Agile Governance and Innovation Measurement Journal
ISSN: xxxx-xxxx (print), xxxx-xxxx (Online)
Vol 2, No 1 (2025): Page no: 40-58

Strengthening Cybersecurity: A Comparative Analysis of Agile Governance in Preventing Data Leakage in Indonesia and Malaysia

Rasya Raditya Hariana[1], Efriza Nur Hadi[2], Adinda Putri Jamal[3]
[1,2] International Program of Government Affairs and Administration, Universitas Muhammadiyah Yogyakarta, Indonesia
[3] Department of International Relations, Universitas Muhammadiyah Yogyakarta, Indonesia
Corresponding Author: rasyaradityahr@gmail.com

Article Info

Article History;
Received:
2025-03-11
Revised:
2025-03-26
Accepted:
2025-03-27
Published:
2025-03-27

Abstract: This research examines the implementation of Agile Governance in mitigating data breaches to strengthen cybersecurity by comparing strategies between Indonesia and Malaysia. As digital transformation accelerates, the risk of cyber threats, including data breaches, continues to increase. Using a comparative approach, this research analyzes the six key principles of Agile Governance: Good Enough Governance, Business-Driven, People-Focused, Based on Quick Wins, Systematic and Adaptive Approach, and Simple Design and Continuous Improvement. Findings show that Malaysia exhibits a more comprehensive cybersecurity framework, supported by early enacted regulations such as the Personal Data Protection Act (PDPA) of 2010, coordinated policies under the National Cyber Security Agency (NACSA), and structured response mechanisms such as MyCERT. In contrast, despite having implemented the Personal Data Protection Act (PDP Act) by 2022 and the role of the National Cyber and Crypto Agency (BSSN), Indonesia still faces regulatory gaps, weak inter-agency coordination, and inadequate infrastructure. This study highlights Malaysia's proactive stance in cybersecurity policy development and resource allocation, contrasting with Indonesia's continued improvements in digital security regulations and public awareness initiatives. The findings of this study suggest that Indonesia can adopt Malaysia's strategic regulatory approach and improve institutional coordination to enhance its cybersecurity resilience. This research contributes to the policy discussion to improve the national cybersecurity framework and calls for further studies on the effectiveness of policy implementation in reducing data breaches.

Keywords: *Cybersecurity Governance, Data Protection, Policy Adaptation*

INTRODUCTION

In the growing digital era, cyber security is crucial in maintaining the stability of a country's data and information. Cyber Security itself is carried out to keep up with the flow of globalization that runs with digital and technological developments, as well as the community's needs to communicate, transact, and store data efficiently and effectively. The effects of globalization make it easier for humans to keep up with the times and make it easy to do things through digital systems. Therefore, it is very important always to improve the quality of Cyber Security to provide a sense of security for every digital user so that the data owned is not misused by someone (Dicoding Intern, 2023). If cybersecurity is weak, various cyber threats, such as hacking, identity theft, malware, and data leaks, can easily occur. Data leakage is an incident where sensitive information, whether belonging to individuals, companies, or governments, is exposed or accessed by

unauthorized parties due to cyberattacks, negligence, or security gaps in digital systems. The impact can be wide-ranging, from misuse of personal data for fraud to damage to an organization's reputation. On a larger scale, data leaks involving strategic state information can threaten national stability and public security (AD-INS, 2023). Indonesia itself, the quality of cyber security is still relatively low. According to Annur (2022), the National Cyber Security Index (NCSI) Report noted that Indonesia's cybersecurity index score was 38.96% out of 100 in 2022. This figure puts Indonesia in the 3rd lowest rank among G20 countries. Globally, Indonesia is ranked 83rd out of 160 countries. As a result of the low quality of cyber security in Indonesia, many cyber crimes must be faced, one of which is data leakage. Meanwhile, Malaysia has relatively strong cyber security standards. Quoted from Muhamad (2023) states that in a report from the National Cyber Security (NCSI), Malaysia is confirmed as a country that has the best cyber security in Southeast Asia with a score of 79.22% out of 100 in 2023. Globally, Malaysia is ranked 22nd out of 160 countries. Malaysia was also ranked third in the Global Cybersecurity Index 2017. The strong quality of Cyber Security is due to strict policies and collaboration with the government and private sector, so the cyber threat in Malaysia is low.

According to Surfshark's cybersecurity breach statistics, Indonesia recorded 176,450,684 million accounts that experienced data leaks in the country in 2024. While Malaysia recorded 60,783,781 million leaked data accounts in 2024, the number of data leaks in Indonesia is almost three times greater than in Malaysia. This indicates the need to increase awareness of digital security, strengthen personal data protection regulations, and implement more sophisticated security technologies to prevent similar incidents in the future (Surfshark, 2025). Although Indonesia passed the Personal Data Protection Law (PDP Law) in 2022, its implementation still faces various challenges, including a lack of infrastructure, weak inter-agency coordination, and low levels of cybersecurity literacy among the public (JDIH BPK, 2022). In contrast, Malaysia has developed a more mature cybersecurity strategy through clear regulations and stricter law enforcement mechanisms. Malaysia itself adopted a stricter cybersecurity policy with the implementation of the Personal Data Protection Act (PDPA) in 2010 (Kementrian Digital Malaysia, 2010). This indicates a gap in policy and implementation between the two countries. The comparison between the two countries is relevant to understand how effective strategies can be implemented in strengthening the cybersecurity system especially in Indonesia. The government must always work on all these challenges quickly because in this era of digitalization, cyber cases will continue to grow and spread widely to the detriment of society and companies, especially in Indonesia itself.

