Berajah Journal
Published by: CV Lafadz Jaya | ISSN: 2797-1805 | E-ISSN: 2797-1882

Volume 6 No. 1 (2026)
Page: 488 – 498
https://ojs.berajah.com/index.php/go/

CYBERSECURITY LAW AND LEGAL RESPONSES TO DATA BREACHES IN GOVERNMENT INSTITUTIONS

Yeni Santi[1]*, Rahmatiyah[2], Agus Prasetyo[3]
Universitas Terbuka
***Email Correspondence:** yenisanti@ecampus.ut.ac.id

Received: 15-03-2026 | **Revised:** 25-03-2026 | **Accepted:** 05-04-2026 | **Published:** 25-04-2026

Abstract

This study aims to analyze the cybersecurity legal framework and legal responses to data breach incidents in government institutions. As the digitalization of public services increases, threats to data security are becoming increasingly complex and have a broad impact on public trust and the stability of state administration. The method used in this study is a literature review, examining various academic sources, regulations, and policy reports related to cybersecurity and data protection in the public sector. This approach allows for the identification of regulatory patterns, legal weaknesses, and best practices in handling data breaches across various jurisdictions. The results of the study indicate that although many countries have developed regulations related to cybersecurity and data protection, gaps remain in their implementation, inter-agency coordination, and law enforcement mechanisms. Legal responses to data breaches in government institutions are often reactive and do not fully prioritize the principles of prevention and risk mitigation. Furthermore, the lack of uniform security standards and limited human resources are major challenges in strengthening government information security systems. Therefore, this study emphasizes the importance of regulatory harmonization, institutional capacity building, and the adoption of a proactive approach to cyber risk management to improve the effectiveness of data protection in the public sector..

Keywords: *Cyber Security, Data Breaches, Cyber Law, Government Institutions, Data Protection*

INTRODUCTION

Developments in information and communication technology have driven massive digital transformation across various sectors, including government administration. The digitization of public services not only increases efficiency and transparency but also expands public access to various administrative services (Mariam, 2024). However, behind this progress, significant new risks have emerged, particularly related to cybersecurity. Government institutions, which store and manage large amounts of data, including citizens' personal data, have become highly attractive targets for cybercriminals. In this context, data breaches have become a crucial issue, impacting not only technical and financial losses but also impacting public trust in the government.

The phenomenon of data leaks in government institutions demonstrates the gap between the acceleration of digitalization and adequate security system readiness. Many data leaks occur due to weak protection systems, a lack of security awareness, and suboptimal implementation of information security policies (Mugamba, 2025a). Furthermore, the ever-evolving complexity of cyber threats, such as ransomware attacks, phishing, and advanced persistent threats (APTs), further complicates data protection efforts. This situation indicates that a purely technical approach is insufficient; it must be supported by a strong and responsive legal framework.

In the legal realm, the existence of regulations related to cybersecurity and data protection is a crucial foundation for addressing the threat of data breaches. Laws serve not only as a preventative instrument through setting security standards, but also as an enforcement mechanism that provides sanctions for violations and protects victims (Xhixho et al., 2025). However, in practice, many countries, including Indonesia, still face challenges in formulating and implementing regulations that are comprehensive and

DOI: https://doi.org/10.47353/bj.v6i2.655

adaptable to the dynamics of cyber threats. Regulatory fragmentation, overlapping authority between institutions, and weak law enforcement are major obstacles to creating an effective cybersecurity ecosystem.

Furthermore, legal responses to data breaches in government institutions are often reactive and not yet systematically integrated. Case handling still focuses on technical and administrative aspects, while legal accountability and the protection of individual rights have not yet been fully prioritized. Yet, from a modern legal perspective, personal data protection is a human right that must be guaranteed by the state (Fan, 2023a). Therefore, a more holistic approach that integrates legal, technological, and governance aspects is needed to address data breach incidents.

On the other hand, developments in global cyber law indicate a trend toward strengthening data protection regulations and increasing the accountability of public institutions. Various countries have adopted stricter legal frameworks, including mandatory incident reporting, the implementation of minimum security standards, and the imposition of strict sanctions for violations. This demonstrates that an effective legal response depends not only on the existence of regulations but also on their consistent implementation and enforcement. In this context, it is crucial for government institutions not only to comply with existing regulations but also to develop internal capacity to manage cybersecurity risks (Shaik et al., 2025).

