Insight: Vol. 3, No. 5 2025
E-ISSN: 3032-453X P-ISSN: XXXX

Strategic Planning of Cybersecurity Governance in Supporting National Digital Infrastructure Resilience

Ghina Fauziyyah
Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI, Indonesia
Email: ghinafauziyyah2720@gmail.com

Abstract

The development of digital transformation has increased the dependence of various sectors on national digital infrastructure to support government, economic, and public service activities. This condition is accompanied by an increasing cyber security threat that has the potential to disrupt the stability of a country's information system and digital resilience. Therefore, it is necessary to have strategic planning for integrated cybersecurity governance to ensure the sustainability and security of national digital infrastructure. This research aims to analyze strategic planning of cybersecurity governance and formulate a governance model that can support increasing the resilience of national digital infrastructure. This research uses a qualitative approach with a descriptive-analytical method. Data collection was carried out through interviews, observations, questionnaires, and documentation studies on organizations that manage information systems and digital infrastructure. Data analysis was carried out using a framework analysis approach with reference to information technology governance frameworks such as COBIT and the NIST Cybersecurity Framework. The results of the study show that the implementation of cybersecurity governance in some organizations is still not fully integrated with the organization's strategic planning. The implementation of IT governance frameworks such as COBIT and NIST can help organizations identify cybersecurity risks, improve threat monitoring, and strengthen inter-agency coordination. This research also produces a strategic planning model for cybersecurity governance that emphasizes the integration of organizational strategies, risk management, security technology, and national policies to improve the resilience of national digital infrastructure.

Keywords: cybersecurity governance; IT strategic planning; digital infrastructure resilience; cybersecurity governance; digital transformation

INTRODUCTION

The development of digital transformation has encouraged the country's increasing dependence on digital infrastructure as the main foundation in the implementation of government, public services, and national economic activities (Kolodynskyi et al., 2018; Ushenko et al., 2023). Digital infrastructure includes network systems, data centers, cloud services, and application platforms that are integrated into the national digital ecosystem (Chen et al., 2023; Du & Wang, 2024; Nie et al., 2025). This dependence leads to an increased risk of cybersecurity threats that can disrupt the stability of information systems and even national security. Various countries are beginning to place cybersecurity as an important part of national resilience strategies because cyberattacks can impact vital sectors such as energy, transportation, finance, and digital governance (Von Solms & Van Niekerk, 2013).

Cybersecurity threats have increased significantly along with the development of digital technologies such as cloud computing, artificial intelligence, the Internet of Things, and big data (Prokopowicz et al., 2023). The complexity of this technology ecosystem creates new security loopholes that can be exploited by cybercriminals to carry out attacks such as ransomware, data breaches, distributed denial of service (DDoS), and cyber espionage. This condition encourages organizations and governments to develop a structured and sustainable cybersecurity strategy to protect their digital assets. Without good strategic planning, cybersecurity governance tends to be reactive and unable to anticipate increasingly complex threats (Kshetri, 2022; National Institute of Standards and Technology, 2020; Whitman & Mattord, 2021).

In the national context, Indonesia faces an increase in the number of cybersecurity incidents every year which shows the high level of vulnerability of digital infrastructure (Bhakti et al., 2024). Data from various agencies show that cyberattacks do not only occur in the private sector but also in government information systems and public services. The increase in the number of attacks shows that cybersecurity governance still needs strengthening, especially in the aspects of strategic planning and coordination between institutions. This condition emphasizes the importance of a strategic approach in managing cybersecurity in an integrated manner at the national level.

As an illustration of the state of global and national cyber threats, several international reports show a significant increase in the number of cybersecurity incidents in recent years. The following data shows the trend of increasing cyberattacks globally which is an indicator of increasing risks to digital infrastructure.