One approach that can be used in improving the quality of cybersecurity is Agile Governance, which emphasizes flexibility, cross-sector collaboration, and policy innovation in dealing with cyber threats. This concept allows the government to respond quickly to the evolving dynamics of digital threats (Firhansyah, 2021). By applying the principles of Agile Governance, Indonesia has the opportunity to improve its cybersecurity governance to be more adaptive and responsive, as has been implemented

in Malaysia. This research aims to analyze how Agile Governance can be implemented to strengthen cybersecurity in Indonesia with reference to the Malaysian case study. This research was conducted due to the high cybersecurity threats in Indonesia. In addition, the cybersecurity quality gap between Indonesia and Malaysia can be seen from the much lower index score and Indonesia's delay in passing data protection regulations. Using a comparative study approach, this research will explore the various policies and strategies implemented in both countries in dealing with cybersecurity threats. The results of this study are expected to provide policy recommendations that the Indonesian government can adopt in strengthening cybersecurity governance more effectively.

LITERATURE REVIEW

Research from (Shahul Ikram, 2024) assessed that data leaks in Malaysia were mainly caused by inadequate security measures, leading to significant business disruptions, financial losses and reputational damage. In line with that, research from Azmi & Zulhuda (2012) discussing the implications of data leaks, particularly through Wikileaks, highlighted concerns over Malaysia's national critical information infrastructure (CII) and the need for legal reforms to address potential data breaches and improve information security in the country. In the face of cyber threats, research from (Pillay & Gowindasamy, 2024) highlights the importance of cybersecurity governance in Malaysia, focusing on the interaction between people, process and technology. It emphasizes human-centered design and alignment of local processes with technological capabilities to enhance defense against evolving cyber threats. Malaysia finally formulated the Personal Data Protection Act 2010 which required amendments to align with international standards for better data security. While in Indonesia, research from (Rizkil et al., 2024) highlighting data leaks in Indonesia is a significant problem, with 35 cases reported from January to June 2023. A total of 377 million personal data records associated with identity cards have been compromised, appearing on the dark web. This data includes sensitive information such as NIK, full name, date of birth, and more. Contributing factors to these leaks include human error, malware, system vulnerabilities, and lack of security awareness, leading to risks such as fraud and identity theft. In the face of cyber threats, Indonesia has created a Personal Data Protection Law (UU PDP) in 2022. However, research from Razi et al. (2024), The PDP Law still faces implementation challenges, including inadequate infrastructure, lack of public awareness, and incidents of data leakage. These obstacles hinder effective enforcement and compliance, requiring improvements to enhance personal data protection in Indonesia. In line with that, research from Sodiq et al. (2024) highlights Indonesia's improved cybersecurity through increased awareness, leadership in Southeast Asia, and rapid digital transformation. However, Indonesia still faces challenges such as a shortage of skilled professionals, limited resources, and a legal framework that requires continuous refinement and adaptation.

Research from Oluwatoyin & Adesola (2024), emphasizes integrating adaptive resilience into the governance framework, enabling real-time adjustments based on threat information. This approach improves cybersecurity by enabling companies to respond effectively to incidents and manage third-party risk, ultimately improving overall security and resilience. In line with that, research from Zaydi et al. (2024) states that by Integrating security and compliance from the beginning of the software development lifecycle through agile methodologies enables organizations to respond quickly to compliance requirements, reduce cybersecurity risks, and turn regulatory constraints into competitive advantages, improving overall cyber resilience. In the implementation of agile governance to minimize data leakage, research from Prem (2025) discusses an adaptive data governance framework, emphasizing policy enforcement and monitoring systems that improve operational efficiency and compliance management, which are critical in minimizing data leakage through effective security controls and risk mitigation strategies across multiple organizational contexts. In line with that, Research from Akoum & Bu Hazzaa (2019) emphasizes the importance of a robust yet agile data governance framework to address data management challenges, including data leakage. Implementing an agile governance structure enables continuous improvement and adaptation to emerging threats. Key aspects include senior management support, proactive change management, and effective communication. Regular reviews of the governance program ensure alignment with evolving business dynamics and regulatory requirements, thereby enhancing the organization's ability to effectively mitigate risks associated with data leakage.

This literature review aims to identify and classify the literature relevant to research on the implementation of Agile Governance in minimizing data leakage for cybersecurity with a comparative study between Indonesia and Malaysia. This research will use 10 scientific journals to identify comparisons from Indonesia and Malaysia. This section will discuss two main aspects that form the basis of this research, namely (1) data leakage and cybersecurity, which includes a study of threats, causal factors, impacts, and strategies to minimize data leakage in Indonesia and Malaysia, as well as regulations that have been implemented in each country, and (2) Agile Governance in cybersecurity, which discusses the concept of Agile Governance, its principles, and its application in strengthening digital security systems. By reviewing previous research related to these two aspects, this study will build a strong conceptual foundation and identify research gaps that can be filled through further analysis.

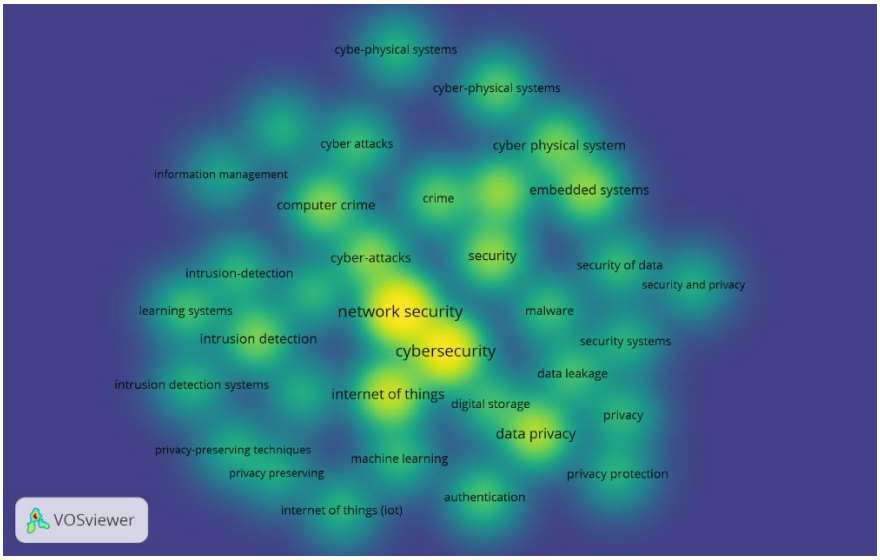

Figure 1. Density Visualization "Cyber Security" and "Digital Governance"