This research is relevant because it seeks to deeply examine how cybersecurity law plays a role in responding to data breach incidents in government institutions. Using a literature review method, this study will explore various legal approaches that have been implemented, identify existing weaknesses and challenges, and offer perspectives for strengthening a more adaptive and responsive legal framework. This study is expected to contribute academically to the development of cyber law and serve as a reference for policymakers in formulating more effective data protection strategies.

The urgency of this research is further strengthened by the increasing frequency and impact of data breaches, which not only harm individuals but also have the potential to disrupt national stability. In an increasingly connected digital era, data security has become an integral part of national security. Therefore, strengthening cybersecurity law and legal responses to data breaches is no longer merely a technical necessity but a strategic priority in modern governance. Therefore, this research is expected to provide a comprehensive understanding of the importance of integrating legal and technological aspects in addressing cybersecurity challenges in government institutions.

LITERATURE REVIEW

Personal Data Protection Regulations in the Government Sector

Personal data protection regulations in the government sector have become an increasingly crucial issue with the increasing digitalization of public services and the use of information technology in governance. The digital transformation adopted by various government agencies has boosted service efficiency, transparency, and accountability, but also opens up the potential risk of leaks and misuse of public personal data. In this context, the existence of comprehensive and implementable regulations is a key foundation for ensuring data security and maintaining public trust in government institutions.

In Indonesia, the strengthening of personal data protection regulations is marked by the enactment of the Personal Data Protection Law (PDP Law), which provides a legal framework for personal data management, including in the government sector. This regulation emphasizes that personal data is an individual right that must be protected, therefore, every government agency as a data controller is obliged to ensure that data collection, processing, storage, and distribution are carried out legally, transparently, and

DOI: https://doi.org/10.47353/bj.v6i2.655

responsibly. In practice, this requires a paradigm shift from merely administrative data management to data management based on the principle of protecting citizens' privacy rights (Rahman, 2025).

One important aspect of this regulation is the principle of legality and a clear purpose in data processing. Government agencies are only permitted to collect data relevant to their duties and functions, and must have a strong legal basis. This aims to prevent excessive data collection practices that can increase the risk of privacy violations. Furthermore, the regulation emphasizes the importance of the principles of data minimization and purpose limitation, which state that collected data may not be used beyond the specified purposes without the consent of the data owner.

In its implementation, the challenges faced by the government sector relate not only to legal aspects but also to infrastructure and human resource readiness. Many government agencies are still in the early stages of implementing adequate information security systems. Weaknesses in technological systems, such as a lack of encryption, suboptimal access management, and minimal security audits, can create opportunities for data leaks (Dumanska et al., 2022). Therefore, personal data protection regulations must be accompanied by supporting technical policies, including strict cybersecurity standards and ongoing monitoring mechanisms. Furthermore, organizational culture plays a crucial role in the effectiveness of regulations. Civil servants' awareness of the importance of personal data protection still needs to be improved. In many cases, data leaks are caused not only by external attacks but also by internal negligence, such as the use of unsecured devices or the distribution of data without clear procedures. Therefore, regulations need to be supported by ongoing education and training programs to improve data security literacy among government employees.

Personal data protection regulations also address the rights of data subjects, such as the right to know, access, correct, and delete their personal data. In the government sector, the fulfillment of these rights is an important indicator of accountability and transparency. However, the implementation of these rights often faces administrative and technical obstacles, especially in systems that are not yet optimally integrated (Marwenny et al., 2024). Therefore, the development of an integrated and responsive information system is necessary to ensure that people's rights are fulfilled effectively.

Oversight and law enforcement are key elements in ensuring compliance with regulations. Without a strong oversight mechanism, regulations will remain merely formal norms that are difficult to implement in practice. In this context, the role of independent oversight bodies is crucial to conduct audits, investigate, and impose sanctions for violations. The administrative and criminal sanctions stipulated in the regulations are expected to have a deterrent effect and encourage government agencies to be more serious about protecting personal data.

Furthermore, collaboration between government agencies is also a crucial factor in creating an effective data protection ecosystem. Data exchange between agencies must be conducted with due regard for security and confidentiality principles, and supported by a secure interoperability system. Without proper coordination, the potential for data leaks will increase, especially in systems involving multiple parties. Therefore, regulations need to establish clear and standardized data exchange mechanisms.

