoing integration of threat mitigation strategies and continuous reassessment within the organization to enhance cyber resilience.

## 4.2 Development of Indicators for Each Evaluation Item

### 4.2.1 Policy

In the policy stage, the necessary elements for formulating, implementing, and reviewing policies to manage threats are presented. The evaluation indicators for policy include the establishment of responsible entities and the definition of scope, policy formulation, and policy maintenance. Establishing responsibility and defining scope involves embedding the cyber resilience framework within the organization to ensure that it can immediately operate when issues arise. Policy formulation entails obtaining management approval for internal regulations and guidelines and clearly communicating them to employees and managers. Policy maintenance involves periodically reviewing and updating policies as needed, in accordance with relevant laws, regulations, higher-level organizational policies, and changes in the internal and external environment, while documenting and managing the history of any changes.

| Evaluation Items | Evaluation Indicators | Details (Sub Indicators) |
|---|---|---|
| 1. Policy | 1.1. Establishing Responsibility and Defining Scope | 1.1.1. Management Participation<br>1.1.2. Appointment of Chief Officer<br>1.1.3. Organizational Structure<br>1.1.4. Scope Definition<br>1.1.5. Resource Allocation |
| | 1.2. Policy Formulation | 1.2.1. Policy Formulation |
| | 1.3. Policy Maintenance | 1.3.1. Policy Maintenance<br>1.3.2. Organizational Maintenance |

Table 7: Cyber Resilience Evaluation Items and Indicators - Policy

### 4.2.2 Identification

In the identification stage, guidelines are provided for identifying infrastructure, prioritizing based on importance, and assessing dependencies among infrastructure systems. The evaluation indicators for identification include the identification of information assets, human assets, and physical assets. These indicators are commonly featured in the cyber resilience frameworks of global institutions and are crucial for defining assets that must be prioritized for recovery in the event of a cyberattack or disaster.

| Evaluation Items | Evaluation Indicators | Details (Sub Indicators) |
|---|---|---|
| 2. Identification | 2.1. Identification of Information Assets | 2.1.1. Identification of Information Assets<br>2.1.2. Management of Information Assets |
| | 2.2. Identification of Human Assets | 2.2.1. Designation and Management of Key Personnel<br>2.2.2. Role Separation |
| | 2.3. Identification of Physical Assets | 2.3.1. Designation of Protected Zones<br>2.3.2. Access Control<br>2.3.3. Protection of Information Systems<br>2.3.4. Operation of Protective Facilities |

Table 8: Cyber Resilience Evaluation Items and Indicators - Identification

#### 4.2.3 Anticipation

In the anticipation stage, vulnerabilities to threats and risks are assessed, and potential outcomes are predicted to perform risk assessments for critical infrastructure. The evaluation indicators for anticipation include monitoring, backup sites, and system redundancy. Monitoring involves establishing a response system that includes real-time detection to prevent incidents. Backup sites and system redundancy ensure business continuity by decentralizing assets, allowing services to continue operating even if an incident occurs.

| Evaluation Items | Evaluation Indicators | Details (Sub Indicators) |
|---|---|---|
| 3. Anticipation | 3.1. Monitoring | 3.1.1. Security System Operation<br>3.1.2. Accident Prevention and Response System Establishment<br>3.1.3. Vulnerability Check and Measures<br>3.1.4. Anomaly Analysis and Monitoring |
| | 3.2. Backup Sites | 3.2.1. Safety Measures for Disasters and Emergencies |
| | 3.3. System Redundancy | 3.3.1. Disaster Recovery Testing and Improvement |

Table 9: Cyber Resilience Evaluation Items and Indicators - Anticipation

#### 4.2.4 Resistance

In the resistance stage, the inherent strength of the infrastructure to withstand incidents is evaluated, and strategic execution plans are provided to address risks and enhance infrastructure resilience. The evaluation indicators for resistance include server security, network security, endpoint security, patch management, and data management. These indicators ensure that policies regarding solutions are predefined before incidents occur, and in the event of an incident, these policies are swiftly implemented to ensure the safe operation of the infrastructure.

| Evaluation Items | Evaluation Indicators | Details (Sub Indicators) |
|---|---|---|
| 4. Resistance | 4.1. Server Security | 4.1.1. Information System Access |
| | 4.2. Network Security | 4.2.1. Network Access |
| | 4.3. Endpoint Security | 4.3.1. Malware Control |
| | 4.4. Patch Management | 4.4.1. Patch Management |
| | 4.5. Data Management | 4.5.1. Database Access |

Table 10: Cyber Resilience Evaluation Items and Indicators - Resistance

#### 4.2.5 Recovery

In the recovery stage, the ability to restore services quickly to an acceptable state, recover critical functions, and replace damaged system components is assessed. The evaluation indicators for recovery include the prioritization of restoration, the selection of recovery time objectives, and the implementation of alternate systems. These indicators ensure that follow-up actions, such as incident response, backup and recovery management, and change management, are executed promptly and effectively.

