Jurnal Manajemen Pelayanan Publik Vol. 08 No. 02, June 2024
http://dx.doi.org/10.24198/jmpp.v8i2.52212

Addressing The Hurdles: Enhancing Better Policies In Indonesia Cyber Security Management Amidst Uncertainty

[a] Mohammad Fadil Imran; [b] Hendra Gunawan; [c] Dwi Asmoro
[a b c] Police Science College, Jakarta, Indonesia

ABSTRAK

Tujuan dari penelitian ini adalah untuk mengatasi hambatan keamanan siber di Indonesia. Dengan menggunakan tinjauan literatur sistematis (SLR) berdasarkan Scopus dan Google Scholar, penelitian ini mengidentifikasi hambatan nyata seperti terkait infrastruktur, rendahnya kesiapan digitalisasi, dan kelangkaan personel terampil. Permasalahan yang tidak berwujud seperti kerangka hukum dan kekosongan peraturan serta pengabaian keamanan siber di kota pintar juga menjadi perhatian. Untuk mengatasi masalah ini, penelitian ini menyarankan sejumlah rekomendasi kebijakan bagi pemerintah Indonesia, termasuk investasi dalam pengembangan keamanan siber, pembuatan model kematangan keamanan siber, peningkatan kemampuan sumber daya manusia, klarifikasi peran, perbaikan undang-undang, dan promosi manajemen keamanan kolaboratif. Jika diikuti, saran-saran ini berpotensi memperkuat pertahanan keamanan siber Indonesia dan menyediakan lingkungan digital yang lebih aman bagi masyarakat dan perusahaan.

ABSTRACT

The purpose of this study is to address obstacles to cyber security in Indonesia. Using a systematic literature review (SLR) based on Scopus and Google Scholar, this study identifies tangible obstacles such as infrastructure-related, low preparedness for digitalization, and scarcity of skilled personnel. Intangible issues such as legal frameworks and regulatory vacuums and neglect of cyber security in smart cities are also noted. To address these issues, this study suggests a number of policy recommendations for the Indonesian government, including investments in cyber security development, creation of a cyber security maturity model, enhancement of human resource capabilities, role clarification, improved legislation, and promotion of collaborative security management. If followed, these suggestions have the potential to strengthen Indonesia's cyber security defenses considerably and provide a safer digital environment for its residents and enterprises.

ARTICLE HISTORY
Submitted: 02 01 2024
Revised: 15 01 2024
Accepted: 13 02 2024
Published: 1 06 2024

KATA KUNCI
Keamanan Cyber; Ketangguhan; Keamanan Digital; Ancaman Keamanan; Hambatan Digital

KEYWORDS
Cyber Security; Resilience; Digital Security; Security Threats; Digital Obstacles

INTRODUCTION

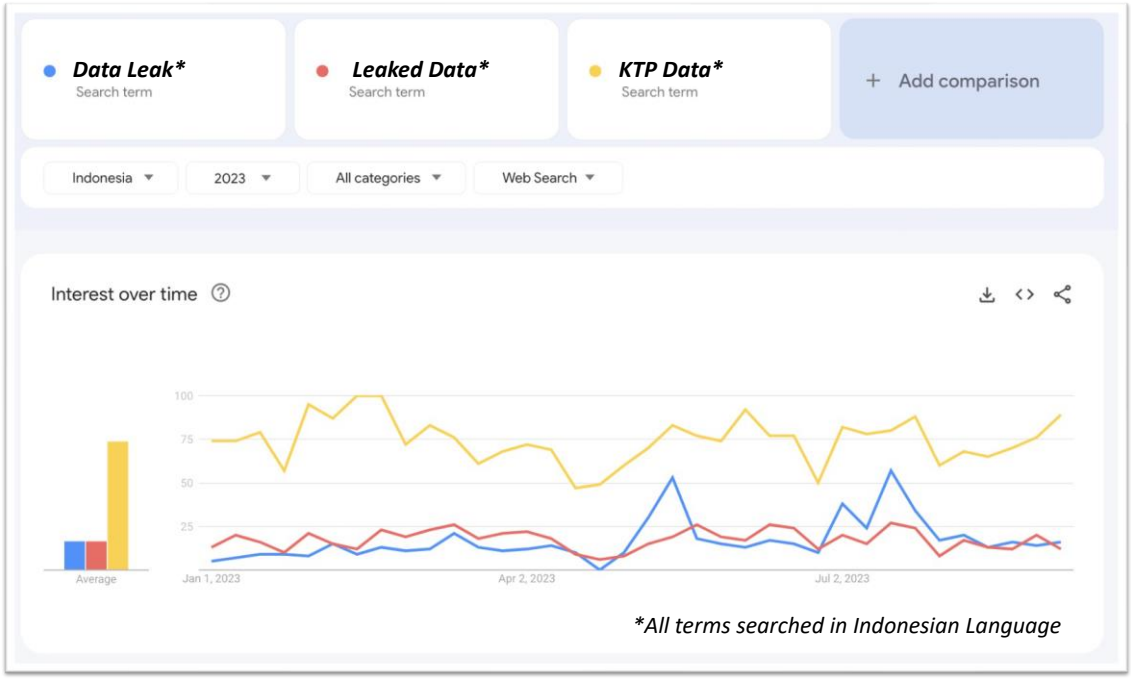
Since the rise of our cyber realm with the advent of the Internet, cyber and information security have become highly critical sectors that must be focused on in every organization (Salim et al., 2022). In Indonesia, data security and cyber policies are becoming increasingly serious issues that must be addressed. According to the findings of a survey performed by the Centre for Strategic and International Studies (CSIS), approximately 69.8% of Indonesian governmental organizations do not yet employ cloud computing services (Annur, 2022a). According to the same data, 55.1% of public organizations were hesitant to implement this technology because of concerns about data security and privacy. This is especially true in public health organizations, which believe that giving service providers authority over data kept in the cloud may increase data security threats. Another factor that surfaced was that approximately 34.7% of public institutions believed they did not require cloud computing services. Others believe that the biggest barriers to implementing this technology are lack of legal clarity (33.1%) and low investment budgets for information technology (31.4%). Other impediments included high