Cybersecurity Integration in E-Government Governance

The integration of cybersecurity into e-government governance is a necessity amidst the government's increasing reliance on digital technology in the delivery of public services (Jha & Jha, 2024). The massive digital transformation in the government sector not only brings efficiency and transparency but also opens up new vulnerabilities to increasingly complex and organized cyber threats. Therefore,

DOI: https://doi.org/10.47353/bj.v6i2.655

cybersecurity can no longer be positioned as a purely technical aspect but must become an integral part of a good governance framework. This integration requires synergy between policies, technology, human resources, and an organizational culture oriented toward information security.

In the context of e-government governance, cybersecurity serves as the foundation for maintaining public trust in government digital systems. Data security is a crucial issue given that the government manages a variety of sensitive information, including citizens' personal data, financial information, and strategic state documents. Without an adequate security system, the potential for data leaks and cyberattacks can result in economic losses, disrupt national stability, and even diminish the government's legitimacy in the eyes of the public. Therefore, cybersecurity integration must be realized through comprehensive and implementable policies capable of anticipating and responding adaptively to various forms of cyber threats.

Furthermore, the integration of cybersecurity into e-government also requires a strong and consistent regulatory framework. The government needs to establish binding information security standards for all agencies, both at the central and regional levels. These regulations must cover data protection, cyber risk management, and security incident handling mechanisms. Furthermore, cross-agency coordination is necessary to ensure that cybersecurity policies are not implemented in isolation but are integrated within a coherent governance system. This approach is crucial to avoid policy fragmentation, which could weaken the effectiveness of protecting the government's digital infrastructure (Raza, 2024).

From an implementation perspective, the integration of cybersecurity into e-government requires significant investment in technological infrastructure and human resource capacity development. Technologies such as data encryption, intrusion detection systems, and identity and access management must be widely adopted to protect government information systems. However, technology alone is insufficient without the support of competent human resources in cybersecurity. Therefore, the government needs to develop training and certification programs for civil servants to increase awareness and skills in dealing with cyber threats. A culture of information security must also be instilled as part of the work ethic within a modern bureaucracy.

Furthermore, the integration of cybersecurity into e-government governance must also consider risk management aspects. The government needs to continuously identify, analyze, and mitigate risks across all digital systems used. This risk-based approach allows the government to prioritize protection of the most critical assets and allocate resources more effectively. In this regard, the implementation of a standardized cyber risk management framework can help improve government preparedness for various threat scenarios (Shah et al., 2022).

Equally important, collaboration with the private sector and the international community is also a key factor in strengthening cybersecurity in e-government. Cyber threats are cross-border, so addressing them requires collaboration involving various parties. The government can leverage partnerships with technology companies to adopt innovative security solutions and participate in international forums to share information and best practices in cybersecurity management. This collaboration not only increases national capacity but also strengthens the country's position in the global cybersecurity ecosystem.

Ultimately, the integration of cybersecurity into e-government governance is a continuous and dynamic process. Rapid technological developments require the government to continuously adapt and improve its security systems. Therefore, a long-term commitment from all stakeholders is needed to make cybersecurity a strategic priority in e-government development. With effective integration, e-government

DOI: https://doi.org/10.47353/bj.v6i2.655

can not only provide efficient and transparent services, but also secure and reliable services for the entire community.

METHOD

This study employs a qualitative approach, employing a literature review, to provide an in-depth analysis of the development of cybersecurity law and legal responses to data breaches within government institutions. The data used is secondary data obtained from various credible scientific sources, such as reputable international journals, conference proceedings, academic books, official agency reports, and regulatory documents related to cybersecurity and personal data protection. Data collection was conducted through searches of electronic databases such as Google Scholar, Scopus, and accredited national journal portals using relevant keywords, including "cybersecurity law," "data breach," "government institutions," and "legal response." Inclusion criteria were established to ensure the relevance and quality of the sources, including publication within a specific timeframe, peer-reviewed, and a focus on the legal and policy context of cybersecurity in the public sector.

The collected data was systematically selected, categorized, and synthesized to generate a comprehensive understanding of the effectiveness of existing regulations and the challenges of their implementation within government. In this process, researchers also compared studies to identify similarities and differences in legal approaches across countries, thus providing a broader perspective. The results of the analysis are then interpreted critically to formulate theoretical and practical implications that are relevant to strengthening policies and legal systems in dealing with cybersecurity threats in the government sector.

