Cerdika: Jurnal Ilmiah Indonesia, 6 (2), 2026
p-ISSN: 2774-6291 e-ISSN: 2774-6534

Available online at http://cerdika.publikasiindonesia.id/index.php/cerdika/index

Cybersecurity as a Pillar of Data Protection in the Digital Era: Strategies, Regulations, and Implementation in Facing Cyber Threats

Harson Kapoh, Sabian Saleh Katijo, Khrisna Suwartono Putra, Raisya Wulandari Nurhamidin, Sintikhe Ranteallo
Politeknik Negeri Manado, Indonesia
Email: hvskapoh@gmail.com, sabiansalehkatijo@gmail.com, Ksuwartonoputra@gmail.com, raisyanurhamidin.1@gmail.com, sintikheranteallo28@gmail.com

Abstract
Digital Transformation has changed the way people work, interact, and carry out daily activities. This revolution has brought high efficiency to communication, commerce, education, and even public services. Data is now considered "the new oil" due to its vital role in decision-making, business strategy, and the development of artificial intelligence–based technologies. However, as the use of digital technology increases, cyber threats have also grown more complex. Attacks such as malware, ransomware, phishing, identity theft, and data breaches have become global issues that can disrupt economic stability, damage an organization's reputation, and even threaten national sovereignty. This study aims to analyze the role of cybersecurity as a pillar of data protection in the digital era. The method used is a literature review that examines various scientific publications, international standards, security reports, and regulations applicable at both national and global levels. The results show that data protection cannot rely solely on advanced technology; it also requires clear regulations, competent professionals, and public awareness of the importance of information security.

Keywords: *Cybersecurity; Data Protection; CIA Triad; ISO 27001; Digital Era*

INTRODUCTION

The development of digital technology has brought many positive impacts to human life. Various activities that previously required a long time can now be carried out quickly, easily, and efficiently thanks to the support of the internet and digital systems (Fatah & Ngamal, 2025; Iskandar, 2025; Kim & Jin, 2024; Lestari & Rachmawati, 2022). Financial transactions now take place conveniently through smartphones; archive storage has shifted to cloud systems that can be accessed anytime, while long-distance communication has become smoother through various online platforms such as social media and video-conference applications. Public services have also widely adopted digital systems, allowing people to handle various administrative needs online without time or location constraints (Priyono et al., 2024; Rahayu et al., 2023). This transformation shows that digitalization has become a fundamental pillar in driving progress in the social, economic, and governmental sectors.

However, behind these conveniences, advancements in digital technology have also introduced new threats in the form of increasingly complex cyberattacks (Setiawan & Lestari, 2020. Cases of personal data breaches affecting government institutions, companies, and even the healthcare sector demonstrate persistent weaknesses in digital information protection (Al Kinoon, 2024; Osawaru, 2024; Wickham, 2019). Ransomware attacks that cripple public service systems, along with the rise of identity theft through phishing and malware methods, indicate that cyber risks cannot be ignored (Thornton & Thornton, 2024; Zahoor et al., 2023).

Data is now valued not only as an economic asset but also as an essential element tied to public trust, institutional reputation, and national sovereignty (Pratama & Handayani, 2021; European Union, 2018). Therefore, the implementation of strong, integrated, and regulation-

compliant cybersecurity systems has become an urgent necessity. Without adequate protection, digital transformation may instead pose serious threats to privacy, integrity, and information security at both individual and national levels (Pimenta Rodrigues et al., 2024; Tao et al., 2019).