Source: VOSviewer

Density Visualization in VOSviewer shows that the distribution and interconnectedness of concepts in cybersecurity research based on a literature review of 180 Scopus articles. The most prominent keywords such as "cybersecurity", "network security", and "data privacy" confirm that the issue of data leakage is the main focus in the reviewed literature. In addition, the presence of "Internet of Things (IoT)" and "intrusion detection" indicates that data leakage is often associated with IoT devices and intrusion detection systems. In the context of Agile Governance Implementation in Minimizing Data Leakage for Cybersecurity, this visualization shows that agile governance plays a role in dynamically managing data protection, as indicated by the keywords "machine learning", "privacy-preserving techniques", and "authentication", which leads to the utilization of adaptive technologies in cybersecurity. In addition, keywords such as "data leakage", "malware" and "computer crime" emphasize that data leakage is a real threat that requires a quick and flexible response in cybersecurity governance, especially in regions such as Indonesia and Malaysia. Although the term "regulation and governance" does not appear explicitly, its association with "security compliance" in the literature suggests that an Agile Governance approach can be a solution in mitigating data leakage and improving cybersecurity, by emphasizing policy flexibility, technology integration, and cross-sector collaboration in the face of evolving cyber threats.

Theoretical Framework

Agile Governance is the concept of agile governance, or in other words, the ability of government to keep up with the times, and be able to meet the demands of society quickly (Kurniawan et al., 2021). The concept has the ability to sense, adapt, and respond quickly and sustainably to changes in its environment, through a coordinated

combination of agile capabilities with governance capabilities to deliver value faster, better, and more efficiently amidst accelerating globalization (Busri et al., 2023). That way, this concept can be a milestone to overcome and minimize cases of data leakage in Indonesia, which has become a digital problem because it includes globalization that follows developments, and glances at Malaysia, which already has strict and responsive regulations. Realizing an agile government is a goal in governance towards a world-class bureaucracy. In this case, agility is required in interoperability within the government itself. Government agencies will not be connected and integrated with each other if an electronic-based government system is not built (Admin Aptika, 2022).

Agile Governance theory has 6 indicators according to Luna et al. (2015) used to realize agile governance objectives include:

1. Good Enough Governance: Government is a concern for governance. Governance should be tailored to the context and capabilities of the government. This can be achieved if the government can create institutions with the capabilities and needs of the country in dealing with cyber threats.
2. Business-Driven: Every decision and policy must be business process-oriented. This can be achieved if cybersecurity is part of the national strategy and digital economy.
3. Human Focused: Governance needs to prioritize aspects of community participation and involvement. This can be achieved if the government can increase awareness and participation of community users in data protection.
4. Based on Quick Wins: Quick successes are celebrated and become the impetus for more stimuli and results. This can be achieved if the government is quick and responsive in handling data leakage incidents with regular monitoring and evaluation.
5. Systematic and Adaptive Approach: The government must be able to develop the ability to quickly and systematically deal with changes, especially in crisis situations. This can be achieved if the government can design strategies to deal with cyber threats with a systematic and adaptive approach that continues to evolve.
6. Simple Design and Continuous Refinement: The government should be able to get quick results and have improvements. Governance should focus on improving policy effectiveness and efficiency. This can be achieved if the government has simple regulations and digital innovation in cybersecurity.

Agile Governance theory is highly relevant in the research as the concept emphasizes rapid response, policy adaptation and agile governance in the face of cyber threats. Indonesia still faces challenges in data security regulation and implementation,

while Malaysia has more stringent and responsive regulations. Using the six indicators of Agile Governance, this research can evaluate how the two countries implement cybersecurity policies, assess the strategies' effectiveness, and identify steps that Indonesia can adopt to improve its data protection system.

METHOD

This research uses qualitative methods, which aim to understand social phenomena through in-depth non-numerical data collection by exploring meanings, values, and patterns of interaction in a particular social context. Qualitative research is often exploratory and descriptive in nature, which allows researchers to gain deep insight into the subject under study (Fadli, 2021) The approach used for this research is Case Study. Based on Creswell (2014), The case study approach aims to understand in depth certain phenomena in a real context, by focusing on a particular case or subject. In the research, the case study approach was chosen because it allows an in-depth understanding of the implementation of Agile Governance in handling data leaks in Indonesia and Malaysia in a real context. Using a comparative method, this study will review how each government responds to data leakage incidents and the strategies implemented to improve the quality of cybersecurity. The study will analyze real cases to evaluate the policies and regulations' effectiveness. In addition, this research will compare the effectiveness of the two countries in implementing the six Agile Governance indicators to identify policy efforts in improving their cybersecurity governance.

This research will use secondary data from news, scientific journals, and social media to enrich the analysis and understand public perceptions of the government's response in addressing data leaks and improving cybersecurity. Data will be collected through document study and content analysis of secondary sources, then analyzed using thematic coding techniques to identify key patterns and themes that emerge from documents and reports related to data leakage and policy responses. The coding framework will be developed based on Agile Governance theory and its six indicators: policy flexibility, stakeholder engagement and adaptability to technological change. To increase the validity of the results, this research applies source triangulation by comparing data from various sources, such as government policies, public statements, and expressed public perceptions. The data that has been coded and analyzed is then interpreted by linking it to theory to gain a more holistic understanding of the effectiveness of cybersecurity policies in both countries.