RESULTS AND DISCUSSION

Comparing Cybersecurity Regulations Across Countries as Policy Learning

The rapid development of digital technology has pushed countries around the world to develop increasingly complex and diverse cybersecurity regulatory frameworks. These differences in regulatory approaches are influenced not only by the level of technological advancement but also by legal systems, national interests, and perspectives on data protection and national security (Odebade & Benkhelifa, 2023). Therefore, comparing cybersecurity regulations across countries is crucial as a basis for policy learning, particularly for developing countries like Indonesia in formulating adaptive, effective, and contextual policies.

Within the European Union, cybersecurity and data protection regulations tend to be comprehensive and integrated. One key regulation is the General Data Protection Regulation (GDPR), which serves as the global standard for personal data protection. The GDPR emphasizes the principles of transparency, accountability, and individual rights over their data, including the right to access, correct, and delete personal data. This regulation also has extraterritorial powers, applying to companies outside the European Union that process data on EU citizens. In addition to the GDPR, the European Union has also developed other regulations, such as the Digital Services Act and the Digital Markets Act, which expand the scope of oversight of digital platforms. This approach demonstrates the EU's prioritization of individual rights protection and digital governance that balances innovation and security (Saleem et al., 2024).

Unlike the EU, the United States adopts a more sectoral and flexible approach to cybersecurity regulation. Its common law-based legal system means that regulation in the United States is not centralized in a single law, but rather spread across various sector-specific rules, such as the Health Insurance Portability

DOI: https://doi.org/10.47353/bj.v6i2.655

and Accountability Act (HIPAA) for the healthcare sector and the Gramm-Leach-Bliley Act (GLBA) for the financial sector. Furthermore, non-mandatory frameworks, such as the NIST Cybersecurity Framework, provide best practice guidance for organizations. This approach allows for rapid adaptation to technological developments, but also presents challenges in the form of inconsistent standards across sectors and compliance complexity for industry players (Mugamba, 2025b).

Meanwhile, China demonstrates a very different approach, placing cybersecurity as an integral part of national security and state sovereignty. Key regulations, such as the Cybersecurity Law, which has been in effect since 2017, emphasize mandatory data localization, strict oversight of network operators, and mandatory cooperation with state authorities on information security. These regulations are reinforced by the Data Security Law and Personal Information Protection Law, which govern data classification, personal information protection, and control of cross-border data transfers. China's approach reflects a focus on state control and the protection of strategic national interests, often at the expense of individual freedom and data transparency (Ngozi Samuel Uzougbo et al., 2024a).

In Southeast Asia, cybersecurity and data protection regulations tend to be still developing and not yet fully standardized. Singapore, for example, has adopted the Personal Data Protection Act (PDPA) and the Cybersecurity Act, which regulate organizations' obligations in managing data and protecting critical infrastructure. However, compared to the GDPR, regulations in this region are generally considered less stringent and have varying levels of enforcement. Indonesia itself has passed the Personal Data Protection Law (PDP Law) as a significant step in strengthening data security, although its implementation still faces challenges, such as infrastructure readiness, institutional capacity, and business awareness.

This comparison shows that there are three main models of global cybersecurity regulation: the individual rights protection model (European Union), the flexible sector-based model (United States), and the state control model (China). Each model has its advantages and disadvantages. The EU model excels in protecting privacy rights but tends to be complex and expensive to implement. The United States model is more adaptable to innovation but lacks consistency in protection standards. Meanwhile, the Chinese model is effective in maintaining national stability but has the potential to limit digital freedom and transparency (Mishra et al., 2022).

From a policy learning perspective, Indonesia and other developing countries can take a hybrid approach by adopting best practices from various models. For example, the GDPR's rights-based data protection principles can be combined with regulatory flexibility, as in the United States, and with strengthening critical infrastructure security, as in China. Furthermore, it is important to pay attention to implementation aspects, including strengthening oversight bodies, increasing digital literacy, and collaboration between the government and the private sector (Mishra et al., 2022).

Thus, comparing cybersecurity regulations across countries not only provides insight into the diversity of legal approaches but also serves as a source of strategic learning in designing policies responsive to digital security challenges. In an increasingly connected global context, regulatory harmonization and international cooperation are also key factors in addressing cross-border cyber threats, so national policies cannot stand alone without considering evolving global dynamics.