Correspondence Mohammad Fadil Imran Email : mfadilimran@stik-ptik.ac.id

expenses (28.8%), a shortage of IT people who understand cloud services (20.3%), and a lack of awareness of cloud services (16.9%).

Cyber security has become a major issue for Indonesian residents, particularly in the aftermath of the e-KTP data breach scandal. Our Google Trends data indicated a notable trend in which the number of individuals seeking information on this topic fluctuated. This tendency continues during the first half of 2023 and is still a matter of discussion.

Figure 1.
Trends of User`s Web-Searching regarding Leaked Personal Data



Source: Google Trends. 2023

According to Veritrans and DailySocial data, Indonesia is among the top ten nations most vulnerable to malware assaults, with a treatment exposure rate of 23.54%. This figure is greater than that of China and Thailand (Databoks, 2017). Moreover, according to the International Telecommunication Union (ITU) study, Indonesia continues to trail behind neighboring nations such as Singapore and Malaysia in terms of cyber security. Even though Indonesia has improved its cyber security rating from year to year, the score of 94.88 attained is still far below that of the United States, which received a flawless score of 100. Indonesia is ranked third in Southeast Asia, ahead of numerous neighboring nations, such as Vietnam, Thailand, the Philippines, and Brunei Darussalam (Kusnandar, 2022a).

In today's digital age, the necessity of cyber security cannot be overstated. Not only must information be safeguarded, but so must financial transactions, which are increasingly being conducted online. Governments and commercial parties that manage public data must improve data security to prevent information from falling into wrong hands and being misused. However, there are obstacles to improving cyber security in Indonesia. One of these is a 60% reduction in the budget of the National Cyber and Crypto Agency (BSSN) in 2022 (Kusnandar, 2022b). The BSSN is projected to increase cyber resilience and security with a lower budget, with a primary focus on creating multi-stakeholder capacities in the early detection and management of cyber security crises. The BSSN was created in 2017 with the goal of effectively and efficiently implementing cyber security by utilizing, developing, and combining all components connected

to cyber security and cyberspace. The function of the BSSN is critical in preserving the security of Indonesia's data and cyber infrastructure, particularly in the face of increasingly sophisticated and complicated cyber threats.

Public data security has grown increasingly critical in the aftermath of a series of data leaks, such as the disclosure of BPJS Health user data and cyber assaults on Bank Syariah, Indonesia. In some of these situations, sensitive data, such as the population identification number (NIK), family card number, date of birth, address, and other personal information, have come into the hands of irresponsible parties (Muhamad, 2023). Discussing cyber security also means discussing data protection. Although the terms "cyber security" and "data protection" are sometimes used interchangeably, they relate to different aspects of information security. Cyber security is the larger discipline concerned with safeguarding digital systems and data against cyber attacks, whereas data protection is a subset focusing on the management and privacy of personal information. Personal data protection is frequently included in a complete cybersecurity policy, therefore they overlap extensively (Miner, 2021; Raul, 2021; von Maltzan, 2019). In the context in Indonesia, Indonesians' degree of knowledge regarding personal data protection remains poor. According to a poll performed by the Ministry of Communication and Information in collaboration with the Katadata Insight Centre (KIC), 53.6% of respondents had a low degree of personal data protection. Only 46.4% of the respondents believed that their personal data were adequately protected. This suggests that many individuals are still unaware of the need to safeguard their personal data in the digital age (Annur, 2022b). According to a study performed by the Kurious-Katadata Insight Center (KIC), the majority of respondents (62.6%) were skeptical about the Indonesian government's data storage center's degree of cyber security (Muhamad, 2023). This indicates that public trust in the security of government-managed data remains low. Some respondents also stated that they were unsure of how secure their data were.

Given these circumstances, there is an urgent need for initial conversations on improving cyber security policies in Indonesia. Previous research examined these topics through a systematic literature review (Nurhaqiqi et al., 2023; Yuadi & Khusniah, 2022). However, these studies only focused on mapping existing research without conducting a comprehensive analysis. In this context, we aim to address the existing gap by exploring the issues encountered while employing identical methodologies. The first step is to address the issues inherent in this situation by observing hurdles. In this context, we aimed to identify and analyze major obstacles in cyber security management. By strengthening our ideas with evidence, we can identify areas where policy improvements are needed, thereby enhancing national security. Indonesia seeks to secure its data and cyber security landscape through these concentrated measures. This will enable both the general public and government institutions to traverse information technology with more confidence, generating greater trust in society.