RESULTS AND DISCUSSIONS

Agile governance focuses on efficiency, responsiveness, and effectiveness in public services, especially in the face of challenges such as data leakage. The concept of agile governance includes not only the ability to respond quickly to public complaints or reports but also ensuring that complaint management officers have the professional competence to follow up reports effectively and thoroughly, thereby increasing public

satisfaction. An agile government in handling data leaks has a close relationship with public service reform, which emphasizes transparency, accountability, and innovation in the bureaucratic system. Realizing an agile government is a strategic step in building a world-class bureaucracy, where agility is a major factor in improving interoperability between government agencies and encouraging rapid and data-based decision making (Suprastiyo et al., 2023). In the context of cybersecurity, Agile Governance principles should be explicitly defined and developed as key parameters in public service reform. These principles include policy flexibility in responding to cyber threats, active involvement of stakeholders in cybersecurity policy formulation, and adaptability to technological developments to strengthen data defense systems. Therefore, the application of Agile Governance in handling data leaks in Indonesia and Malaysia needs to focus on improving cybersecurity indicators through structural reforms and digitalization of a more adaptive, transparent and collaborative bureaucratic system.

The principles of agile governance are aligned with efforts to digitize public services as both emphasize flexibility, responsiveness, and innovation in the face of rapid change in the digital era. The *Good Enough Governance* principle ensures that policies and regulations are good enough to drive efficiency without being an obstacle to technological development. The *Business-Driven* principle emphasizes that the digitization of public services must be oriented to the needs of the community and the business world, so that the solutions implemented provide real benefits. Furthermore, the *Human Focused* principle ensures that aspects of digital literacy and cybersecurity are considered so that people can use digital services safely and effectively. The *Based on Quick Wins* principle underlines the importance of achieving quick results in digital policy implementation to increase public trust and accelerate the benefits of digital services. Meanwhile, the *Systematic and Adaptive Approach* principle allows the government to manage risks and increase the resilience of digital systems sustainably. Finally, the principle of *Simple Design and Continuous Refinement* ensures that digital services are designed in a simple and accessible manner, with continuous improvement based on user feedback. By applying these principles, the government can create an inclusive, adaptive, and sustainable digital service ecosystem to support the development of a more advanced society in the digital era. To achieve good agile governance and overcome data leakage cases, it is necessary to develop parameters from the principles of agile governance to improve cybersecurity indicators and quality in Indonesia and Malaysia.

Table 1. Comparison of Cybersecurity Agile Governance in Indonesia and Malaysia

Principles	**Indonesia**	**Malaysia**
Good Enough Governance	National Cyber and Crypto Agency (BSSN)	National Cyber Security Agency (NACSA)
Business-Driven	National Strategy for Digital Economy Development 2030	Malaysia Cyber Security Strategy (MCSS) 2020-2024
Human Focused	National Digital Literacy Movement	CyberSAFE (Cyber Security Awareness for Everyone)
Based on Quick Wins	Indonesia Security Incident Response Team on Internet Infrastructure (Id-SIRTII/CC)	Malaysia Computer Emergency Response Team (MyCERT)
Systematic and Adaptive Approach	Resilience	Coordination
Simple Design and Continuous Refinement	Personal Data Protection Law no. 27 by 2022	Personal Data Protection Act 2010

Source: Processed by Author (2025)

The table above shows that to achieve the implementation of Agile Governance, there are efforts given by the governments of Indonesia and Malaysia. In this case, the government must be able to improve the implementation of agile governance in minimizing data leakage to improve cybersecurity. In the growing digital era, cybersecurity is crucial in maintaining economic stability and data protection in a country. Cyber threats, such as data leaks and cyberattacks, can have a serious impact on the public and private sectors. Therefore, both Indonesia and Malaysia have adopted various policies and strategies to strengthen their cybersecurity systems. Some principles need to be evaluated and need to be identified. The application of Agile Governance principles in addressing data leakage in Indonesia and Malaysia is an important step to strengthen data governance and improve cybersecurity. The following

are various efforts that have been implemented by Indonesia and Malaysia in dealing with data leakage incidents in strengthening cybersecurity:

1. Good Enough Governance

Good Enough Governance emphasizes the importance of governance that is tailored to government capabilities as well as the specific needs of a country in facing cybersecurity challenges. In the Good Enough Governance effort, Indonesia has established the National Cyber and Crypto Agency (BSSN) as the main agency in Indonesia that handles signals intelligence, cyber intelligence, cyber defense, and cyber security. BSSN is responsible for protecting national critical infrastructure from cyber-attacks and ensuring the security of government and public data. (Harruma, 2022). BSSN acts as an institution in maintaining national cybersecurity with a focus on protecting critical infrastructure, strengthening regulations, and improving detection and response capabilities to cyber threats. BSSN's efforts include cybersecurity policy development, cross-sector coordination, and public education on data security (SWA, 2025). With its strategic role, in line with good enough governance BSSN supports the strengthening of cybersecurity governance in Indonesia to be in line with the country's needs in facing increasingly complex digital threats.

Meanwhile, Malaysia established the National Cyber Security Agency (NACSA) which acts as the lead agency in strengthening the country's cyber resilience by coordinating various cyber security initiatives at the national level. NACSA seeks to strengthen regulations, increase public awareness of cyber threats, and build cooperation with the private and international sectors to strengthen Malaysia's cyber defense (NACSA, 2024b). One of the important steps taken is the development of a national cybersecurity strategy that focuses on threat mitigation as well as increasing the capacity of human resources in the cyber field. With NACSA in place, Malaysia has a more adaptive, national needs-oriented cybersecurity governance system that is able to address digital challenges with a risk-based approach and cross-sector coordination in line with the principles of good enough governance.

2. Business-Driven

In a business-driven effort where every decision is oriented towards business processes, Indonesia, through its National Strategy for Digital Economy Development 2030, emphasizes the importance of cybersecurity as an integral part of the national strategy and the digital economy. The strategy covers six key pillars, including infrastructure, human resources, business climate and cybersecurity, research and innovation, funding and investment, and policy and regulation (Limanseto, 2023). The strategy aims to increase the contribution of the digital economy to Indonesia's GDP to around 20% by 2030, through the development of network infrastructure, IT infrastructure, and digitized infrastructure including data protection and cybersecurity.