This research offers novelties that distinguish it from previous studies, both empirically, methodologically, and conceptually. Empirically, this study uses the latest data from the Central Statistics Agency (BPS) and the Indonesian Internet Service Providers Association (APJII) for 2025, which have not been widely discussed in scientific publications. This allows it to provide a more up-to-date picture of internet penetration and digital mapping in Indonesia. Methodologically, this study employs a mixed approach that integrates descriptive statistical analysis of national secondary data with thematic analysis of policy documents and literature, differing from previous studies that tend to be geographically and thematically fragmented. Conceptually, this study explicitly outlines the infrastructure-biased digital development paradigm by providing empirical evidence that connectivity does not automatically result in economic participation and by introducing the term infrastructure error to describe the gap between access availability and the utilization of the digital economy European Union. (2018). General Data Protection Regulation (GDPR). Official Journal of the European Union. This study also offers a new conceptual framework for the transition from digitalization to digital development that emphasizes the balance between infrastructure, human capacity, local institutions, and social aspirations, while expanding the implementation of the capability approach in the context of digital transformation. With this framework, this research not only critiques existing policies but also reformulates the direction of national digital policy through an affirmative approach, decentralization of digital policy, and programs integrating digital literacy and the empowerment of MSMEs as an integral part of development infrastructure.

This research aims to analyze the level of internet penetration and the digital access gap in Indonesia, identify factors that hinder the utilization of the digital economy by unconnected communities, evaluate the orientation of national digital development policies, and develop a strategic framework for inclusive and sustainable digital transformation. Theoretically, this research also aims to advance the study of development communication and the digital economy, critique the technodeterminism paradigm, and expand the application of the capability approach in the context of digital transformation. This research is expected to provide practical benefits for the Ministry of Communication and Digital Affairs, local governments, technology industry players, and civil society organizations in designing digital literacy policies, intervention programs, and empowerment strategies that are more targeted. For the public, this research is expected to raise awareness of the complexity of digital transformation and encourage government and corporate accountability in realizing an equitable digital ecosystem. Academically, this research contributes to the development of studies on the digital divide, the digital economy, and development communication in Indonesia.

This research implies the need for a paradigm shift from infrastructure development to digital ecosystem development. Proposed policy implications include affirmative action policies for digital platforms, consumer and personal data protection, fiscal incentives for MSME technology adoption, and the decentralization of digital policies that grant authority and resources to local governments. Furthermore, this research emphasizes that digital transformation must be understood as a process of lifting communities out of poverty and powerlessness, not merely a technical achievement. Therefore, a key implication of this

research is that bridging the digital divide requires a multidimensional approach that addresses not only access but also skills, trust, and institutional support to ensure a sustainable and equitable digital transformation in Indonesia.

METHOD

This research employs a literature review method as the primary approach, as it is considered the most appropriate for thoroughly exploring the concepts, principles, and cybersecurity practices that have been examined by experts and official institutions. This approach enables the researcher to identify trends, compare various frameworks, and understand the development of regulations and standards applied at both global and national levels.

The data sources used include scientific journals and academic books discussing cybersecurity theories and implementations, global security reports from international institutions such as the Verizon Data Breach Investigations Report (DBIR) and the Symantec Internet Security Threat Report (ISTR), as well as official regulatory and standard documents such as ISO/IEC 27001, the NIST Cybersecurity Framework, the Electronic Information and Transactions Law (UU ITE), the Personal Data Protection Law (UU PDP), and the General Data Protection Regulation (GDPR).

By integrating these authoritative sources, this research aims to present a comprehensive analysis of the role of cybersecurity as a key pillar of data protection in the digital era, while also highlighting the relevance of implementing international standards in shaping national policies in Indonesia.

RESULTS AND DISCUSSION

Based on a literature review of various sources such as the Verizon Data Breach Investigations Report (DBIR) 2023, the World Economic Forum Global Cybersecurity Outlook 2024, and the 2023 Indonesia Cyber Security Annual Report by BSSN, it was found that the level of cyber threats worldwide, including in Indonesia, has increased significantly from year to year.

Verizon (2023) notes that around 74% of data breach incidents are caused by human factors, whether in the form of negligence, system misconfiguration, or weak basic security practices. BSSN (2023) also reported more than 370 million cyber traffic anomalies in Indonesia throughout 2023, with the most common types of threats being phishing, malware, ransomware, and data leakage.