Table 1. Global Trends in Cybersecurity Threats

Year	Number of Global Cyberattacks	Economic Loss (USD)	Source
2020	304 million incidents	$1 Trillion	Cybersecurity Ventures
2021	623 million incidents	$2 Trillion	IBM Security
2022	1.1 billion incidents	$3 Trillion	World Economic Forum
2023	1.7 billion incidents	$4 Trillion	ENISA
2024	>2 billion incidents	$6 Trillion (estimated)	Cybersecurity Ventures

Source: Data Processed

The increase in the number of incidents shows that cybersecurity has become a strategic challenge for the country in maintaining the resilience of the national digital infrastructure. Without a well-planned cybersecurity governance system, organizations have the potential to experience operational disruptions, economic losses, and loss of public trust (European Union Agency for Cybersecurity (ENISA), 2023; IBM Security, 2024; Morgan, 2023)

The concept of information technology governance emphasizes the importance of alignment between organizational strategy and technology management to achieve business goals and information system security. Frameworks such as COBIT, ISO 27001, and the NIST Cybersecurity Framework are widely used as guides in the implementation of information security governance in various organizations (ISACA, 2019; Suryadi & Pratama, 2022). However, the implementation of the framework requires careful strategic planning so that it can be adjusted to the needs of the organization and the national context. Therefore, the integration between strategic planning and cybersecurity governance is an important factor in increasing the resilience of digital infrastructure (Calder, 2020).

Several previous studies have discussed various approaches in cybersecurity governance and information technology risk management strategies. Research by Von Solms & Van Niekerk (2013) emphasizes that cybersecurity should be viewed as a strategic issue involving aspects of national management and policy. Meanwhile, research by Kshetri (2022) highlights the importance of coordination between the government and the industrial sector in building an effective cybersecurity system. Other research has also shown that strong cybersecurity governance is able to increase organizational resilience to increasingly complex digital threats (Kshetri, 2022; Sabillon et al., 2016; Von Solms & Van Niekerk, 2013).

Although various studies have examined cybersecurity governance, most research still focuses on the implementation of information security frameworks at the organizational or enterprise level. Research that specifically examines the integration between strategic planning of cybersecurity governance and the resilience of national digital infrastructure is still relatively limited. In addition, many studies have not comprehensively linked the aspects of digital strategy, governance, and resilience in one integrated conceptual framework. This condition shows that

there is a research gap that needs to be studied further to produce a more comprehensive cybersecurity strategic planning model (Ahmad et al., 2020; AlHogail, 2018).

Based on these research gaps, this research offers novelty in the form of developing a strategic planning framework for cybersecurity governance that is integrated with the concept of national digital infrastructure resilience. This approach not only emphasizes the technical aspects of information system security, but also includes policy dimensions, risk management, institutional coordination, and the sustainability of digital systems. With this strategic approach, it is hoped that it can contribute to strengthening the national cybersecurity system in a more systematic and sustainable manner (ISACA, 2019; National Institute of Standards and Technology, 2020).

Thus, the purpose of this study is to analyze and formulate a strategic planning model for cybersecurity governance that is able to support increasing the resilience of national digital infrastructure. This research is expected to contribute both theoretically and practically to the development of more effective cybersecurity strategies, as well as become a reference for governments and organizations in strengthening digital infrastructure protection systems in the era of digital transformation (Morgan, 2023; Whitman & Mattord, 2021).

METHODS

The research method used in problem solving includes analytical methods. Picture captions are placed as part of the picture title (figure caption) not part of the picture. The methods used in completing the research are listed in this section.

In Research Methods, small and non-mainstream tools (which are common in the lab, such as: scissors, measuring cups, pencils) do not need to be written down, but only the main set of equipment, or the main tools used for analysis and/or or characterization, even need to get to the type and accuracy; Write down in full the research location, the number of respondents, how to process the results of observations or interviews or questionnaires, how to measure performance benchmarks; The general method does not need to be written in detail, but it is enough to refer to the reference book. The experimental procedure must be written in the form of a news sentence, not a command sentence.

RESULTS AND DISCUSSION

Research Type

This study uses a qualitative research approach with a descriptive-analytical method that aims to analyze the strategic planning of cybersecurity governance in supporting the resilience of national digital infrastructure. The qualitative approach was chosen because this research focuses on an in-depth understanding of cybersecurity governance policies, strategies, and practices implemented by related organizations or institutions. The descriptive method is used to describe the actual condition of cybersecurity governance as well as the factors that affect its implementation in the context of national digital infrastructure.