The Role of Data Protection Laws in Preventing Information Security Breaches

The role of data protection laws in preventing information security breaches has become increasingly crucial amidst the rapid digital transformation that is changing the way individuals, organizations, and

DOI: https://doi.org/10.47353/bj.v6i2.655

governments manage and utilize data. Personal data is now viewed not merely as information but as a strategic asset with significant economic, social, and political value. This situation has led to an increased risk of information security breaches, whether in the form of data leaks, misuse of personal information, or increasingly complex cyberattacks. In this context, data protection laws serve as a legal instrument that provides a normative framework for regulating how data is collected, processed, stored, and protected from unauthorized access (Chukwudi Tabitha Aghaunor et al., 2023).

Data protection laws play a preventive role by establishing security standards that all data management entities must adhere to. Provisions regarding mandatory implementation of technical and organizational measures serve as a key foundation for preventing information security breaches. These include the implementation of encryption, access control, security audits, and structured risk management policies (Pimenta Rodrigues et al., 2024). With these obligations, organizations can no longer ignore security as an option, but rather as a legal obligation that must be met. The implication of this regulation is the creation of a culture of compliance that encourages organizations to proactively identify and mitigate potential vulnerabilities in their information systems.

Furthermore, data protection laws also play a role in strengthening the accountability of data managers. The principle of accountability requires organizations not only to comply with legal provisions but also to demonstrate that they have taken adequate steps to protect data. In practice, this is realized through documented security policies, incident reporting, and regular evaluation mechanisms for data protection systems. With these mechanisms in place, any information security breaches can be systematically traced, facilitating investigations and law enforcement. Furthermore, accountability also encourages transparency to the public, ultimately increasing public trust in institutions that manage data.

Another important role of data protection laws lies in regulating the rights of data subjects. The right to know, access, correct, and erase personal data gives individuals greater control over their own information. With these rights, individuals can play an active role in overseeing the use of their personal data, thereby minimizing the potential for misuse (Gudepu & Jaladi, 2022). In the context of preventing information security breaches, the active participation of data subjects is a crucial element that complements the protection efforts undertaken by organizations and the state. This creates a collaborative data protection ecosystem, where responsibility does not rest solely with one party.

Data protection laws also have an equally important repressive function, namely through the imposition of sanctions for violations. Administrative sanctions, fines, and even criminal sanctions are law enforcement instruments aimed at deterring perpetrators. These sanctions serve not only as punishment but also as an effective deterrent. Organizations will tend to be more careful in managing data if there is a risk of significant legal consequences. In the long term, consistent law enforcement will create higher compliance standards across all sectors, thereby systematically reducing the rate of information security breaches.

Furthermore, data protection laws play a role in promoting the harmonization of information security standards at the national and international levels. In the era of digital globalization, cross-border data flows are inevitable (Fan, 2023b). Therefore, regulatory alignment between countries is crucial to ensure that data remains protected even when processed in different jurisdictions. Comprehensive data protection laws typically adopt universal principles such as lawful processing, data minimization, and purpose limitation. By adopting these principles, a country can enhance international trust and facilitate global cooperation in the field of information security.

DOI: https://doi.org/10.47353/bj.v6i2.655

On the other hand, the success of data protection laws in preventing information security breaches also depends heavily on the effectiveness of their implementation. Frequent challenges include limited resources, lack of organizational awareness, and technological developments that outpace regulations (Li et al., n.d.). Therefore, ongoing efforts are needed in the form of outreach, capacity building, and regulatory updates to maintain their relevance to technological dynamics. The government also needs to strengthen oversight bodies with the authority to conduct independent audits, investigations, and law enforcement.

In the Indonesian context, strengthening the role of data protection laws is crucial given the increasing number of data breach incidents in recent years. Digital transformation in the public and private sectors must be balanced with adequate data protection systems to prevent new risks to the public. Data protection laws serve not only as regulatory tools but also as instruments for building digital trust, a key foundation for developing a data-driven economy.