These data indicate that the main challenges in cybersecurity are not only technical in nature, but are also closely related to human factors and suboptimal organizational governance. This phenomenon shows that investment in security technologies alone is not sufficient without being accompanied by increased awareness and a strong culture of digital security at all levels of organizations and society.

In theoretical terms, cybersecurity is built upon the three core principles of the CIA Triad (Confidentiality, Integrity, Availability), which serve as the foundation of all data protection policies and security systems.

a. **The principle of confidentiality** is maintained through access control and data encryption using technologies such as AES, RSA, and TLS to ensure that sensitive information is not

accessed by unauthorized parties.
b. **The principle of integrity** is ensured through the use of hashing algorithms such as SHA-256 and audit trail systems to guarantee that data is not altered without authorization.
c. **The principle of availability** is supported through system redundancy, cloud backup, and disaster recovery plans (DRP), ensuring that systems remain functional even during attacks or technical disruptions.

The implementation of the CIA Triad principles is further developed within the ISO/IEC 27001:2022 framework, the international standard for Information Security Management Systems (ISMS). According to a study by Sari and Wibowo (2023), institutions that consistently implement ISO 27001 experience a reduction of up to 40% in data breach incidents due to systematic processes ranging from risk identification and security controls to periodic audits. This approach strengthens information security governance, in which cyber risk management becomes a strategic responsibility shared by all elements of the organization, not just the IT department.

In addition, the adoption of Zero Trust Architecture (ZTA) has emerged as a modern strategy to address increasingly sophisticated cyberattacks. This concept emphasizes the principle of "never trust, always verify," where every user, device, and application must be verified before being granted access—even if they originate from within the organization's network. Yaqin and Suryana (2022) show that the implementation of Zero Trust Architecture in national digital infrastructure can reduce lateral movement attacks and accelerate the detection of network anomalies. This strategy is highly relevant in the era of cloud computing and remote work, when traditional network boundaries have become increasingly blurred.

In the Indonesian context, efforts to strengthen cybersecurity are supported by various regulations, such as Law No. 11 of 2008 on Electronic Information and Transactions (UU ITE) and Law No. 27 of 2022 on Personal Data Protection (UU PDP). The PDP Law is an important milestone because it mandates data controllers to protect personal data through principles of transparency, accountability, and security. However, its implementation still faces several challenges, such as limited skilled human resources, low public digital literacy, and regulatory gaps across government institutions.

Beyond domestic approaches, cross-sector and international collaboration also play an essential role in strengthening cyber resilience. Interpol (2022), in its Global Cybercrime Report, emphasizes the need for cross-border collaborative responses to tackle transnational threats such as financial cybercrime, online fraud, and attacks on critical infrastructure. Globally, the concept of Cyber Resilience is now widely adopted as a new paradigm, highlighting an organization's adaptive and responsive capabilities against recurring attacks. This approach aligns with the ISO/IEC 27005 risk management cycle based on the Plan–Do–Check–Act (PDCA) principle, which ensures information security is maintained through continuous evaluation and improvement.

In practice, strengthening cybersecurity as a pillar of data protection requires a holistic approach that integrates technology, governance, and human factors. Organizations need to move beyond a purely compliance-based mindset and adopt a risk-based approach that continuously evaluates emerging threats and business impacts. This includes conducting regular vulnerability assessments and penetration testing, integrating security into system development life cycles (DevSecOps), and implementing continuous monitoring through

Security Operations Centers (SOC) and Security Information and Event Management (SIEM) solutions. Equally important is the development of a strong security culture through structured awareness programs, phishing simulations, and clear incident reporting mechanisms that empower employees to act as the "first line of defense." For Indonesia, aligning national regulations with international best practices—while considering local socio-economic conditions—is crucial to avoid a mere "tick-box" implementation. Collaboration between government, the private sector, academia, and civil society is also needed to build shared threat intelligence and standardized incident response procedures. Through this integrated and collaborative approach, cybersecurity can function not only as a technical safeguard but also as a strategic enabler of trust in digital transformation and sustainable national development.

