Cybersecurity in the Digital Era: Ensuring the Sustainability of Global Information Systems

[1]Rico Tampaty*, [2]Shearly Tantowi, [3]Efrando, [4]Mirna, [5]Adisuputra
[1-5] Universitas Pertiba

*Corresponding Author:
rtampati964@gmail.com

Abstract

Cybersecurity has become a crucial aspect in the digital era to maintain the sustainability of global information systems, including in Indonesia. The ever-evolving cyber threats can disrupt public services, the economy, and critical infrastructure. This study aims to analyze the state of cybersecurity in Indonesia and identify challenges as well as mitigation strategies that can be implemented. Using a qualitative approach and literature review, the study finds that Indonesia's cybersecurity readiness still faces various challenges, including a lack of user awareness and regulatory limitations. Therefore, stronger policies and broader education are needed to enhance protection against cyber threats.

Keywords: Cybersecurity, Digital Era, Information Systems, Indonesia, Sustainability.

1. INTRODUCTION

The development of information technology has had a significant impact on various aspects of life, including business, government, and society. With the increasing adoption of technology, cybersecurity has become one of the main challenges faced by individuals, organizations, and nations. Cyber threats do not only target the business sector but also public services, the financial sector, and critical infrastructure such as energy and transportation (ISO, 2021).

According to a report from the National Cyber and Crypto Agency (BSSN), cyberattacks in Indonesia have sharply increased in recent years. In 2022 alone, BSSN recorded more than 1.6 billion cyberattack attempts targeting various sectors in Indonesia (BSSN, 2023). The most common types of attacks include malware, phishing, and Distributed Denial of Service (DDoS), which aim to steal data, damage systems, or disrupt service operations (Kominfo, 2022).

Cybersecurity is becoming increasingly important due to the rapid digital transformation across various sectors. The digitalization of public services and e-commerce businesses has increased dependence on information systems, thus raising the potential risk of cyberattacks (World Economic Forum, 2023). Additionally, the emergence of new technologies such as the Internet of Things (IoT) and artificial intelligence (AI) has opened new vulnerabilities for increasingly complex cyber threats (Symantec, 2022). As attack methods become more sophisticated, organizations and individuals need to enhance their security systems to protect important data and information from hacking and data breaches (Aminah et al., 2023).

Beyond technical aspects, human factors are also a major cause of data breaches and successful cyberattacks. Studies show that most cybersecurity incidents occur due to user negligence in safeguarding personal information, such as using weak or easily guessed passwords (Kominfo, 2022). Therefore, digital security education and awareness are essential steps in strengthening Indonesia’s cyber defense. Training programs for company employees, government institutions, and the general public can help reduce the risk of cyberattacks caused by human error (ISO, 2021).

As digitalization expands across various sectors, cybersecurity regulations are also continuously being developed. The Indonesian government has implemented several policies, such as Presidential Regulation No. 82 of 2022 on the Protection of Critical Information Infrastructure and Law No. 11 of 2008 on Electronic Information and Transactions (ITE),

which has been revised to enhance cybersecurity (Setneg, 2022). However, the implementation of these regulations still faces challenges in terms of socialization, compliance, and effectiveness in addressing evolving threats (Aminah et al., 2023). Additionally, international cooperation in cybersecurity is becoming increasingly important, given the cross-border nature of cyber threats that can affect the stability of global information systems (BSSN, 2023).

With the rise of increasingly complex and difficult-to-detect cyberattacks, many countries have begun adopting AI-based security strategies and big data analytics to detect threats more proactively. Indonesia also needs to develop more advanced cyber defense technologies to anticipate increasingly diverse and aggressive attacks. Furthermore, collaboration between the government, private sector, and academia is crucial to strengthening the nation's digital security system.

Therefore, this study aims to explore the state of cybersecurity in Indonesia and the strategies that can be implemented to enhance protection against digital threats. The main focus of this research is to identify key cybersecurity challenges and evaluate strategic measures to improve the protection of global information systems.

2. METHOD

This study employs a qualitative method with a literature review approach and secondary data analysis. The data sources include government reports, academic journals, and publications from cybersecurity institutions such as BSSN and the Ministry of Communication and Informatics. The data is analyzed using a descriptive approach to understand cyber threat trends and the policies that have been implemented in Indonesia.

3. RESULTS AND DISCUSSION

Based on data analysis, it was found that Indonesia faces several key challenges in cybersecurity, namely:

1. **Lack of Public Awareness:**
   Many individuals and companies still lack sufficient understanding of the importance of data security and information protection practices (Kominfo, 2022).
2. **Regulatory Limitations:**
   Although the government has issued cybersecurity regulations, their implementation remains suboptimal across various sectors (BSSN, 2023).
3. **Complex Cyberattacks:**
   Threats such as ransomware, phishing, and DDoS attacks are becoming increasingly sophisticated and difficult to detect using conventional security systems (Symantec, 2022).

Source: BSSN, 2023

Figure 1. Increase in the Number of Cyberattacks in Indonesia (2020-2023)

This graph shows the trend of increasing cyberattacks in Indonesia based on reports from the National Cyber and Crypto Agency (BSSN). The data indicates that the number of cyberattacks rose from 800 million attacks in 2020 to 1.6 billion attacks in 2023.