Literature Review

Managing Cyber Security

Cyber security has taken the forefront in the current expanding digital world, catching the attention of governments, organizations, and people alike (Fichtner, 2018). The importance of this topic is highlighted by the realization that technological advancement and capacity building are essential to accomplishing the Millennium Development Goals and, eventually, Sustainable Development by 2030. Governments worldwide are aware that combating cybercrime is critical for attaining long-term economic development (Kalogiannidis et al., 2023). To address these multifaceted difficulties, four main paradigms in cyber security have emerged: (1) the relentless pursuit of repairing and breaking technical objects, (2) combating erroneous computer use, (3) countering

malicious political actions carried out using digital tools, and (4) the dynamic social construction of expertise surrounding what is deemed worthy of protection (Michalec et al., 2022). Furthermore, the cyber security sector is undergoing tremendous development. It is no longer limited to national security; rather, it has spread horizontally across a variety of policy sectors, while concurrently increasing on the political agenda (Dunn Cavelty & Wenger, 2020). This paradigm change reflects the changing nature of the threat landscape, in which the impact of cyber intrusions goes well beyond government and corporate boardrooms to disrupt people's daily lives. Organizations and nations have adopted extensive security risk management strategies to properly navigate this complex terrain (Harkin & Molnar, 2023). These procedures are intended to protect the privacy, integrity, and availability of data and assets in the cyberspace. These include a wide range of rules, guidelines, protections, technologies, tools, and training programs. Governments and organizations hope to strengthen the cyber environment and safeguard users by enacting these policies. Nonetheless, determining the exact degree of harm caused by cyber-attacks remains difficult. While governments and companies recognize the economic and social implications of cyber security breaches, reliable quantification is difficult to achieve (Silva, 2013). The complexity of the danger landscape and its potential for widespread impact highlight the importance of implementing effective risk mitigation techniques. Cyber security has become increasingly important in the field of defense. It depicts a constant effort to create technical defence mechanisms while encouraging prosperity, creativity, and the preservation of democracy. The convergence of these issues underscores the critical role of cyber security in guaranteeing continuity and security in a society that is increasingly reliant on technology (Efthymiopoulos, 2019). Therefore, in today's linked world, the value of efficiently managing cyber security cannot be emphasized. As previously stated, cyber security has far-reaching implications that go beyond national security or economic interests

Consensus among governments and scientists is unanimous in recognizing the necessity of implementing a cybersecurity management model to protect critical infrastructure, including online voting systems, financial systems, and crucial energy infrastructure. While there is no universally applicable cybersecurity management methodology, several countries recognize the need of effectively managing and safeguarding critical resources (Limba et al., 2017).

According to Techopedia's online lexicon, the cyber security strategy includes identity management, risk management, and incident management, which are all part of a wider range of activities (Jenab & Moslehpour, 2016). Additionally, Limba included features related to cyber security management, encompassing six levels that evaluate certain traits necessary for a satisfactory framework of a cyber security management model.

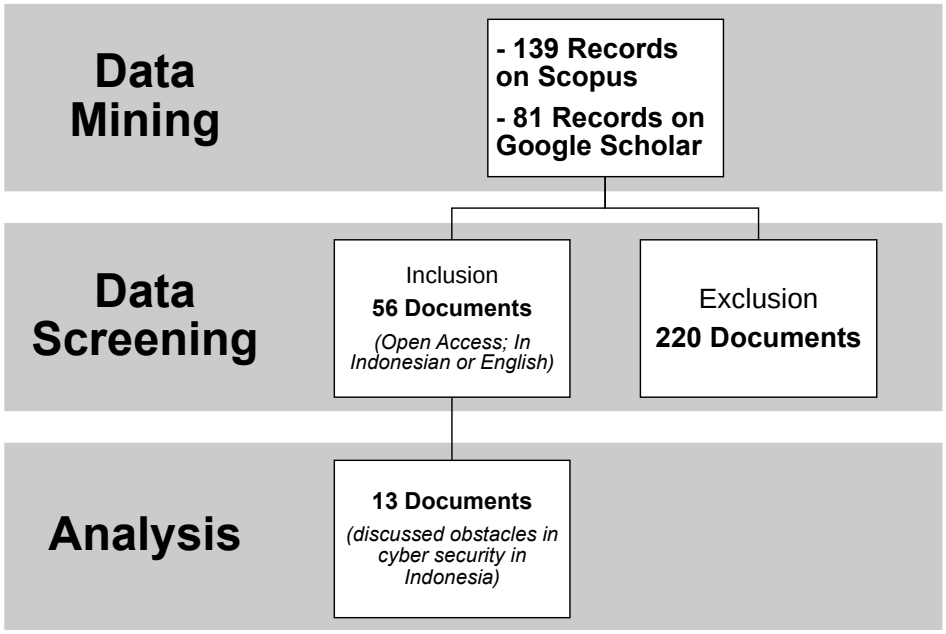
The key components are legislative regulation, robust governance, effective risk management, a strong security culture, efficient technology management, and a well-coordinated incident response (Limba et al., 2017). One argument is that the field of cyber security management is extensive, but there are few guidelines for tackling it, which means that cyber security can be interpreted in many ways. One important aspect of security risk management is the identification of vital assets (Ahmad et al., 2020). This involves mapping threats to assets in order to identify potential risk scenarios. The next step is to estimate the chance and effect of these risk scenarios. Once this is done, risk response strategies may be developed. Finally, it is important to assess the risk management plans (Ahmad et al., 2020; Finne, 2000; Gerber & Von Solms, 2005; Shedden et al., 2010; Stoneburner et al., 2002).