In a business-driven context, the Indonesian government has encouraged cybersecurity as an integral part of digital economic growth by strengthening the role of the National Cyber and Crypto Agency (BSSN) in securing the national digital ecosystem, as well as requiring security certification for technology-based businesses (Indonesia.Go.Id, 2024)

Malaysia, through the Malaysia Cyber Security Strategy (MCSS) 2020-2024, seeks to strengthen cybersecurity as part of its national strategy and digital economy. The strategy encompasses five key pillars namely Governance, legislative strengthening, technology industry innovation, human resource capacity, and global cooperation. The MCSS is designed to increase confidence in the country's cyber environment by setting regulatory standards for national cyber defense (National Security Council, 2020). Through the MCSS, Malaysia allocated more than RM 1.8 billion (approximately USD 400 million) for the strengthening of the national cybersecurity ecosystem, including support for technology companies in improving their security standards. The strategy also supports business development by ensuring regulations do not stifle innovation, but still provide optimal protection for consumers and businesses (Majlis Keselamatan Negara, 2020).

3. Human Focused

Human Focused is a principle in digital governance that emphasizes active participation and engagement of the community in creating a safe digital environment. In Indonesia, the National Digital Literacy Movement is a government initiative that aims to increase people's digital awareness and skills in dealing with cyber threats. The program was initiated by the Ministry of Communication and Information Technology (Kominfo) with a focus on four main pillars, namely digital skills, digital ethics, digital safety, and digital culture (Vania, 2022). In its implementation, the program involves various elements of society, including academics, industry sectors, and communities, to provide comprehensive education related to cybersecurity. Since its launch, the National Digital Literacy Movement has reached more than 24 million participants across Indonesia, through seminars, online trainings, and public campaigns to raise awareness of the importance of personal data protection (Rochman, 2024). With this inclusive and participatory approach, Indonesia seeks to ensure that all levels of society have sufficient understanding in maintaining cybersecurity, thus in line with the Human Focused principle that places community involvement as a key aspect in digital governance.

Meanwhile, Malaysia applies the Human Focused principle through the CyberSAFE (Cyber Security Awareness for Everyone) program managed by CyberSecurity Malaysia, an agency under the Ministry of Communications and Digital Malaysia. The program aims to increase public awareness of cyber threats and how to protect themselves from digital crime, with a focus on educating children, youth, and industry players. Key strategies in the implementation of CyberSAFE include workshops, media campaigns, and hands-on training targeting various groups of people to better

understand cybersecurity risks and mitigation measures to be taken (Haris, 2024). One of the flagship initiatives in this program is the provision of interactive learning modules as well as cyber threat simulations. By strengthening cybersecurity literacy at the individual level, Malaysia ensures that every citizen can play an active role in creating a safer digital environment, in line with the Human Focused principle in cybersecurity governance.

4. Based on Quick Wins

Based on Quick Wins adalah prinsip dalam tata kelola yang menekankan keberhasilan jangka pendek sebagai pendorong untuk mencapai hasil yang lebih besar. Di Indonesia, penerapan prinsip Based on Quick Wins dalam keamanan siber diwujudkan melalui Indonesia Security Incident Response Team on Internet Infrastructure (Id-SIRTII/CC), which acts as an emergency response team to cyber incidents. Id-SIRTII/CC is responsible for monitoring, early detection, and mitigation of cyberattacks on national critical infrastructure, with a fast and responsive approach. One of Id-SIRTII/CC's main strategies is the implementation of a real-time monitoring system to detect anomalies and cyberattacks, which is then accompanied by rapid coordination with relevant agencies to respond to emerging threats (Id-SIRTII/CC, 2018). Success in dealing with incidents quickly can prevent wider impacts, which is in line with the principle of Based on Quick Wins, where a quick response to data leaks is the impetus for improving national cyber resilience (Yogar et al., 2023).

Meanwhile, in Malaysia, the implementation of Based on Quick Wins is done through the Malaysia Computer Emergency Response Team (MyCERT) which operates under CyberSecurity Malaysia. MyCERT is tasked with detecting, analyzing and responding to cybersecurity incidents quickly and systematically, especially in dealing with malware, phishing and data leakage attacks. One of MyCERT's key strategies is to provide Cyber999 service, a cyber incident reporting platform that allows individuals and organizations to quickly report threats and get immediate mitigation solutions. In addition, MyCERT also regularly publishes cyber threat reports and security recommendations to government agencies and industry sectors, to improve preparedness for potential future incidents (MyCERT, 2025). With this rapid detection and response mechanism in place, Malaysia can ensure that any cyber threats are effectively addressed, thus supporting the principle of Based on Quick Wins, where responsive action to data leakage is key in enhancing the country's cybersecurity.

5. Systematic and Adaptive Approach

Systematic and Adaptive Approach is a principle in governance that emphasizes the importance of a structured system, based on clear policies, and the ability to adapt to environmental changes. In Indonesia, the Systematic and Adaptive Approach in cybersecurity is realized through the cyber resilience strategy implemented by the

National Cyber and Crypto Agency (BSSN). Cyber resilience includes strengthening regulations, developing security infrastructure, and increasing human resource capacity in the face of evolving cyber threats. One concrete step is strengthening the early detection system against cyber-attacks through the Electronic-Based Government System (SPBE) that integrates digital security in various government sectors (Muñoz et al., 2022). In addition, BSSN also actively conducts cyber-attack simulations (Cybersecurity Drills) with government agencies and the industrial sector to ensure readiness in facing dynamic threats (Loviana, 2022). With this strategy, Indonesia can adapt quickly to the changing cyber threat landscape, which is by the principle of Systematic and Adaptive Approach, where the cybersecurity system continues to evolve according to new needs and challenges.