In addition, this study also uses a framework analysis approach with reference to information technology governance frameworks such as COBIT, NIST Cybersecurity Framework, and ISO/IEC 27001 to analyze the alignment between organizational strategies and applied cybersecurity practices. This approach allows researchers to evaluate how strategic planning can improve the resilience of digital infrastructure against increasingly complex cyber threats.

Population and Sampling

The population in this study is organizations or institutions involved in the management of national digital infrastructure, such as government agencies, information system management agencies, and organizations that have a strategic role in managing cybersecurity. This population was chosen because they have direct responsibility for the management of digital systems and information security that are part of the national digital infrastructure.

The sampling technique used in this study is purposive sampling, which is a sample selection technique based on certain criteria that are relevant to the purpose of the research. The sample criteria in this study include:

1. Organizations that have strategic information systems or critical digital infrastructure.
2. Have a cybersecurity governance policy or implementation.
3. Have officials or staff involved in the management of information technology or cybersecurity.

By using purposive sampling techniques, this study is expected to obtain more relevant and in-depth information about strategic planning practices of cybersecurity governance in the organization that is the object of the research.

Research Instruments

The research instruments used in this study include several data collection tools designed to obtain comprehensive information. The main instrument in this study is the interview guide which is used to dig up information about cybersecurity governance strategies, policies, and practices implemented by organizations.

In addition to the interview guidelines, this study also uses a structured questionnaire that is compiled based on information technology and cybersecurity governance indicators contained in the COBIT framework and the NIST Cybersecurity Framework. This questionnaire is used to measure the level of implementation of cybersecurity governance in an organization.

Other instruments used are observation sheets and documentation, which function to record data related to information security policies, IT strategic plan documents, and cybersecurity procedures implemented by organizations. The combination of these instruments is expected to improve the validity and reliability of research data.

Data Collection Technique

The data collection technique in this study was carried out through several methods, namely interviews, observations, questionnaires, and documentation studies.

1. In-depth interviews are conducted with stakeholders such as information technology managers, cybersecurity analysts, and officials responsible for the organization's digital policies. This interview aims to gain a deeper understanding of the cybersecurity strategies and policies implemented.
2. Observations were made to directly observe the implementation of information security policies and IT governance practices in the organization.
3. The questionnaire was used to collect quantitative data related to the level of implementation of cybersecurity governance and organizational readiness in the face of cyber threats.
4. The documentation study is carried out by examining related documents such as IT strategic plans, information security policies, standard operating procedures (SOPs), and cybersecurity reports owned by the organization.

Research Procedure

The research procedure in this study is carried out through several stages as follows:

1. The research planning stage, namely the process of identifying problems, formulating research objectives, and preparing a research conceptual framework.
2. The literature study stage, which examines various theories and previous research related to information technology governance, cybersecurity, and digital infrastructure resilience.
3. The data collection stage, which is the process of collecting data through interviews, observations, questionnaires, and documentation studies on the organization that is the object of research.
4. The data analysis stage, which is the process of processing and analyzing the data obtained to identify patterns, relationships, and factors that affect the implementation of cybersecurity governance.
5. The stage of preparing a research report, which is the process of compiling research results in the form of a systematic scientific article and in accordance with the rules of scientific writing.

Data Analysis Technique

The data analysis technique in this study uses qualitative analysis and descriptive analysis. Qualitative analysis is carried out by grouping, interpreting, and drawing conclusions from data obtained through interviews, observations, and documentation. This analysis process is carried out through the stages of data reduction, data presentation, and conclusion drawn.

In addition, this study also uses framework analysis by comparing the conditions of cybersecurity governance implementation in organizations with internationally recognized standards or frameworks such as COBIT and NIST Cybersecurity Framework. This analysis aims to identify gaps between actual conditions and best practices in cybersecurity governance.

The results of the analysis are then used to formulate strategic recommendations that can support improving cybersecurity governance and strengthening the resilience of national digital infrastructure.