RESEARCH METHODS

The major goal of this study was to identify and analyze the hurdles and problems in the realm of cyber security in Indonesia. A thorough and well-structured systematic literature review process was used to accomplish this purpose following previous studies (Alzahrani & Alfouzan, 2022; Fauzi et al., 2019; Pal et al., 2021; Panahi Rizi & Hosseini Seno, 2022; Rosyda & Raharja, 2020; Thompson et al., 2012). This technique enables a thorough examination of the current body of information (Yusuf et al., 2023), providing insight into the multiple difficulties confronting Indonesia's cyber security scene. This systematic literature evaluation was founded on a thorough search of relevant academic literature in two recognized source databases: Scopus and Google Scholar. The initial data-mining step yielded 139 entries from Scopus and 81 from Google Scholar. These records were selected based on a carefully prepared query intended to capture a wide range of relevant information. The query was as follows: (TITLE-ABS-KEY (cyber* OR digital* OR data* OR inform* AND secur* OR protect*) AND ALL (indonesia) AND ALL ("cyber security") AND ALL (policy) AND ALL (government) AND ALL (challenge* OR restraint* OR obstacle*)). This thorough inquiry guaranteed that the search results were exact and included all conceivable aspects of cyber security concerns within the framework of Indonesia's policy and the government arena.

Following initial data mining, a careful screening procedure was performed to extract the most relevant and pertinent documents from a large corpus. The goal of this three-tiered screening method is to include materials that not only satisfy linguistic requirements, but are also easily available for in-depth research. The 220 records obtained were submitted to a language and document accessibility filter during the first screening step. Documents that did not provide full-text access or were not in English or Indonesian were excluded from the study. Because of open access, 56 papers were subjected to a more severe review in the second screening step. Those who did not provide full-text access were once again disqualified from consideration. This paper was given a thorough observed of its entirety. The 13 selected papers were extensively scrutinized and evaluated for their relevance to the study issue, which centered on the identification and in-depth analysis of impediments in Indonesian cyber security policy. Following this thorough examination, 43 documents were rejected because they did not engage in in-depth discussion of the issues. Following this rigorous filtering procedure, the remaining 13 documents were analyzed and thoroughly interpreted. This interpretive phase intended to dive into the details of these papers, collecting useful insights and information on the challenges and obstacles experienced in the field of Indonesian cyber security policy. This study intends to provide a thorough and detailed picture of the issues encountered by Indonesia in developing and implementing effective cyber security policies via meticulous analysis and synthesis of these selected documents. This study project adds to a better knowledge of the challenges the country has in protecting its digital environment and serves as a basis for future research and policy development in the field of cyber security in Indonesia.

Figure 2.
Methods Flowchart



Source: Authors` Processed. 2023

RESULTS AND DISCUSSIONS

Examining the Cyber security Obstacles

The challenges associated with cyber security policy in Indonesia play a crucial role in safeguarding digital infrastructure, sensitive data, and individual rights within a rapidly evolving and perilous digital landscape. The complexities and intricacies of data and cyber security policy in Indonesia necessitate a thorough analysis in order to comprehend the various challenges and threats involved. This comprehensive analysis seeks to explore the multiple facets of these challenges while establishing a link between the interconnected discussions. Indonesia is currently confronted with a significant and formidable challenge in cybercrime, resulting in considerable economic losses. According to recent estimates, the aforementioned losses have experienced a significant increase, reaching a value of USD 895 billion, which corresponds to approximately 1.20% of the total global losses attributed to cybercrime (Indah & Sidabutar, 2022). The significant magnitude of these losses highlights the imperative nature of addressing cyber security concerns within the nation. The multidimensional nature of threats refers to the complex and multifaceted characteristics of the various risks and dangers that exist in different domains. Indonesia's challenges pertain to the multifaceted nature of cyberthreats. The scope of these threats extends beyond the jurisdiction of any individual ministry or agency, thus necessitating a coordinated and comprehensive approach. The multifaceted nature of cyber security necessitates the involvement of various ministries, including but not limited to the TNI, Polri, Ministry of Defence, and Ministry of Communication and Information (Hajj et al., 2022). The intricate nature of this situation requires a collective endeavour involving various branches of the government.