In Malaysia, the Systematic and Adaptive Approach is implemented through the national cyber security coordination policy, which is managed by the National Cyber Security Agency (NACSA). NACSA's role is to design cybersecurity policies that are flexible and responsive to changes in technology and digital threats. One of the key strategies implemented is the Cyber Security Act 2024 (ACT 845), which provides the legal basis for strengthening cybersecurity regulations in Malaysia. The CSA aims to improve inter-agency coordination, clarify the responsibilities of the entity handling cybersecurity, the National Critical Information Infrastructure (NCII), as well as ensure compliance with strict security standards (NACSA, 2024a). In addition, Malaysia is also implementing the Malaysia Cyber Security Strategy (MCSS) 2020-2024, which focuses on strengthening regulations, developing security technologies, and enhancing cooperation with the private sector and international organizations (digwatch, 2020). With this systematic and adaptive approach, Malaysia can anticipate and adapt its cybersecurity strategy to changing threats, thus in line with the Systematic and Adaptive Approach principle in maintaining the country's digital resilience.

6. Simple Design and Continuous Refinement

Simple Design and Continuous Refinement is a principle in governance that emphasizes the importance of regulations or systems that are simple, easy to understand, but still open to continuous improvement. In Indonesia, the application of Simple Design and Continuous Refinement in cybersecurity is realized through the Personal Data Protection Law (PDP Law) No. 27 of 2022. This law aims to simplify data protection regulations and provide a clear legal framework for individuals and organizations in managing personal data. With more systematic rules, the PDP Law regulates the rights of data subjects, the obligations of data controllers, and sanctions for data leakage violations, thus creating legal certainty and efficiency in data governance (JDIH BPK, 2022). In addition, the government also continues to refine the implementation of this law through the establishment of an independent supervisory authority to ensure compliance and strengthen data security systems in the public and private sectors (Hidayat, 2020). This move reflects the principles of Simple Design and Continuous

Refinement, where regulations are made simpler but still dynamically evolve to match the ever-changing cybersecurity challenges (Yogar et al., 2022).

In Malaysia, the same approach is implemented through the Personal Data Protection Act (PDPA) 2010, which is designed to protect individuals' personal data in commercial transactions with simple and effective policies. The PDPA provides clear guidelines on how personal data should be collected, stored and processed while setting out the responsibilities of companies in keeping customer information secure. In addition, the regulation undergoes periodic enhancements, with revisions aimed at improving the effectiveness of implementation and ensuring compatibility with new technological developments and cyber threats (Kementrian Digital Malaysia, 2010). One of the initiatives supporting these improvements is the establishment of the Department of Personal Data Protection (JPDP) as a supervisory body that continuously evaluates and optimizes the implementation of the PDPA (mydx.my, 2025). With this approach, Malaysia ensures that regulations remain simple, accessible, yet flexible in adapting to changes in the digital world, in accordance with the principles of Simple Design and Continuous Refinement.

The implementation of Agile Governance in cybersecurity in Indonesia and Malaysia is seen through various indicators, such as Good Enough Governance, Business-Driven, Human Focused, Based on Quick Wins, Systematic and Adaptive Approach, and Simple Design and Continuous Refinement. Indonesia and Malaysia have different strategies, but both prioritize flexibility in regulation, adaptation to cyber threats, and strengthening coordination between the public and private sectors. Indonesia, with BSSN as the centre of cybersecurity management, focuses on protecting critical infrastructure, improving regulation, and digital education through the National Digital Literacy Movement. Malaysia, through NACSA, implements a more comprehensive cybersecurity strategy by allocating greater investment and has a more mature legal framework, such as the Cyber Security Act 2024 (ACT 845) and the Malaysia Cyber Security Strategy (MCSS) 2020-2024. Both countries also implement rapid response to data leakage incidents through Id-SIRTII/CC in Indonesia and MyCERT in Malaysia, which ensures that any threats can be addressed quickly and effectively.

CONCLUSION

This research highlights the comparison of cybersecurity strategies between Indonesia and Malaysia in the context of Agile Governance to minimize data leakage. Through the six leading indicators of Good Enough Governance, Business-Driven, Human Focused, Based on Quick Wins, Systematic and Adaptive Approach, and Simple Design and Continuous Refinement, it can be concluded that Malaysia has a more comprehensive approach to cybersecurity than Indonesia. Malaysia's success in implementing more mature regulations and better coordination between institutions contributes to strengthening a more adaptive and resilient cybersecurity system. Meanwhile, Indonesia

still faces challenges in policy implementation, infrastructure, and inter-agency coordination. In the context of Agile Governance, Malaysia is superior in rapid response to cyber threats, as well as in the implementation of risk-based strategies and mitigation of data leakage, while Indonesia is still in the stage of strengthening regulations and increasing the capacity of human resources.

Based on this study's results, several policy recommendations can be implemented in Indonesia: strengthening cybersecurity infrastructure, improving more effective inter-agency coordination, and accelerating the adoption of AI-based cyber threat detection technology. In addition, Indonesia needs to follow Malaysia's approach in accelerating the revision of data security policies to be more responsive to evolving digital threats. The managerial implications of this study also emphasize the importance of the private sector's role in supporting cybersecurity policies more actively through investment in data security technology and training for the workforce. However, this study has limitations in covering empirical data on the effectiveness of policy implementation in each country. Therefore, future research can focus more on specific data leakage case studies and direct evaluation of the impact of policies implemented in improving cybersecurity in Indonesia and Malaysia.