As digital ecosystems continue to expand under globalization, cybersecurity is no longer merely a technical concern but has evolved into a strategic national and organizational priority. The increasing interdependence of global information systems means that a single vulnerability can cascade across borders, industries, and institutions. Consequently, cybersecurity must be understood as a multidimensional discipline encompassing technological safeguards, governance frameworks, human behavior, and international cooperation.

At the strategic level, cybersecurity plays a critical role in protecting national interests and economic stability. Digital infrastructure now supports essential services such as banking, healthcare, transportation, energy distribution, and government administration. Disruptions to these systems can result in significant financial losses and social instability. Therefore, cybersecurity is increasingly recognized as part of national security policy. Many countries have established dedicated cyber agencies and national cyber strategies to coordinate defense mechanisms, intelligence sharing, and incident response. For Indonesia, the role of the National Cyber and Crypto Agency (BSSN) is central to orchestrating cybersecurity initiatives across government institutions and critical sectors.

However, institutional readiness remains uneven. While large organizations may possess advanced security capabilities, small and medium enterprises often lack resources and expertise. This asymmetry creates systemic vulnerabilities, as attackers frequently exploit weaker entities to gain access to larger networks through supply chain attacks. Hence, cybersecurity strategies must extend beyond individual organizations and address ecosystem-wide resilience.

Human factors remain one of the most significant vulnerabilities in cybersecurity. Despite advances in encryption, firewalls, and intrusion detection systems, social engineering attacks such as phishing continue to be among the most effective attack vectors. Employees who lack cybersecurity awareness may unintentionally expose sensitive data or compromise credentials. Studies consistently show that a substantial percentage of security incidents originate from human error rather than technological failure.

Building a strong security culture is therefore essential. This involves regular training programs, simulated cyberattack exercises, and clear policies regarding acceptable digital behavior. Security awareness should not be limited to technical staff; all employees, including executives, must understand their role in safeguarding organizational assets. Leadership commitment is particularly important, as it shapes organizational attitudes toward cybersecurity investment and compliance.

From a technological perspective, cybersecurity architectures are undergoing rapid transformation. Traditional perimeter-based security models are increasingly inadequate in cloud-native and hybrid environments. The widespread adoption of mobile devices, remote work, and Internet of Things (IoT) technologies has dissolved conventional network boundaries. As a result, organizations are shifting toward identity-centric security models, where access decisions are based on continuous verification of user identity, device posture, and contextual risk.

Artificial intelligence and machine learning are now widely applied in threat detection and response. These technologies enable security systems to analyze vast volumes of network traffic and identify anomalies in real time. Automated incident response mechanisms can isolate compromised systems and mitigate damage before human intervention becomes necessary. However, attackers also leverage AI to develop more sophisticated malware and evade detection, leading to an ongoing technological arms race.

IoT security presents another emerging challenge. Smart devices deployed in homes, factories, and cities often lack robust security controls and are rarely updated after installation. Compromised IoT devices can be used to launch distributed denial-of-service (DDoS) attacks or serve as entry points into corporate networks. As Indonesia advances smart city initiatives and industrial digitalization, securing IoT ecosystems must become a policy priority.

Data protection has also become increasingly complex in a globalized environment. Cross-border data flows are essential for cloud services, e-commerce, and multinational operations, yet they raise concerns regarding jurisdiction, privacy, and accountability. Organizations must navigate diverse regulatory landscapes while ensuring compliance with domestic laws such as Indonesia's Personal Data Protection Law. Effective data governance frameworks are required to classify data, define ownership, and establish clear protocols for data sharing and retention.

The economic implications of cybersecurity are substantial. Cyber incidents can disrupt business operations, erode customer trust, and damage corporate reputation. According to various global estimates, the cost of cybercrime now rivals that of traditional organized crime. Investment in cybersecurity should therefore be viewed not as an expense but as a strategic investment in business continuity and competitiveness.