It begins with the legal framework, and the regulatory vacuum refers to the absence of comprehensive legislation and regulations in a particular domain. This situation creates a lack of clear guidelines and oversight, leading to uncertainty and potential challenges in enforcing legal

standards. One prominent issue revolves around the insufficiency of the existing legal frameworks concerning cyber security. Indonesia's current legal framework concerning cyber security is inadequate in its comprehensiveness, as evidenced by the insufficiency of existing legislation such as Electronic Information and Transaction Law (EIT) in effectively addressing contemporary cyber threats (Gojali, 2023). The lack of an officially approved Cyber security and Resilience Bill has given rise to a regulatory void, leading to inconsistencies and ambiguities in the state's strategy towards safeguarding data. The absence of regulations in this area poses a significant challenge to the government's capacity to safeguard individuals' data and undermines the principle of data sovereignty (Aji, 2023). Then, the regulations pertaining to data protection are characterized by fragmentation. The data protection strategy in Indonesia exhibits fragmentation and lacks a cohesive legal framework. Regulations pertaining to the protection of personal data are distributed among multiple sectoral laws, amounting to a considerable number of 32 regulations. The absence of harmonization at the normative level gives rise to legal uncertainties and inefficiencies (Mirna et al., 2023). The lack of dedicated legislation pertaining to safeguarding personal data creates deficiencies in the preservation of privacy, which is inconsistent with established global norms (Mirna et al., 2023).

The management of cybercrime in Indonesia presents notable difficulties that are primarily attributable to the absence of precise delineations and legislative measures. The act of gaining unauthorized entry into computer systems is commonly referred to as interception. However, the lack of comprehensive legislation in this domain leads to a state of ambiguity and complexity in prosecuting individuals involved in cybercriminal activities. This inadequacy hinders the nation's capacity to effectively apprehend cybercriminals (Sandjojo et al., 2020). The present discourse revolves around challenges encountered in law enforcement and interception. The lack of precise delineations of personal data within the Electronic Information and Transactions (EIT) Law and its associated regulations present obstacles for Lawful Interception (LI) conducted by Indonesian Law Enforcement Agencies (LEAs). The effectiveness of LI efforts is influenced by ambiguities in the definition of personal data (Rumata & Sastrosubroto, 2019).

Indonesia encounters various obstacles pertaining to the implementation of cyber security measures, primarily centered around its infrastructure. The adoption of eGovernment in certain regions is impeded by the presence of uneven and costly infrastructure, which restricts the accessibility of essential services (Utomo et al., 2020). Critical infrastructure includes encompassing essential components such as electrical systems, transportation systems, and communications, which are interconnected with the Internet, rendering them susceptible to cyberattacks.

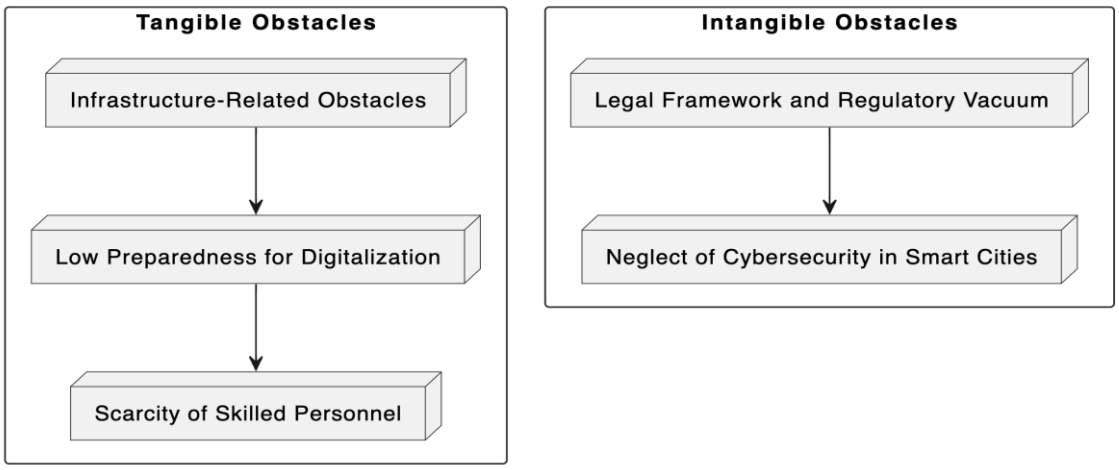
Despite the implementation of proactive measures, the level of preparedness in Indonesia for the adoption of digitalization and encryption remains relatively low. The persistence of risks related to rights infringements and data theft is evident, as organizations have documented instances of breaches encompassing malware attacks and thefts of digital certificates (Yusni & Sigalingging, 2021). The adoption of cyber security standards and frameworks poses challenges for organizations in Indonesia (Syafrizal et al., 2020). Meanwhile, the Digital Governance Assessment framework (DGRA) has identified a notable deficiency in Indonesia's performance within the domains of cyber security, privacy, and resilience. This statement highlights the urgency of addressing a country's cyber security, privacy protection, and resilience capabilities (Kusmiarto et al., 2021).