REFERENCE

AD-INS. (2023). *Memahami Kebocoran Data: Jenis, Penyebab & Dampaknya*. AD-INS. https://www.ad-ins.com/id/our-story/kisah-adins/memahami-kebocoran-data-jenis-penyebab-dan-dampaknya/

Admin Aptika. (2022, October 13). *Menkominfo: Keamanan Data Tanggung Jawab Seluruh Pemangku Kepentingan*. KOMINFO. https://aptika.kominfo.go.id/2022/10/menkominfo-keamanan-data-tanggung-jawab-seluruh-pemangku-kepentingan/

Akoum, M., & Bu Hazzaa, H. (2019, October 21). A Data Governance Framework - The Foundation for Data Management Excellence. *Day 2 Tue, October 22, 2019*. https://doi.org/10.2118/198593-MS

Annur, C. M. (2022, September 13). *Indeks Keamanan Siber Indonesia Peringkat ke-3 Terendah di Antara Negara G20*. Databoks. https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/40085035d61073f/indeks-keamanan-siber-indonesia-peringkat-ke-3-terendah-di-antara-negara-g20

Azmi, I. M. A. G., & Zulhuda, S. P. W. J. S. (2012). Data leak, critical information infrastructure and the legal options: what does wikileaks teach us? *International Journal of Cyber-Security and Digital Forensics*, *1*(3), 226–231.

Busri, Ihyani Malik, & Nur Wahid. (2023). Implementasi Agile Governance pada Reformasi Birokrasi 4.0 di Puslatbang KMP LAN Kota Makassar. *Jurnal Administrasi Publik*, *19*(1), 85–119. https://doi.org/10.52316/jap.v19i1.134

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4th ed.). SAGE.

Dicoding Intern. (2023, May 17). *Cyber Security: Pengertian, Jenis, dan Ancamannya*. Dicoding. https://www.dicoding.com/blog/cyber-security-pengertian-jenis-dan-ancamannya/

digwatch. (2020, August). *Malaysia Cybersecurity Strategy*. Digwatch. https://dig.watch/resource/malaysia-cybersecurity-strategy

Fadli, M. R. (2021). Memahami desain metode penelitian kualitatif. *HUMANIKA*, *21*(1), 33–54. https://doi.org/10.21831/hum.v21i1.38075

Firhansyah, M. (2021, February 15). *Agile Governance dalam Perspektif Pelayanan Publik Propartif*. OMBUDSMAN. https://ombudsman.go.id/artikel/r/artikel--agile-governance-dalam-perspektif-pelayanan-publik-propartif

Haris, A. (2024, June 5). *7 Fungsi CyberSecurity Malaysia*. Log Masuk. https://logmasuk.my/cybersecurity-malaysia/

Harruma, I. (2022, September 16). *Badan Siber dan Sandi Negara: Sejarah, Tugas dan Fungsinya*. KOMPAS.Com. https://nasional.kompas.com/read/2022/09/16/05050021/badan-siber-dan-sandi-negara--sejarah-tugas-dan-fungsinya

Hidayat, R. (2020, August 11). *Tiga Model Pembentukan Otoritas Independen Perlindungan Data Pribadi*. Hukum Online.

Id-SIRTII/CC. (2018). *Sejarah Id-SIRTII/CC*. Id-SIRTII/CC. https://idsirtii.or.id/halaman/tentang/sejarah-id-sirtii-cc.html#:~:text=Menteri%20Komunikasi%20dan%20Informatika%20dalam%20hal%20ini%20menunjuk,melakukan%20pengawasan%20keamanan%20jaringan%20telekomunikasi%20berbasis%20protokol%20internet.

Indonesia.Go.Id. (2024, September 13). *Masa Depan Ekonomi Digital Indonesia, Strategi Menuju 2030*. Indonesia.Go.Id. https://indonesia.go.id/kategori/editorial/8497/masa-depan-ekonomi-digital-indonesia-strategi-menuju-2030?lang=1

JDIH BPK. (2022). *Undang-undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi*. https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

Kementrian Digital Malaysia. (2010). *UU Malaysia PDP 2010 • Perlindungan Data Pribadi*. https://www.pdp.gov.my/ppdpv1/en/akta/pdp-act-2010/

Kurniawan, D. I., Maulana, A., & Wicaksono, I. (2021). AGILE GOVERNANCE SEBAGAI BENTUK TRANSFORMASI INOVASI PEMERINTAH DAERAH. *Repository UNMUH Jember*, 1–9. http://repository.unmuhjember.ac.id/9842/10/10.%20Artikel.pdf

Limanseto, H. (2023, December 4). *Siapkan Guideline bagi Transformasi Digital, Pemerintah Segera Luncurkan Buku Putih Strategi Nasional Pengembangan Ekonomi Digital Indonesia 2030*. KEMENTERIAN KOORDINATOR BIDANG PEREKONOMIAN REPUBLIK INDONESIA. https://www.ekon.go.id/publikasi/detail/5531/siapkan-guideline-bagi-transformasi-digital-pemerintah-segera-luncurkan-buku-putih-strategi-nasional-pengembangan-ekonomi-digital-indonesia-2030

Loviana, K. (2022). Cybersecurity and Cyber Resilience in Indonesia: Challenges and Opportunities. *Center for Digital Society (CfDS)*, 1–5. https://cfds.fisipol.ugm.ac.id/wp-content/uploads/sites/1423/2022/05/Commentaries-Cybersecurity-and-Cyber-Resilience-in-Indonesia-English-2.pdf

Luna, A. J. H. de O., Kruchten, P., & Moura, H. (2015). Agile Governance Theory: conceptual development. *12th International Conference on Management of Technology and Information*, 1–22. https://www.researchgate.net/publication/277141416_Agile_Governance_Theory_conceptual_development

Majlis Keselamatan Negara. (2020, October 19). *Kerajaan lancar Strategi Keselamatan Siber Malaysia RM1.8 bilion*. Majlis Keselamatan Negara. https://www.mkn.gov.my/web/ms/2020/10/19/kerajaan-lancar-strategi-keselamatan-siber-malaysia-rm1-8-bilion/

Muhamad, N. (2023, November 29). *Indeks Keamanan Siber Indonesia Tertinggi ke-5 di ASEAN 2023*. Databoks. https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/5bf8dbfb3998ee8/indeks-keamanan-siber-indonesia-tertinggi-ke-5-di-asean-2023#:~:text=Sementara%20itu%2C%20Malaysia%20dikukuhkan%20sebagai,peringkat%20ke%2D22%20secara%20global