For developing economies, cybersecurity capacity building is closely linked to digital economic growth. Investors are more likely to engage in markets where digital infrastructure is secure and regulatory frameworks are transparent. Strengthening cybersecurity can thus enhance national attractiveness for foreign investment and support the expansion of digital industries.

Cybersecurity also intersects with issues of digital inclusion. Marginalized communities may face greater exposure to online scams and misinformation due to limited digital literacy. As governments promote digital services, ensuring that citizens understand how to protect themselves online becomes a matter of social equity. Public education campaigns, community training centers, and accessible cybersecurity resources can help bridge this gap.

Ethical considerations are increasingly prominent in cybersecurity discourse. Surveillance technologies, biometric systems, and data analytics tools can enhance security but also pose risks to civil liberties. Balancing security objectives with individual rights requires

transparent governance mechanisms and independent oversight. Ethical frameworks should guide the deployment of security technologies to prevent abuse and discrimination.

In the international arena, cybersecurity cooperation is both necessary and challenging. Cyber threats do not respect national borders, yet geopolitical tensions often hinder collaboration. Establishing norms of responsible state behavior in cyberspace remains an ongoing effort within forums such as the United Nations (UN). Regional cooperation platforms, including ASEAN, offer opportunities for joint capacity building, information sharing, and coordinated responses to cyber incidents.

Cyber diplomacy is emerging as a key component of foreign policy, encompassing negotiations on digital trade, data protection standards, and cyber norms. For Indonesia, active participation in these discussions enables the country to influence global governance frameworks while safeguarding national interests.

Education and research play a foundational role in advancing cybersecurity capabilities. Universities must adapt curricula to include practical cybersecurity skills, ethical reasoning, and interdisciplinary perspectives. Research institutions can contribute by developing locally relevant security solutions and conducting threat analyses tailored to regional contexts. Collaboration between academia and industry is essential to ensure that graduates possess skills aligned with real-world needs.

Workforce development remains a pressing issue. The global shortage of cybersecurity professionals continues to widen, creating intense competition for talent. Indonesia can address this challenge through scholarships, certification programs, and vocational training initiatives that encourage young people to pursue careers in cybersecurity. Inclusive policies that promote participation by women and underrepresented groups can further expand the talent pool.

Looking forward, cybersecurity must be embedded into the broader digital transformation agenda. Security-by-design principles should guide the development of new systems and applications, rather than being retrofitted after deployment. Integrating security into software development processes (DevSecOps) ensures that vulnerabilities are identified and addressed early in the lifecycle.

Resilience is another critical concept shaping modern cybersecurity strategies. Rather than focusing solely on prevention, organizations must prepare for the inevitability of breaches by developing robust incident response and recovery capabilities. This includes maintaining backups, conducting tabletop exercises, and establishing communication protocols for crisis situations. Cyber resilience emphasizes the ability to adapt, recover, and continue operations in the face of disruption.

For Indonesia, achieving cyber resilience requires coordinated efforts across government, industry, academia, and civil society. National policies must be supported by practical implementation, adequate funding, and continuous evaluation. Public–private partnerships can facilitate knowledge transfer and resource sharing, while community engagement initiatives can foster grassroots awareness.

In conclusion, cybersecurity in the era of globalization is a complex and evolving challenge that extends far beyond technical controls. It encompasses strategic governance, human behavior, economic development, ethical responsibility, and international cooperation. The integration of frameworks such as the CIA Triad, ISO/IEC 27001, and Zero Trust

Architecture provides a solid foundation, but sustainable cybersecurity requires continuous adaptation to emerging threats and technologies.

For Indonesia, strengthening cybersecurity is essential to realizing the full potential of digital transformation. By investing in human capital, enhancing regulatory coherence, promoting ethical practices, and fostering collaborative ecosystems, the nation can build a secure and inclusive digital future. Ultimately, cybersecurity should be understood not merely as a defensive mechanism but as a strategic enabler of trust, innovation, and sustainable development in a globally interconnected world.