These challenges are primarily attributed to the scarcity of skilled personnel in the field of cyber security. The process of selecting a suitable standard is intricate given the intricacy involved in showcasing adherence to legal requirements and established norms. Furthermore, the absence

of familiarity with standard components makes it difficult to discern the initial stages of safeguarding (Syafrizal et al., 2020). This is an additional obstacle that Indonesia faces owing to the scarcity of adequately trained cyber security experts. The domain of cyber security is experiencing rapid growth; however, the scarcity of adequately trained personnel has emerged as a significant impediment to safeguarding the digital infrastructure. Cultural factors also play a role, including a deficiency in the culture of sharing, resistance towards openness, and reluctance to alter mindsets (Utomo et al., 2020).

Furthermore, in Indonesia, government and public service providers have paid less attention to cyber security in the support of smart cities. Web-based public service applications are frequently constructed in haste with little regard to data security and privacy protection. Lack of collaboration between industry and the defense environment and lack of cooperation between foreign ministries on cyber war and cybercrime have also been identified as barriers to preventing cybercrime (Alam & Ibrahim, 2019). Without the participation of stakeholders (ranging from official institutions to the corporate sector, universities, and civil society), the challenge of fixing cyber security concerns would remain one-sided and incomplete (Ariyaningsih et al., 2023).

Figure 3.
Obstacles in Indonesia`s Cyber Security



Source: Authors` Analysis. 2023

Invaluable Insight from the Field

Lessons learned from other countries' data and cyber security regulations provide useful insights into the methods and techniques that can be used to promote cyber security and protect personal data. Numerous countries have created specific cyber force units as part of their defense and security systems to anticipate cyber assaults on computer networks, the internet, and infrastructure. In 2011, the United States Department of Defense, for example, designated the Internet or cyberspace as a new combat dimension alongside land, sea, and air (Sakban et al., 2020). The United States has shown a significant commitment to cyber security by establishing The National Cyber Security Agency (NCSD), a specialized agency tasked with tackling national cyber security threats. This division, which is supported by public-private partnerships, is in charge of the National Security Decision Directive-145 (NSDD-145) and The National Cyber Security Agency (NCSD), developing and maintaining an effective national cyber security system, executing risk management programs, and reacting to urgent circumstances via the National Cyberspace Response System (Hajj et al., 2022; Rofii, 2020). This strategy emphasizes the significance of a designated body in dealing with national cyber risk.

Moreover, other countries have passed robust data protection legislation. To address personal data concerns, Hong Kong established the Privacy Commissioner for Personal Data, emphasizing the significance of a separate body (Septi Jayanti & Suraji, 2022). The Personal Information Protection Act (Pipa) of South Korea prioritises data acquisition, accuracy, and security. Personal information security and data disclosure and accountability plans are prioritized in this country (Manik et al., 2022). The Data Protection Act of Japan emphasizes the confidentiality of personal data and the right of data owners to know the purpose of data usage. Other nations, including the EU, the US, China, Mexico, India, and Brazil, have also enacted data protection legislation. The European Union's General Data Protection Regulation (GDPR) is notable for its comprehensive framework that offers consumer rights, such as access to personal data, the right to be forgotten, and the ability to alter data (Panahi Rizi & Hosseini Seno, 2022). These data protection regulations provide other nations that want to improve their data and cyber security policies. In Southeast Asia, Vietnam has complete legislation that covers data security and protection in one law, namely, Cyber Information Security (LCIS) legislation. Meanwhile, Malaysia extends the Personal Data Protection Act to commercial activities, excluding data handled by the government (Mizan et al., 2020). Then, It is worth mentioning that Malaysia has devised a mechanism for assigning cyber security obligations. These countries have a vertical system in which tasks are delegated by the central government to local authorities (Persadha et al., 2016). This method provides a coordinated effort at all levels of the government to solve cyber security concerns.

In addition, there is International Cooperation at the Combined Communications Electronics Board (CCEB). The CCEB, which includes countries such as Australia, Canada, New Zealand, the United Kingdom, and the United States, has released a report titled 'Information Assurance for Allied Communications and Information Systems.' This multinational partnership presents recommendations on information assurance principles, policies, and procedures for a secure mixed-information environment (Utomo et al., 2020). International collaboration and standardization can help to create a safer cyber environment. Furthermore, the impact of China's 2016 cyber security law on foreign technology organizations, as well as its relationship to China's big data and smart city projects, provides important insights. This highlights the significance of incorporating cyber security measures into the deployment of technologies in smart cities, ensuring that security is a basic factor in technology-driven urban development (Alzahrani & Alfouzan, 2022).

The lessons learnt from evidence about cyber security policies from various countries highlight the significance of comprehensive laws, specialised agencies, international coordination, and the integration of cyber security coordination with technological efforts. These lessons provide significant insights for countries looking to improve their own cyber security policies and plans, emphasising the importance of a multifaceted strategy to dealing with growing cyber threats in the digital era. Moreover, as previously mentioned, there is no single cybersecurity management model. However, one of the valuable findings from our analysis was also the existence of a cyber security management model proposed by (Limba et al., 2017) where each of the six steps evaluates a different cybersecurity management system aspect. Legal regulation evaluates an organization's cybersecurity knowledge, goals, and readiness, while risk management evaluates its ability to identify and address new risks. Security Culture assesses staff knowledge of cybersecurity, Technology Management assesses knowledge of all elements and vulnerabilities, and Incident Management assesses whether the organization has a special incident consequence management plan (Limba et al., 2017; Tvaronavičienė et al., 2020). This can also be a basis for making policy recommendations to strengthen cyber security.