Trend Analysis of Increasing Cyberattacks:

1. Year 2020 (800 million attacks):
   - The COVID-19 pandemic accelerated digital transformation in Indonesia, increasing the use of online services.
   - Many businesses and public services transitioned to digital platforms without adequate security preparation, creating vulnerabilities for cyberattacks.
2. Year 2021 (1.05 billion attacks, a 31.25% increase from the previous year):
   - The rise of e-commerce and digital banking led to more phishing and malware attacks.
   - Distributed Denial of Service (DDoS) attacks targeting government websites and financial institutions began to increase.
3. Year 2022 (1.35 billion attacks, a 28.57% increase from the previous year):
   - Ransomware attacks surged, particularly targeting hospitals and educational institutions.
   - The emergence of Internet of Things (IoT) technology introduced new security vulnerabilities.
4. Year 2023 (1.6 billion attacks, an 18.52% increase from the previous year):
   - Cyber threats became more complex with hackers utilizing AI.
   - Attacks on critical infrastructure, such as government systems and digital transportation services, increased.

Table 1. Types of Cyberattacks and Their Impact in Indonesia

Type of Attack	Main Impact	Example Cases in Indonesia
Malware	Data theft, system malfunction	Ransomware attack on government institutions (2022)
Phishing	Credential theft and sensitive information leaks	Email and SMS banking fraud
DDoS	Online service disruption	Attack on government websites (2021)
Ransomware	Data encryption, ransom extortion	Hospitals and educational institutions targeted

Type of Attack	Main Impact	Example Cases in Indonesia
Website Defacement	Alteration of website appearance	Several government agency websites hacked

Source: BSSN Report (2023), Ministry of Communication and Informatics (2022), Aminah et al. (2023).

This table highlights various common cyberattacks in Indonesia and their impact on the national information system. To address these challenges, several strategies can be implemented, including:

1. **Enhancing Cyber Education and Awareness** through national campaigns and training programs for the public and industry sectors.
2. **Strengthening Regulations and Law Enforcement** to ensure all entities adhere to strict security standards in digital data management.
3. **Utilizing Modern Security Technologies** such as artificial intelligence (AI) and big data analytics to detect and prevent threats in real-time.

4. CONCLUSION

Cybersecurity is a crucial aspect of ensuring the sustainability of global information systems, particularly in Indonesia. Challenges such as a lack of public awareness, regulatory limitations, and increasingly complex cyber threats require serious attention. Therefore, strategies such as enhancing education, strengthening regulations, and implementing advanced technologies must continue to be developed. With strong collaboration between the government, the private sector, academia, and society, Indonesia can strengthen its digital resilience and address the growing cyber threats in the future.

Furthermore, investing in cybersecurity infrastructure is essential to ensure the reliability of digital systems across various sectors. The government must accelerate the implementation of stricter regulations and provide incentives for companies committed to data security. Additionally, organizations should adopt multi-layered security systems, including multi-factor authentication, data encryption, and real-time threat monitoring.

Beyond technical approaches, education plays a crucial role. Increasing public digital literacy can help reduce attacks that exploit human factors, such as phishing and social engineering. With the growing number of internet users in Indonesia, large-scale and continuous educational programs will be an effective solution to raise awareness of the importance of personal data protection.

Cybersecurity is not only the responsibility of the government or the technology sector but also all stakeholders, including the general public. Therefore, fostering a culture of cybersecurity from an early age through both formal and informal education is a strategic step that must be taken. With integrated and sustainable measures, Indonesia can build a stronger digital security system that is more adaptive to evolving threats.

ACKNOWLEDGMENTS

The author expresses gratitude to all parties who have supported this research, including the supervising professors, fellow academics, and institutions that provided data and references related to cybersecurity. Special thanks are also extended to the National Cyber and Crypto Agency (BSSN) and the Ministry of Communication and Informatics for their insights and reports, which served as the foundation for this study. The support from family and friends has also been invaluable in successfully completing this research.

NOVELTY

This research presents several novel contributions to the study of cybersecurity in Indonesia:

1. **Specific Analysis of Cybersecurity in Indonesia**
   Unlike previous studies that take a more global perspective, this research focuses on Indonesia's cybersecurity landscape, including challenges and strategies that align with existing regulations and infrastructure.
2. **Multi-Stakeholder Approach**
   This study emphasizes the importance of collaboration among various stakeholders including the government, private sector, academia, and the general public to enhance cybersecurity collectively.
3. **Implementation of Adaptive Cybersecurity Technologies**
   The research highlights the need for adaptive security strategies in response to technological advancements, including the use of artificial intelligence, advanced encryption, and predictive analytics to anticipate cyber threats.
4. **Integration of Public Education and Awareness**
   A key novelty of this study is its emphasis on digital literacy and cybersecurity awareness as crucial elements in mitigating cyber threats, considering that many attacks exploit low digital literacy levels.
5. **Regulation-Based Strategic Recommendations**
   This research provides policy-based recommendations tailored to Indonesia's regulatory framework, including the role of the National Cyber and Crypto Agency (BSSN) in shaping more effective digital security policies.

With these findings, this study is expected to serve as a valuable reference for policymakers, academics, and cybersecurity practitioners in developing more effective strategies to counter evolving cyber threats.

REFERENCE

Aminah, R., et al. (2023). Cybersecurity Challenges and Solutions in Indonesia. Journal of Cyber Studies, 15(2), 45-60.

Badan Siber dan Sandi Negara (BSSN). (2023). Laporan Tahunan Keamanan Siber Indonesia. Jakarta: BSSN.

ISO. (2021). Cybersecurity Standards and Best Practices. Geneva: International Organization for Standardization.

Kominfo. (2022). Statistik Keamanan Siber Indonesia. Jakarta: Kementerian Komunikasi dan Informatika.

Setneg. (2022). Peraturan Presiden No. 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital. Jakarta: Sekretariat Negara.

Symantec. (2022). The State of Cyber Threats in the Digital Era. USA: Symantec Research.

World Economic Forum. (2023). Global Cybersecurity Outlook 2023. Geneva: WEF.