| Evaluation Items | Evaluation Indicators | Details (Sub Indicators) |
|---|---|---|
| 5. Recovery | 5.1. Prioritization of Restoration | 5.1.1. Backup and Recovery Management |
| | 5.2. Selection of Recovery Time Objectives | 5.2.1. Incident Response and Recovery |
| | 5.3. Alternate Systems | 5.3.1. Change Management |

Table 11: Cyber Resilience Evaluation Items and Indicators - Recovery

#### 4.2.6 Learning & Evolving

In the learning & evolving stage, the focus is on continuously reviewing and analyzing previous evaluation indicators and response systems to enhance preventive capabilities. The evaluation indicators for this stage include analysis and improvement, as well as continuous training. By utilizing benchmarks, best practices, and ongoing training, the goal is to foster the enhancement and development of cyber resilience.

| Evaluation Items | Evaluation Indicators | Details (Sub Indicators) |
|---|---|---|
| 6. Learning & Evolving | 6.1. Analysis and Improvement | 6.1.1. Analysis of Measurement Indicators<br>6.1.2. Improvement of Safety Measures for Disasters and Emergencies |
| | 6.2. Continuous Training | 6.2.1. Incident Response Training and Improvement<br>6.2.2. Disaster Recovery Testing and Improvement |

Table 12: Cyber Resilience Evaluation Items and Indicators - Learning & Evolving

## 5 Conclusion and Discussions

This study examined the fundamental components of cyber resilience and analyzed global institutions' frameworks to propose new evaluation items and indicators for cyber resilience. The derived evaluation items and indicators are designed to integrate seamlessly with existing information security management systems, making it easier for organizations and companies to enhance their cyber resilience. The goals and objectives of cyber resilience emphasize incident

response through interdependency, connectivity, and integration of evaluation indicators, which are expected to contribute to ensuring business continuity.

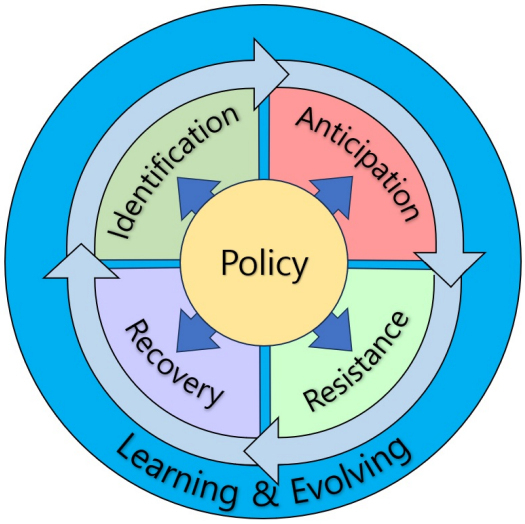


Figure 1: Integrated Cyber Resilience Items

Future research will focus on developing a new or improved framework that expands the concept of cyber resilience within information security management systems, based on the evaluation items proposed in this study. While the proposed framework is tailored for large organizations and governmental institutions, we will explore how smaller organizations and startups can adopt it cost-effectively and practically. By implementing the framework in real-world scenarios, we aim to validate its reliability and enhance its robustness.

Additionally, future studies will investigate specific areas such as Business Continuity Planning (BCP) through Business Impact Analysis (BIA), backup recovery testing strategies, monitoring tools and alert systems, and strategies for cyber resilience education and awareness. We will also focus on continuous assessment and improvement of organizational defense capabilities in response to rapidly changing cyber threat environments, as well as establishing public-private collaboration systems. Through these efforts, we seek to develop a more practical and comprehensive cyber resilience framework.

## 6 Acknowledgement

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation(IITP) grant funded by the Korea goverment(MSIT) (No.RS-2024-00439139, Development of a Cyber Crisis Response and Resilience Test Evaluation Systems). Also, this work was supported by the MSIT(Ministry of Science and ICT), Korea, under the Graduate School of Metaverse Convergence support program(IITP-2024-RS-2023-00254129) supervised by the IITP(Institute for Information & Communications Technology Planning & Evaluation).

# References


[1] Gavin Ashton. Maersk, me & notpetya. https://gvnshtn.com/posts/maersk-me-notpetya/, last viewed September 2024, 2020.

[2] National center of Incident readiness and Strategy for Cybersecurity (NISC). *Cybersecurity Strategy*. NISC, Japan, 2021.

[3] National center of Incident readiness and Strategy for Cybersecurity (NISC). *Cybersecurity Strategy Overview*. NISC, Japan, 2021.

[4] Cybersecurity and Infrastructure Security Agency (CISA). *Infrastructure Resilience Planning Framework (IRPF) (Version 1.2)*. CISA, 2024.

[5] Nicola Danti. *Report on the proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020*. Committee on Industry, Research and Energy, European Parliament, 2023.