Building Stronger Foundations: Proposed Policy Recommendations

The emergence of BSSN (Badan Siber dan Sandi Negara), exemplifies the necessity for better legislation and more comprehensive cyber security safeguards (Indah & Sidabutar, 2022). The results of our study underscore the necessity of promptly establishing a centralised governing body to coordinate and address cyber threats (Syarief, 2022). A centralized authority can oversee the creation and execution of regulatory ideas, including personal data security principles, regulations, processes, and institutions (Kadek et al., 2021). This approach addresses the need for a centralized body to manage cyber security activities, as well as the requirement for clear legislation to safeguard data protection and privacy. In order to practically implement the establishment of a centralized governing body for cybersecurity in Indonesia, a phased approach is paramount. The first step involves close collaboration with existing bodies, particularly BSSN, to determine their roles and identify convergence points for seamless integration into the new central body. Government agencies, industry professionals, and cybersecurity experts must be consulted for diverse perspectives and a holistic policy approach. The central authority should monitor principles, regulations, methods, and organization construction.

Comprehensive legislation, such as the cyber security law, is also advised to prioritize the protection of people's data, privacy, and transactions (Gojali, 2023). This legislative framework would provide clear norms and obligations for both government and industry, promoting a safe digital environment. Simultaneously, there is a push to simplify cyber security standards and procedures so that they are consistent with best practices worldwide (Syafrizal et al., 2020). Combining these proposals highlights the necessity of legislative and regulatory measures as well as adherence to global cyber security standards in creating a strong cyber security ecosystem in Indonesia. This centralised agency may monitor the growth of a community-based strategy based on the Indonesian notion of "gotong royong" (mutual collaboration) (Persadha et al., 2016). This strategy ensures both centralized regulatory authority and active community engagement in cyber security initiatives by encouraging stakeholder collaboration. In information system security, security policies for information systems are essential because they primarily remove threats. This refers to a set of regulations developed by a company to guarantee that all information technology users remain within the company's domain (Sandjojo et al., 2020).

Additionally, efforts to strengthen cyber security in Indonesia should involve the development of a cyber security maturity model that is capable of assessing an organization's cyber security capabilities. This approach would aid in determining an organization's cyber security maturity level on a scale relevant to the current situation. It is also necessary to evaluate national standards that adhere to the National Institute of Standards and Technology (NIST), ISO 27002, COBIT, and PCI DSS security standards in ICT management (Sulistyowati et al., 2020). These standards are anticipated to aid in measuring ICT management performance in organizations, particularly government organizations.

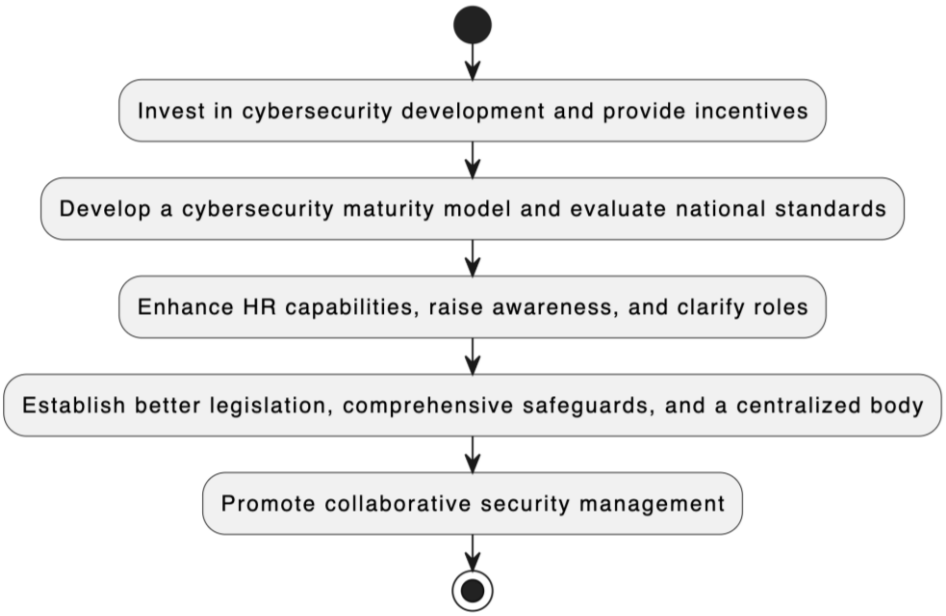
Moreover, it is necessary to build better information technology facilities and infrastructure, content management, communications and networking, Internet development, and online trade. The management of cyber security resources must be incorporated into the company management process. (Hajj et al., 2022). Investments in research and development (R&D) and innovation in the field of cyber security play a crucial role in addressing the escalating complexity of threats. It is imperative for the government to allocate financial resources and offer incentives to research institutions and companies that are dedicated to the advancement of cyber security solutions. Still related into tackling the tangible obstacles, components of defence strategy and