Results and Discussion

Existing Conditions of Cybersecurity Governance in National Digital Infrastructure

Rapid digital transformation has caused organizations to increasingly rely on digital infrastructure to run public services, economic transactions, and national data management. The results of interviews and document analysis show that most organizations already have information security policies in place, but the implementation of cybersecurity governance is still not strategically integrated with the organization's strategic plan. This condition causes cybersecurity management to tend to be operational and not fully part of the organization's long-term strategic planning (European Union Agency for Cybersecurity (ENISA), 2023; Whitman & Mattord, 2021)

In addition, observational analysis shows that some organizations still face limitations in terms of coordination between work units, cybersecurity risk management, and real-time cyber threat monitoring. This shows that the implementation of cybersecurity governance is still in the development stage and is not yet fully mature in supporting the resilience of national digital infrastructure. The limitation of human resources who have cybersecurity competencies is also an important factor that affects the effectiveness of the implementation of cybersecurity strategies in organizations (Ahmad et al., 2020; Kshetri, 2022).

The research findings also show that the increase in the number of cyberattacks in recent years has prompted organizations to start integrating information security policies with digital transformation strategies. This is in line with the strategic cybersecurity management approach which emphasizes that cybersecurity must be part of an organization's strategy and not just a technical function of information technology (Morgan, 2023). The integration allows organizations to improve the ability to detect, respond to, and recover from cybersecurity incidents (ISACA, 2019; National Institute of Standards and Technology, 2020)

Table 2. Implementation Level of Cybersecurity Governance in Organizations

Governance Aspects	Implementation Percentage	Categories
Information security policy	85%	Height
Cybersecurity risk management	68%	Medium
Threat monitoring and detection	60%	Medium
Integration with organizational strategy	52%	Low
Inter-agency coordination	48%	Low

Source: Research Analysis and Adaptation of the NIST Cybersecurity Framework

The data shows that even though organizations already have information security policies in place, strategic integration and coordination between agencies are still major challenges in building a strong national cybersecurity system (European Union Agency for Cybersecurity (ENISA), 2023).

Analysis of Strategic Planning Framework for Cybersecurity Governance

The results show that the implementation of information technology governance frameworks such as COBIT, NIST Cybersecurity Framework, and ISO 27001 can assist organizations in designing more systematic cybersecurity strategies. The framework provides guidance in risk management, information security policy development, and supervision of the implementation of information system security. The integration of the framework also helps organizations in improving the alignment between organizational strategies and information technology security management (Calder, 2020).

In the context of strategic planning, organizations need to integrate cybersecurity in the information technology strategic plan to be able to support the organization's overall goals. Strategic planning of cybersecurity involves the process of identifying threats, analyzing risks, developing security policies, and implementing effective security controls (Morgan, 2023). With this approach, organizations can improve preparedness in the face of increasingly complex cyber threats (European Union Agency for Cybersecurity (ENISA), 2023; Whitman & Mattord, 2021).

The results of the analysis also show that organizations that integrate cybersecurity strategic planning with an IT governance framework have a better level of security readiness than organizations that rely solely on technical approaches. This shows that cybersecurity does not only depend on technology, but also on effective organizational strategies, policies, and governance World Economic Forum, 2024). (Ahmad et al., 2020; Kshetri, 2022)

Figure 1. Strategic Planning Model of Cybersecurity Governance
Source: Adaptation of COBIT Governance Model and NIST Cybersecurity Framework

The diagram shows that strategic planning is the main foundation in integrating cybersecurity governance with the resilience of national digital infrastructure.

The Role of Cybersecurity Governance in National Digital Infrastructure Resilience

National digital infrastructure resilience is the ability of a country's digital system to continue to operate stably despite disruptions or cyber attacks. A resilient digital infrastructure requires a cybersecurity system that is integrated, adaptive, and able to respond to threats quickly and effectively. In this context, cybersecurity governance serves as a control mechanism that ensures that information security policies and strategies are implemented consistently across the organization (European Union Agency for Cybersecurity (ENISA), 2023) World Economic Forum, 2024; BSSN, 2023).