As digital transformation accelerates worldwide, the concept of cybersecurity is increasingly intertwined with digital sovereignty—the ability of a nation to control its digital assets, infrastructure, and data governance. In a globalized economy, where cloud services, software platforms, and hardware supply chains are dominated by multinational corporations, maintaining sovereignty becomes both complex and critical. Countries must strike a delicate balance between leveraging global technological ecosystems and preserving national autonomy.

For Indonesia, digital sovereignty involves securing national data, strengthening domestic technological capabilities, and reducing dependence on foreign infrastructure. The establishment of the National Data Center represents an important step toward consolidating government data and improving security oversight. However, sovereignty extends beyond infrastructure; it also encompasses regulatory authority, talent development, and innovation capacity. Without strong domestic expertise, reliance on external vendors can limit strategic flexibility and expose critical systems to geopolitical risks.

One of the most significant future challenges in cybersecurity is the exponential growth of data. The proliferation of IoT devices, social media platforms, and digital services generates massive volumes of information that must be stored, processed, and protected. Big Data analytics offers powerful insights for economic planning and public services, yet it also increases the attack surface for cybercriminals. Advanced Persistent Threats (APTs) increasingly target sensitive datasets, including biometric records and health information, which can have long-lasting consequences if compromised.

To address this, organizations must adopt advanced data-centric security models. These models prioritize encryption, tokenization, and access control at the data level rather than relying solely on network defenses. Privacy-enhancing technologies (PETs), such as secure multi-party computation and homomorphic encryption, are emerging as promising tools that allow data to be analyzed without exposing raw information. Although still in early stages of adoption, these technologies could redefine how sensitive data is shared across borders while maintaining confidentiality.

Cybersecurity governance must also evolve to accommodate the pace of technological change. Static regulations often struggle to keep up with innovations such as artificial intelligence (AI), blockchain, and autonomous systems. Agile regulatory approaches, including regulatory sandboxes and adaptive policy frameworks, enable governments to test new technologies under controlled conditions. This allows policymakers to learn from real-world implementation while minimizing systemic risks.

Artificial intelligence itself introduces new dimensions of cyber risk. AI systems can be manipulated through data poisoning, model inversion, and adversarial attacks, potentially

leading to inaccurate decisions or security breaches. Protecting AI pipelines—from data collection to model deployment—requires specialized security controls and ethical oversight. Moreover, transparency in AI decision-making is essential to ensure accountability, particularly in high-stakes applications such as law enforcement and financial services.

Another emerging concern is the security of supply chains. Modern digital systems rely on complex networks of software components and hardware manufacturers spread across multiple countries. Vulnerabilities introduced at any point in this chain can compromise entire ecosystems. Recent global incidents have demonstrated how compromised software updates or embedded hardware backdoors can facilitate widespread attacks. Strengthening supply chain security requires rigorous vendor assessments, Software Bill of Materials (SBOM) documentation, and continuous monitoring of third-party risks.

The role of cloud computing in future cybersecurity strategies cannot be overstated. While cloud platforms offer scalability and advanced security features, they also concentrate risk. Misconfigured cloud environments remain a leading cause of data breaches. Organizations must develop cloud security competencies, including identity and access management, secure configuration practices, and shared responsibility awareness. National guidelines and certification schemes can help standardize cloud security practices across industries.

In parallel, the rise of remote work has permanently altered organizational security postures. Employees accessing corporate systems from diverse locations and devices increase exposure to cyber threats. Endpoint security, secure remote access solutions, and continuous authentication mechanisms are now fundamental components of enterprise security architectures. Zero Trust principles become particularly relevant in this context, as trust is no longer based on physical network location but on verified identity and behavior.

Cybersecurity also plays a critical role in protecting democratic processes. Election systems, public information platforms, and media channels are increasingly targeted by disinformation campaigns and cyber interference. Safeguarding digital democracy requires coordinated efforts between electoral bodies, technology companies, and civil society organizations. Media literacy programs can empower citizens to critically evaluate online content, reducing the impact of misinformation.