Challenges in Implementing Cybersecurity Law in Government Institutions

The implementation of cybersecurity law in government institutions faces complex and multidimensional challenges, particularly with the acceleration of digital transformation in governance. On the one hand, the digitalization of public services provides greater efficiency, transparency, and accessibility for the public. However, on the other hand, increased reliance on digital systems also opens up vulnerabilities to increasingly sophisticated cyber threats. The primary challenge in implementing cybersecurity law lies in the gap between rapid technological developments and the regulatory capacity to keep pace. Existing regulations are often reactive and lag behind the dynamics of cyber threats, making it difficult to provide adequate legal protection for government data and systems (Hafiz Abdul Rehman Saleem et al., 2025).

One crucial challenge is the limited harmonization of regulations across government institutions. In many cases, cybersecurity regulations are scattered across various sectoral regulations that are not always systematically integrated (Lawal Qudus, 2025). This leads to overlapping authority, inconsistencies in policy implementation, and confusion in law enforcement when cybersecurity incidents occur. Government institutions often have varying security standards, creating security gaps that cybercriminals can exploit. Furthermore, a lack of coordination between agencies hampers a swift and integrated response to cyberattacks, which should require a cross-sectoral and collaborative approach.

Another challenge relates to human resource capacity in understanding and implementing cybersecurity laws. Government officials do not always possess adequate technical competence or legal understanding related to cybersecurity. This results in weak implementation of information security policies, both in prevention and incident response. The lack of ongoing training and minimal investment in digital competency development exacerbate this situation. As a result, even when regulations are in place, their implementation is suboptimal due to limited capacity of implementers on the ground (Savaş & Karataş, 2022).

Furthermore, challenges arise from the organizational culture within government institutions. Awareness of the importance of cybersecurity remains relatively low, especially at the managerial level, which is not directly involved in technical aspects. Cybersecurity is often seen as solely the responsibility of the information technology unit, rather than as an integral part of organizational risk management. In fact, cyber threats have strategic implications that can impact the stability of public services, public trust, and even national security. This low awareness leads to a lack of commitment in allocating budgets and resources to strengthen cybersecurity systems.

DOI: https://doi.org/10.47353/bj.v6i2.655

From a law enforcement perspective, challenges arise in terms of evidence and jurisdiction. Cybercrime has cross-border characteristics, complicating investigation and prosecution. Perpetrators can operate from multiple countries using sophisticated anonymity technology, making them difficult to track and identify. Furthermore, international cooperation mechanisms for cyber law enforcement are not yet fully effective, particularly in developing countries with limited access and capacity for digital diplomacy. This results in low prosecution rates for cybercriminals, which ultimately reduces the deterrent effect (Supriya Dhananjay Paigude, 2024).

Another challenge is the limited technological infrastructure supporting the implementation of cybersecurity laws. Many government institutions still use legacy systems that are not designed to meet modern security standards. Integrating legacy and new systems often creates additional vulnerabilities that are difficult to address without significant investment. Furthermore, budget constraints hinder comprehensive technological infrastructure modernization. This creates a dilemma between the need to increase security and the limited resources available.

Personal data protection is also a significant challenge in the implementation of cybersecurity laws in government institutions. The government, as the manager of public data, has a significant responsibility to maintain the confidentiality and integrity of public data. However, in practice, data leaks often occur due to weak security systems and lack of compliance with existing regulations. This challenge is exacerbated by the lack of oversight mechanisms and strict sanctions for data security breaches. Without clear accountability, the implementation of cybersecurity laws is less effective in providing optimal protection.

Furthermore, the development of new technologies such as artificial intelligence, the Internet of Things (IoT), and cloud computing also adds complexity to the implementation of cybersecurity laws. These technologies bring significant benefits, but also expand the attack surface that must be protected. Existing regulations often fail to accommodate the new risks arising from the use of these technologies. This calls for an adaptive and risk-based regulatory approach that anticipates future technological developments (Ngozi Samuel Uzougbo et al., 2024b).

In the context of public policy, the challenge of implementing cybersecurity laws also relates to the need to balance security and individual freedom. Efforts to improve cybersecurity often involve increased scrutiny of digital activity, which can raise concerns about privacy and human rights. Therefore, a legal framework is needed that is not only effective in protecting systems and data but also respects democratic principles and civil liberties. Overall, the challenges of implementing cybersecurity law in government institutions reflect the complex interactions between technological, legal, organizational, and social aspects. Addressing these challenges requires a holistic and integrated approach, involving strengthening regulations, increasing human resource capacity, modernizing infrastructure, and enhancing security awareness and culture across the organization. Without comprehensive efforts, the implementation of cybersecurity law will continue to face obstacles that could hinder the creation of a secure and trustworthy digital government system.