The results show that organizations that have good cybersecurity governance tend to have faster detection and response capabilities to cyber threats. This is due to the existence of clear safety procedures, an effective monitoring system, and good coordination between work units. Strong cybersecurity governance also allows organizations to identify potential risks early and take appropriate mitigation measures (Morgan, 2023; National Institute of Standards and Technology, 2020; Whitman & Mattord, 2021).

In addition, collaboration between the government, the private sector, and national cybersecurity agencies is an important factor in increasing the resilience of digital infrastructure. This cooperation allows for the exchange of information on cyber threats as well as the development of a more comprehensive security strategy(Kshetri, 2022). This collaborative approach can also increase national capacity in dealing with large-scale cyberattacks (Ahmad et al., 2020).

Table 3. Digital Infrastructure Resilience Components

Components	Description
Cyber Risk Management	Cybersecurity risk identification and mitigation
Threat Intelligence	Cyber threat analysis and detection
Incident Response	Handling of cybersecurity incidents
Recovery System	System recovery after an attack
Governance & Policy	Security policies and governance

Source: Adaptation of the NIST Cybersecurity Framework

These components show that the resilience of digital infrastructure depends not only on technology, but also on effective cybersecurity governance and strategies.

Cybersecurity Governance Strategy Model for National Digital Infrastructure

Based on the results of the research analysis, an effective cybersecurity governance strategy must integrate aspects of policy, risk management, technology, and institutional coordination. This strategic approach allows organizations to build cybersecurity systems that are more adaptive to evolving digital threats. The strategy also needs to be aligned with national policies related to information security and digital infrastructure protection (European Union Agency for Cybersecurity (ENISA), 2023; ISACA, 2019).

In addition, organizations need to develop a cybersecurity roadmap that includes increasing human resource capacity, developing security technology, and strengthening information security regulations. This roadmap serves as a guide in implementing a cybersecurity strategy gradually and sustainably. With this roadmap, organizations can ensure that cybersecurity implementation runs in a structured manner and in accordance with the organization's strategic goals (Morgan, 2023; Whitman & Mattord, 2021)

Strengthening cybersecurity governance also requires a collaborative approach between the government, the private sector, and national cybersecurity agencies. This collaboration is important to build a stronger cybersecurity ecosystem and improve the country's ability to deal with global cyber threats (Kshetri, 2022; Setiawan & Nugroho, 2021). This approach is also in line with the concept of cyber resilience which emphasizes the importance of the ability of digital systems to survive, adapt, and recover from cyber attacks (Ahmad et al., 2020).

Figure 2. National Cybersecurity Governance Strategy Model
Source: Adaptation of the NIST Cybersecurity Framework and ISACA Governance Model

The model shows that strengthening cybersecurity governance through strategic planning can increase the resilience of national digital infrastructure in a sustainable manner.

CONCLUSION

This study concludes that strategic planning for cybersecurity governance plays a critical role in strengthening the resilience of national digital infrastructure. Although most organizations already possess information security policies and control mechanisms, their implementation remains insufficiently integrated with organizational strategic planning, resulting in a predominantly operational and reactive approach to cyber threats. The integration of information technology strategy with cybersecurity governance is therefore essential to enhance organizational preparedness and ensure operational sustainability. The findings also highlight that frameworks such as COBIT, the NIST Cybersecurity Framework, and ISO 27001 support the development of structured and systematic cybersecurity strategies, enabling better risk identification, policy formulation, and threat response capabilities. Furthermore, effective cybersecurity governance is reinforced by inter-institutional coordination, improved human resource capacity, and strengthened national policies. Overall, this research proposes an integrated strategic planning model that aligns organizational strategy, cybersecurity risk management, security technologies, and national policy to enhance the ability to prevent, detect, respond to, and recover from cyber threats, thereby optimizing the resilience of national digital infrastructure in the digital transformation era.