Economic resilience is closely linked to cybersecurity maturity. Digital disruptions can cascade through supply chains, financial systems, and public services. Integrating cybersecurity into national risk management frameworks ensures that cyber threats are considered alongside natural disasters and economic shocks. Scenario planning and cyber stress testing can help governments and organizations prepare for worst-case scenarios.

Capacity building remains a cornerstone of sustainable cybersecurity. Technical solutions alone are insufficient without skilled professionals to design, operate, and maintain them. National scholarship programs, international training partnerships, and professional certification pathways can strengthen workforce pipelines. Encouraging interdisciplinary education—combining IT with law, economics, and social sciences—fosters holistic perspectives on cyber risk.

Community-level engagement further enhances resilience. Local governments, schools, and small businesses often lack dedicated security resources, making them attractive targets for attackers. Establishing regional cybersecurity centers and community outreach programs

can provide practical support and raise awareness. Such initiatives ensure that cybersecurity benefits are distributed beyond major urban centers.

Internationally, trust-building measures are essential to reduce cyber conflict. Confidence-building mechanisms, incident notification protocols, and joint exercises can improve transparency and cooperation between states. Although geopolitical tensions persist, pragmatic collaboration on cybercrime prevention and critical infrastructure protection remains in the shared interest of all nations.

Ultimately, cybersecurity must be integrated into broader sustainability agendas. Digital infrastructure consumes significant energy and resources, prompting the need for environmentally responsible security practices. Green cybersecurity initiatives—such as energy-efficient data centers and sustainable hardware procurement—align digital growth with climate goals.

In conclusion, future-oriented cybersecurity strategies require a comprehensive approach that addresses technological innovation, governance reform, human development, and international cooperation. For Indonesia, strengthening digital sovereignty while remaining engaged in the global digital economy is both a challenge and an opportunity. By adopting adaptive policies, investing in talent, and fostering collaborative ecosystems, the nation can build resilient digital foundations that support inclusive economic growth.

Cybersecurity should thus be viewed not merely as a protective shield but as an integral component of national development strategy. When aligned with ethical principles and social inclusion, it becomes a powerful enabler of trust, innovation, and long-term prosperity in an increasingly interconnected world.

CONCLUSION

Based on the findings of the literature review, it can be concluded that cybersecurity is a fundamental pillar of data protection in the digital era. Digital transformation indeed brings convenience and efficiency across various sectors, but it also introduces increasingly complex cyber threats. Therefore, cybersecurity is not merely a technical matter; it must also form part of organizational governance, regulatory frameworks, and public awareness.

The application of the CIA Triad principles (Confidentiality, Integrity, Availability), the ISO/IEC 27001 standard, and the Zero Trust Architecture (ZTA) serves as an essential foundation for building a strong data protection system. The success of these frameworks depends on the synergy between technology, risk management, and compliance with regulations such as the Electronic Information and Transactions Law (UU ITE) and the Personal Data Protection Law (UU PDP).

Although regulations are in place, challenges persist in terms of implementation, particularly the limited availability of skilled professionals and low levels of digital literacy. Therefore, collaboration between the government, the private sector, and the public is needed to strengthen the national cybersecurity ecosystem. Ultimately, cybersecurity is not only about protecting data; it also plays a vital role in safeguarding public trust, economic stability, and the nation’s digital sovereignty.

BIBLIOGRAPHY

Al Kinoon, M. (2024). *A comprehensive and comparative examination of healthcare data breaches: assessing security, privacy, and performance*.

European Union. (2018). *General Data Protection Regulation (GDPR).* Official Journal of the European Union.