CONCLUSION

This research confirms that the development of information technology in governance has increased the complexity of cybersecurity risks, particularly related to data breach incidents that have a broad impact on public trust and the stability of state institutions. The existing legal framework generally accommodates the principles of data protection and information security, but its implementation still faces various obstacles

DOI: https://doi.org/10.47353/bj.v6i2.655

such as limited institutional capacity, lack of coordination between institutions, and suboptimal law enforcement mechanisms. Legal responses to data breaches within the government tend to be reactive, necessitating a more preventative approach through strengthened regulations, standardized system security, and increased legal and technological literacy among state officials.

Furthermore, this research also shows that the effectiveness of legal responses is greatly influenced by the integration of cybersecurity policies with transparent and accountable governance practices. Handling data breach incidents requires not only legal sanctions but also a comprehensive recovery strategy, including protection of data subjects and continuous security system improvements. Therefore, legal reforms that adapt to the dynamics of cyber threats, as well as collaboration between the government, the private sector, and the public, are needed to build a resilient digital security ecosystem. Thus, strengthening cybersecurity laws not only serves as a control instrument, but also as a foundation for building public trust in digital-based government services.

REFERENCES

Chukwudi Tabitha Aghaunor, Patience Eshua, Tawo Obah, & Oluwatoyin Aromokeye. (2023). Data security strategies to avoid data breaches in modern information systems. *World Journal of Advanced Research and Reviews*, *20*(3), 2122–2144. https://doi.org/10.30574/wjarr.2023.20.3.2515

Dumanska, I. Y., Guseva, O. Y., Kazarova, I. O., Gorodetskyy, M., Melnichuk, L. V., & Saienko, V. H. (2022). *Personal Data Protection Policy Impact on the Company Development*. https://elar.khmnu.edu.ua/handle/123456789/12535

Fan, J. (2023a). Legal Policies Failing on Data Breaches?–An Empirical Study of U.S. Information Security Law Implementations. *Procedia Computer Science, Tenth International Conference on Information Technology and Quantitative Management (ITQM 2023)*, *221*, 971–978. https://doi.org/10.1016/j.procs.2023.08.076

Fan, J. (2023b). Legal Policies Failing on Data Breaches?–An Empirical Study of U.S. Information Security Law Implementations. *Procedia Computer Science, Tenth International Conference on Information Technology and Quantitative Management (ITQM 2023)*, *221*, 971–978. https://doi.org/10.1016/j.procs.2023.08.076

Gudepu, B. K., & Jaladi, D. S. (2022). Data Discovery and Security: Protecting Sensitive Information. *International Journal of Acta Informatica*, *1*(1), 176–187.

Hafiz Abdul Rehman Saleem, Ali Bukhtiar, Babar Zaheer, & Muhammad Asad Ullah Farooq. (2025). Challenges Faced by the Judiciary in Implementing Cybersecurity Laws in Pakistan. *The Critical Review of Social Sciences Studies*, *3*(1), 1052–1066. https://doi.org/10.59075/1wyx0v30

Jha, R. K., & Jha, M. (2024). Optimizing E-Government Cybersecurity through Artificial Intelligence Integration. *Journal of Trends in Computer Science and Smart Technology*, *6*(1), 67–87. https://doi.org/10.36548/jtcsst.2024.1.005

Lawal Qudus. (2025). Cybersecurity governance: Strengthening policy frameworks to address global cybercrime and data privacy challenges. *International Journal of Science and Research Archive*, *14*(1), 1146–1163. https://doi.org/10.30574/ijsra.2025.14.1.0225

Li, W. W., Leung, A. C. M., & Yue, W. T. (n.d.). *Where is IT in Information Security? The Interrelationship among IT Investment, Security Awareness, and Data Breaches1*. Retrieved April 24, 2026, from https://dx.doi.org/10.25300/MISQ/2022/15713

Mariam, S. (2024). Legal and Ethical Challenges in International Cybersecurity: Addressing Cross-Border Data Breaches. *Journal of Advances in Cybersecurity Science, Threat Intelligence, and Countermeasures*, *8*(12), 22–32.