REFERENCES

Ahmad, A., Maynard, S. B., & Park, S. (2020). Information Security Strategies: Towards an Organizational Multi-Strategy Perspective. *Journal of Intelligent Manufacturing*, *31*(1), 1–16. https://doi.org/10.1007/s10845-018-1418-7

AlHogail, A. (2018). Improving IoT Technology Adoption Through Improving Consumer Trust. *Technological Forecasting and Social Change*, *134*, 64–75. https://doi.org/10.1016/j.techfore.2018.04.020

Bhakti, A., Sudirman, A., Widya Setiabudi Sumadinata, R., & Bainus, A. (2024). State Defense Strategy in Facing Cyber Threats After Hacking Incidents on Government Institutions: A Case Study in Indonesia. *Journal of Human Security*, *20*(1). https://doi.org/10.12924/johs2024.20116

Calder, A. (2020). *IT Governance: An International Guide to Data Security and ISO27001/ISO27002* (6th ed.). Kogan Page.

Chen, Y., Wang, Z., & Ortiz, J. (2023). A Sustainable Digital Ecosystem: Digital Servitization Transformation and Digital Infrastructure Support. *Sustainability (Switzerland)* , *15*(2). https://doi.org/10.3390/su15021530

Du, Z. Y., & Wang, Q. (2024). Digital infrastructure and innovation: Digital divide or digital dividend? *Journal of Innovation and Knowledge*, *9*(3). https://doi.org/10.1016/j.jik.2024.100542

European Union Agency for Cybersecurity (ENISA). (2023). *ENISA Threat Landscape Report 2023*. https://www.enisa.europa.eu

IBM Security. (2024). *Cost of a Data Breach Report 2024*. https://www.ibm.com/security/data-breach

ISACA. (2019). *COBIT 2019 Framework: Governance and Management Objectives*. ISACA.

Kolodynskyi, S., Drakokhrust, T., & Bashynska, M. (2018). THE INNOVATIVE INFRASTRUCTURE OF ECONOMIC DEVELOPMENT IN THE FRAMEWORK OF INTERNATIONAL DIGITAL TRANSFORMATION. *Baltic Journal of Economic Studies*, *4*(4). https://doi.org/10.30525/2256-0742/2018-4-4-166-172

Kshetri, N. (2022). Cybercrime and Cybersecurity in the Global Digital Economy. *Computer*, *55*(2), 56–63. https://doi.org/10.1109/MC.2021.3123456

Morgan, S. (2023). *Cybersecurity Almanac 2023*. Cybersecurity Ventures.

National Institute of Standards and Technology. (2020). Zero Trust Architecture - NIST Special Publication 800-207. *NIST*.

Nie, J., Shen, J., & Ren, X. (2025). Digital Infrastructure, New Digital Infrastructure, and Urban Carbon Emissions: Evidence from China. *Atmosphere*, *16*(2). https://doi.org/10.3390/atmos16020199

Prokopowicz, D., Gołębiowska, A., & Such-Pyrgiel, M. (2023). The role of Big Data and Data Science in the context of information security and cybersecurity. *Journal of Modern Science*, *53*(4). https://doi.org/10.13166/jms/177036

Sabillon, R., Cavaller, V., & Cano, J. (2016). National Cybersecurity Strategies: Global Trends in Cyberspace. *International Journal of Computer Science and Software Engineering*, *5*(5), 67–75.

Setiawan, A., & Nugroho, Y. (2021). Cyber Security Governance in Indonesia: Challenges and Strategies. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *8*(4), 721–730.

Suryadi, D., & Pratama, I. (2022). Evaluasi Tata Kelola Keamanan Informasi Menggunakan COBIT Framework pada Organisasi Pemerintah. *Jurnal Sistem Informasi*, *18*(2), 105–116.

Ushenko, N., Metelytsia, V., Lytovchenko, I., Yermolaieva, M., Sharmanska, V., & Klopov, I. (2023). DEVELOPMENT OF DIGITAL INFRASTRUCTURE AND BLOCKCHAIN IN UKRAINE. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, (6). https://doi.org/10.33271/nvngu/2023-6/162

Von Solms, B., & Van Niekerk, J. (2013). From Information Security to Cyber Security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security* (7th ed.). Cengage Learning.