[6] Jen Easterly. *CISA Strategic Plan 2023-2025*. Cybersecurity and Infrastructure Security Agency, 2022.

[7] S. Ghafur, S. Kristensen, K. Honeyford, G. Martin, A. Darzi, and P. Aylin. A retrospective impact analysis of the wannacry cyberattack on the nhs. *NPJ digital medicine*, 2(1): 98, 2019.

[8] Cybersecurity Strategic Headquarters. *Action Plan for Cybersecurity of Critical Infrastructure (Revision)*. Cybersecurity Strategic Headquarters, Japan, 2024.

[9] The White House. Office of the national cyber director. https://www.whitehouse.gov/oncd/, last viewed September 2024, 2021.

[10] The White House. *National Cybersecurity Strategy*. The White House, Washington, 2023.

[11] Jae hyeok Choi, Wan ju Kim, and Jae sung Lim. A study on maturity model for the assessment of cyber resilience level in the defence information system. *Journal of The Korea Institute of Information Security & Cryptology*, 29(5): 1153-1165, 2019.

[12] Angela SM Irwin and Caitlin Dawson. Following the cyber money trail: Global challenges when investigating ransomware attacks and how regulation can help. *Journal of money laundering control*, 22(1): 110-131, 2019.

[13] Ming Jin, Javad Lavaei, and Karl Henrik Johansson. Power grid ac-based state estimation: Vulnerability analysis against cyber attacks. *IEEE Transactions on Automatic Control*, 64(5): 1784-1799, 2018.

[14] Azfar Khalid, Pierre Kirisci, Zeashan Hameed Khan, Zied Ghrairi, Klaus-Dieter Thoben, and Jürgen Pannek. Security framework for industrial collaborative robotic cyber-physical systems. *Computers in Industry*, 97: 132-145, 2018.

[15] E.A. Ko, H.B. Kim, J.K. Kim, and J.Y. Yoon. *Cybersecurity Direction and Implications for Building the Digital Future of the EU*. KISA Insight, 2023.

[16] J.S. Lee, S.M. Choi, C.M. Ahn, and Y. Yoo. Trends and implications of cybersecurity policies in major countries. *Electronics and Telecommunications Trends*, 38(4): 58-69, 2023.

[17] Wei Li, Yahong Shi, and Yajie Li. Research on secure control and communication for cyber-physical systems under cyber-attacks. *Transactions of the Institute of Measurement and Control*, 41(12): 3421-3437, 2019.

[18] Ramin Moslemi, Afshin Mesbahi, and Javad Mohammadpour Velni. A fast, decentralized covariance selection-based approach to detect cyber attacks in smart grids. *IEEE Transactions on Smart Grid*, 9(5): 4930-4941, 2017.

[19] European Court of Auditors. *Cybersecurity of EU institutions, bodies and agencies*. European Union Special report, 2022.

[20] National Institute of Standards and Technology (NIST). *The NIST Cybersecurity Framework (CSF) 2.0*. NIST, U.S. Department of Commerce, 2024.

[21] Board of the International Organization of Securities Commissions. *Guidance on cyber resilience for financial market infrastructures*. Bank for International Settlements and International Organization of Securities Commissions, 2016.

[22] Technical Committee of the International Organization of Securities Commissions. *Principles for financial market infrastructures*. Bank for International Settlements and International Organization of Securities Commissions, 2012.

[23] Ron Ross, Victoria Pillitteri, Richard Graubart, Deborah Bodeau, and Rosalie Mcquaid. *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*. NIST Special Publication 800-160, Volume 2, Revision 1, National Institute of Standards and Technology, U.S. Department of Commerce, 2021.

[24] Ashutosh Sharma, Geetanjali Rathee, Rajiv Kumar, Hemraj Saini, Vijayakumar Varadarajan, Yunyoung Nam, and Naveen Chilamkurti. A secure, energy-and sla-efficient (sese) e-healthcare framework for quickest data transmission using cyber-physical system. *Sensors*, 19(9): 2119, 2019.

[25] William Smart. *Lessons learned review of the WannaCry Ransomware Cyber Attack*. Department of Health & Social Care, gov.uk, 2018.

[26] Yuan-Cheng Sun and Guang-Hong Yang. Periodic event-triggered resilient control for cyber-physical systems under denial-of-service attacks. *Journal of the Franklin Institute*, 355(13): 5613-5631, 2018.

[27] MingJian Tang, Mamoun Alazab, Yuxiu Luo, and Matthew Donlon. Disclosure of cyber security vulnerabilities: time series modelling. *International Journal of Electronic Security and Digital Forensics*, 10(3): 255-275, 2018.

[28] Huanhuan Yuan and Yuanqing Xia. Resilient strategy design for cyber-physical system under dos attack over a multi-channel framework. *Information Sciences*, 454: 312-327, 2018.