Marwenny, E., Syafwar, R., & Yani, P. (2024). Personal Data Protection in Public Services. *Jurnal Ilmiah Ekotrans & Erudisi*, *4*(2), 74–85. https://doi.org/10.69989/yjew5p90

Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity Enterprises Policies: A Comparative Study. *Sensors*, *22*(2), 538. https://doi.org/10.3390/s22020538

Mugamba, E. (2025a). GLOBAL DATA GOVERNANCE IN DIGITAL LAW: A COMPARATIVE ANALYSIS OF EU AND GLOBAL APPROACHES TO CYBERSECURITY LEGISLATION. *Journal of Smart Computing and Quantum Technologies*, *1*(1), 10–28. https://doi.org/10.63456/jscqt-1-1-39

Mugamba, E. (2025b). GLOBAL DATA GOVERNANCE IN DIGITAL LAW: A COMPARATIVE ANALYSIS OF EU AND GLOBAL APPROACHES TO CYBERSECURITY LEGISLATION. *Journal of Smart Computing and Quantum Technologies*, *1*(1), 10–28. https://doi.org/10.63456/jscqt-1-1-39

Ngozi Samuel Uzougbo, Chinonso Gladys Ikegwu, & Adefolake Olachi Adewusi. (2024a). Cybersecurity compliance in financial institutions: A comparative analysis of global standards and regulations. *International Journal of Science and Research Archive*, *12*(1), 533–548. https://doi.org/10.30574/ijsra.2024.12.1.0802

Ngozi Samuel Uzougbo, Chinonso Gladys Ikegwu, & Adefolake Olachi Adewusi. (2024b). Cybersecurity compliance in financial institutions: A comparative analysis of global standards and regulations. *International Journal of Science and Research Archive*, *12*(1), 533–548. https://doi.org/10.30574/ijsra.2024.12.1.0802

Odebade, A. T., & Benkhelifa, E. (2023). *A Comparative Study of National Cyber Security Strategies of ten nations* (arXiv:2303.13938). arXiv. https://doi.org/10.48550/arXiv.2303.13938

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. https://doi.org/10.3390/data9020027

Rahman, F. (2025). SAFEGUARDING PERSONAL DATA IN THE PUBLIC SECTOR: UNVEILING THE IMPACT OF THE NEW PERSONAL DATA PROTECTION ACT IN INDONESIA. *UUM Journal of Legal Studies*, *16*(1), 1–18. https://doi.org/10.32890/uumjls2025.16.1.1

Raza, D. A. (2024). A REVIEW OF CYBERSECURITY THREATS IN E-GOVERNMENT SYSTEMS: TOWARDS SECURE DIGITAL GOVERNANCE. *Multidisciplinary Research in Computing Information Systems*, *4*(3), 131–142. https://doi.org/10.71465/mrcis74

Saleem, B., Ahmed, M., Zahra, M., Hassan, F., Iqbal, M. A., & Muhammad, Z. (2024). A survey of cybersecurity laws, regulations, and policies in technologically advanced nations: A case study of Pakistan to bridge the gap. *International Cybersecurity Law Review*, *5*(4), 533–561. https://doi.org/10.1365/s43439-024-00128-y

Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: An overview of cybersecurity governance. *International Cybersecurity Law Review*, *3*(1), 7–34. https://doi.org/10.1365/s43439-021-00045-4

Shah, I. A., Habeeb, R. A. A., Rajper, S., & Laraib, A. (2022). The Influence of Cybersecurity Attacks on E-Governance. In *Cybersecurity Measures for E-Government Frameworks* (pp. 77–95). IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-7998-9624-1.ch005

Shaik, N., Chandana, B. H., Chitralingappa, P., & Sasikala, C. (2025). Protecting in the Digital Age. In *Next-Generation Systems and Secure Computing* (pp. 105–135). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781394228522.ch6

Supriya Dhananjay Paigude. (2024). A Review of Cybersecurity Policies in the Public Sector: Challenges and Solutions. *Computer Fraud and Security*, 07–12. https://doi.org/10.52710/cfs.28

Xhixho, E., Pazylov, N., Savchenko, V., Patiev, N., & Pazylova, M. (2025). Digital transformation in the legal sector: Challenges and opportunities for cybersecurity and data protection. *Law, State and Telecommunications Review*, *17*(1). https://ora.ox.ac.uk/objects/uuid:417c3c66-ff7c-49da-88a1-f5ee46574da7