Muñoz, J. L. R., Ojeda, F. M., Jurado, D. L. A., Peña, P. F. P., Carranza, C. P. M., Berríos, H. Q., Molina, S. U., Farfan, A. R. M., Arias-Gonzáles, J. L., & Vasquez-Pauca, M. J. (2022). Systematic Review of Adaptive Learning Technology for Learning in Higher Education. Eurasian Journal of Educational Research, 2022(98), 221–233. https://doi.org/10.14689/ejer.2022.98.014

Mutiarin, D., Wahdania C.S, N., & Misran. (2022). Formulation of e-Participation design in realizing agile government based on technology and information: A case study in Indonesia. International Conference on Public Organization (ICONPO 2021), 209 (Iconpo 2021), 207–214. https://www.atlantis-press.com/proceedings/iconpo-21/125970944

MyCERT. (2025). *MyCERT: Peranan dan Tanggungjawab*. MyCERT. https://www.mycert.org.my/portal/full?id=d8032294-04b2-4ba0-9e46-62c898bb4983

mydx.my. (2025). *Department of Personal Data Protection*. Mydx.My. https://mydx.my/directory/view/department-of-personal-data-protection#:~:text=Jabatan%20Perlindungan%20Data%20Peribadi%20%28JPDP%29%20is%20Malaysia%27s%20independent,Protection%20Act%202010%20%28PDPA%29%20and%20its%20associated%20regulations.

NACSA. (2024a). *CYBER SECURITY ACT 2024 (ACT 854)*. NACSA. https://www.nacsa.gov.my/act854.php

NACSA. (2024b). *National Cyber Security Agency (NACSA), Malaysia*. Kementrian Digital Malaysia. https://www.nacsa.gov.my/

National Security Council. (2020). *Malaysia Cyber Security Strategy 2020-2024*. https://asset.mkn.gov.my/web/wp-content/uploads/sites/3/2019/08/MalaysiaCyberSecurityStrategy2020-2024Compressed.pdf

Oluwatoyin, F. A., & Adesola, O. A. (2024). Advancing Cybersecurity Governance: Adaptive Resilience and Strategic Third-Party Risk Management in Financial Services. *World Journal of Advanced Research and Reviews*, *24*(2), 293–302. https://doi.org/10.30574/wjarr.2024.24.2.3312

Pillay, L., & Gowindasamy, M. (2024). People, processes, and technology in cybersecurity: Malaysian insights. In *Recent Research in Management, Accounting and Economics (RRMAE)* (pp. 633–635). Routledge. https://doi.org/10.4324/9781003606642-139

Prem, K. T. (2025). Implementing Adaptive Data Governance: A Technical Perspective. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *11*(1), 454–462. https://doi.org/10.32628/CSEIT25111244

Razi, F., Tuasikal, H., & Pratiwi Markus, D. (2024). Implementation and Challenges of the Personal Data Protection Law in Indonesia. *Jurnal Indonesia Sosial Teknologi*, *5*(12), 6015–6021. https://doi.org/10.59141/jist.v5i12.1285

Rizkil, M., Herawati, A. R., & Santoso, S. (2024). Protection of Personal Data in the Use of Digital ID Cards against Misuse of Data from Cyber Hack. *Journal La Sociale*, *5*(2), 471–478. https://doi.org/10.37899/journal-la-sociale.v5i2.1132

Rochman, F. (2024, January 8). *Kemenkominfo latih lebih 24 juta orang tentang literasi digital*. ANTARA. https://www.antaranews.com/berita/3905859/kemenkominfo-latih-lebih-24-juta-orang-tentang-literasi-digital#google_vignette

Shahul Ikram, N. A. H. (2024). DATA BREACHES EXIT STRATEGY: A COMPARATIVE ANALYSIS OF DATA PRIVACY LAWS. *Malaysian Journal of Syariah and Law*, *12*(1), 135–147. https://doi.org/10.33102/mjsl.vol12no1.458

Sodiq, M. D., Supono, S., Hendri, F., & Ningsih, E. M. (2024). Kebijakan dan Regulasi Spionase Siber di Indonesia. *Ideas: Jurnal Pendidikan, Sosial, Dan Budaya*, *10*(4), 1183. https://doi.org/10.32884/ideas.v10i4.1909

Suprastiyo, A., Warsono, H., & Astuti, R. S. (2023). *Agile Governance Aplikasi Dalam Pelayanan Publik* (N. Rismawati, Ed.). Widina Bhakti Persada. https://repository.penerbitwidina.com/media/publications/560156-agile-governance-aplikasi-dalam-pelayana-54702dbc.pdf

Surfshark. (2025, January 28). *Data Breach Statistics Globally*. https://surfshark.com/research/data-breach-monitoring

SWA. (2025, February 25). *Bermitra dengan Komdigi dan BSSN, Platform Pencegahan Kejahatan Siber Resmi Diluncurkan*. SWA. https://swa.co.id/read/456877/bermitra-dengan-komdigi-dan-bssn-platform-pencegahan-kejahatan-siber-resmi-diluncurkan

Vania, H. F. (2022, April 13). *Kenalan Yuk dengan 4 Pilar Literasi Digital*. Katadata.Co.Id. https://katadata.co.id/infografik/625689fbd47ce/kenalan-yuk-dengan-4-pilar-literasi-digital

Yogar, B. N. A., Mutiarin, D., & Eko Saputro, M. N. C. (2023). Jogja Smart Service as a Digital Public Services: Based on Agile Governance Perspective. INFOTECH : Jurnal Informatika & Teknologi, 4(1), 105–113. https://doi.org/10.37373/infotech.v4i1.562

Zaydi, M., Maleh, Y., Zaydi, H., Khourdifi, Y., Nassereddine, B., & Bakouri, Z. (2024). Agile security and compliance integration. In *Agile Security in the Digital Era* (pp. 68–91). CRC Press. https://doi.org/10.1201/9781003478676-4