Fatah, M., & Ngamal, Y. (2025). Digital paradox in Indonesia's GovTech transformation. *Communicator: Journal of Communication, 2*(2), 110–127. https://doi.org/10.59373/comm.v2i2.171

Iskandar, R. (2025). Digital citizenship literacy in Indonesia: The role of privacy awareness and participation. *Computers & Education: Digital Learning, 1*(3), 55–69. https://doi.org/10.1016/j.caeai.2025.00XXX

Kim, J., & Jin, W. (2024). Impact of digital capabilities on entrepreneurial performance in SMEs. *Journal of Innovation & Knowledge, 9*(3), Article 100538. https://doi.org/10.1016/j.jik.2024.100538

Lestari, R., & Rachmawati, A. (2022). Digital literacy gaps and the challenges of cyber security in Indonesia's peripheral areas. *International Journal of Digital Society, 13*(1), 45–57. https://doi.org/10.20533/IJDS.2040.2570.2022.0106

Lythreatis, S., Singh, S. K., & El-Kassar, A.-N. (2022). The digital divide: A review and future research agenda. *Technological Forecasting and Social Change, 175*, Article 121359. https://doi.org/10.1016/j.techfore.2021.121359

Mia, M. A., Nasir, S., & Hasan, M. (2024). Digital infrastructure and innovation: Digital divide or digital dividend? *Journal of Innovation & Knowledge, 9*(2), Article 100524. https://doi.org/10.1016/j.jik.2024.100524

Muñoz-Arteaga, J., Vargas-Archila, J. A., & Rodríguez-Flores, T. (2024). Bridging the digital divide: Exploring the challenges and solutions for digital exclusion in rural South Africa. *Discover Global Society, 2*(1), 89. https://doi.org/10.1007/s44282-025-00189-2

Osawaru, G. (2024). *Electronic health record data breaches in US healthcare industry: a quantitative study using the protection motivation theory (PMT) to mitigate data breaches*. University of the Cumberlands.

Pimenta Rodrigues, G. A., Marques Serrano, A. L., Lopes Espiñeira Lemos, A. N., Canedo, E. D., Mendonça, F. L. L. de, de Oliveira Albuquerque, R., Sandoval Orozco, A. L., & García Villalba, L. J. (2024). Understanding data breach from a global perspective: Incident visualization and data protection law review. *Data*, *9*(2), 27.

Pratama, R. A., & Handayani, P. W. (2021). Analisis manajemen risiko siber menggunakan ISO/IEC 27005: Studi kasus pada lembaga pemerintahan. *Jurnal Sistem Informasi Indonesia, 6*(1), 33–44.

Priyono, A., Moin, A., & Putri, V. N. A. O. (2024). Linking digital capability to small business performance: The mediating role of digital business transformation. *Cogent Business & Management, 11*(1), Article 2342486. https://doi.org/10.1080/23311975.2024.2342486

Rahayu, S. K., Budiarti, I., Firdauas, D. W., & Onegina, V. (2023). Digitalization and informal MSME: Digital financial inclusion for MSME development in the formal economy. *Journal of Eastern European and Central Asian Research, 10*(1), 1–15. https://doi.org/10.15549/jeecar.v10i1.1234

Setiawan, A., & Lestari, R. (2020). Literasi keamanan siber dan kesadaran digital di era transformasi teknologi. *Jurnal Ilmu Komputer dan Informasi, 15*(3), 112–120.

Tao, H., Bhuiyan, M. Z. A., Rahman, M. A., Wang, G., Wang, T., Ahmed, M. M., & Li, J. (2019). Economic perspective analysis of protecting big data security and privacy. *Future Generation Computer Systems*, *98*, 660–671.

Thornton, J., & Thornton, A. (2024). ICT4D and the capability approach: Understanding how freedom of expression on ICTs affects human development at the country-level. *Information Technology for Development, 30*(2), 145–168. https://doi.org/10.1080/02681102.2024.2337048

Wickham, M. H. (2019). *Exploring data breaches and means to mitigate future occurrences in healthcare institutions: A content analysis*. Northcentral University.

Zahoor, N., Zopiatis, A., Adomako, S., & Lamprinakos, G. (2023). The micro-foundations of digitally transforming SMEs: How digital literacy and technology interact with managerial attributes. *Journal of Business Research, 159*, Article 113748. https://doi.org/10.1016/j.jbusres.2023.113748