human factor are advised as a plan to attain the minimal degree of secure and trusted e-government environment (Priyambodo & Prayudi, 2016). Indonesia is equipped with Indonesia's National Work Competence Standards (SKKNI) in the information security sector, serving as the fundamental framework for enhancing the capabilities of human resources entrusted with the task of safeguarding cyber security (Setiadi et al., 2012). Nevertheless, the continuous progress of technology necessitates a significant degree of expertise and credentials for individuals working within this domain. There is a need to enhance the level of awareness among senior government officials and board members of critical national infrastructure operators regarding cyber risks, and the corresponding measures they can implement to safeguard security-sensitive information. Establishing well-defined roles and responsibilities pertaining to information security is imperative. In addition, it is crucial to implement crisis management exercises on a national scale, foster the advancement of cyber security training and educational initiatives, and establish a designated hub of exceptional expertise in the field of cyber security. (Yuliana & Hasibuan, 2022).

Furthermore, it is critical to develop efficient security management that encourages collaboration, as security governance requires the collaboration of numerous fast-moving infrastructure components. (Salim et al., 2022) . The concept of strong intersector cooperation refers to the collaborative efforts and partnerships established between different sectors, such as the government, private industry, and civil society, to address common challenges. Collaboration among different sectors is crucial for effectively addressing and mitigating cyber threats. It is imperative for governments, the private sector, and academic institutions to collaborate to effectively exchange information pertaining to cyber threats, discern vulnerabilities, and collectively devise solutions by some schemes, including public–private partnerships (Saputra et al., 2019), or international collaboration. This international collaboration can include collaboration between government agencies or companies providing personal data protection services. This is important because the cyber domain is an area where technological innovation and operational art have far outstripped regional policies and strategies. Some argue that a cyber security treaty or any international telecommunications treaty is unnecessary because inter-governmental coordination can be handled through soft law or bilateral or regional agreements. Unfortunately, because there are no agreements on how to interpret and implement existing international law, the current practice of covert (and unacknowledged) cyber-attacks and mass surveillance benefits from the lack of treaty-level cooperation on network security concerns (Hill, 2015).

A holistic strategy to improve data and cyber policy in Indonesia would benefit from combining and integrating diverse proposals. Indonesia can successfully preserve data, privacy, and digital assets by addressing legislative frameworks, centralized monitoring, community engagement, technical measures, and awareness programs. This strategy acknowledges the changing nature of cyber threats and the necessity of a comprehensive response. All of these strategies address the prevention of incidents as well as risk response. The effective security discipline includes both proactive preparation prior to an attack and prompt and competent response in the event of an event. This includes the organization's ability to quickly recover and expand to completely mitigate or reduce the likelihood of the aforementioned occurrence in future instances. (Salim et al., 2022).

Figure 4.
Proposed Policy Recommendations in Indonesia`s Cyber Security



Source: Authors` Analysis. 2023

CONCLUSIONS

This analysis explores the multiple issues and obstacles confronting Indonesian cyber security policy, highlighting the critical need for comprehensive solutions. These difficulties range from a lack of an effective legislative framework and regulatory vacuum to a shortage of experienced cyber security personnel. A series of policy recommendations were provided to strengthen the foundation for cyber security in Indonesia. These include strengthening a centralized governing body, creating a cyber security maturity model, and assessing national norms. Investments in cyber security research and development, improved human resource competencies, and the promotion of stakeholder engagement are all critical components of policy recommendations. Furthermore, the report emphasizes the significance of simplifying cyber security regulations and procedures while promoting compliance with best practices. Furthermore, lessons learned from other countries' cyber security policies highlight the importance of comprehensive legislation, specialized agencies, international cooperation, and the incorporation of cyber security into technical breakthroughs. These lessons can help Indonesia to improve its cyber security policy and protect itself from cyber threats. Although this study provides useful insights into cyber security concerns and policy suggestions for Indonesia, several limitations must be acknowledged. For beginnings, this study depends primarily on existing research and may not objectively represent the most recent developments in the rapidly growing subject of cyber security. Furthermore, while the focus has been on identifying difficulties and suggesting regulatory solutions, further research into the sociocultural aspects impacting cyber security procedures in Indonesia is required. More studies should be conducted to investigate the possible economic and societal implications of implementing the recommended regulations as well as the efficacy of international cooperation in improving Indonesia's cyber security landscape. Finally, this study offers the groundwork for future research to address these shortcomings and refine the recommended policy actions for a more resilient cyber security environment in Indonesia.

REFERENCES

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, *71*(8), 939–953. https://doi.org/10.1002/asi.24311

Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *13*(2), 222–238. https://doi.org/10.22212/jp.v13i2.3299

Alam, R. G. G., & Ibrahim, H. (2019). Cybersecurity Strategy for Smart City Implementation. *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences - ISPRS Archives*, *42*(4/W17), 3–6. https://doi.org/10.5194/isprs-archives-XLII-4-W17-3-2019

Alzahrani, N. M., & Alfouzan, F. A. (2022). Augmented Reality (AR) and Cyber-Security for Smart Cities—A Systematic Literature Review. *Sensors*, *22*(7), 1–17. https://doi.org/10.3390/s22072792

Annur, C. M. (2022a). *Banyak Lembaga Publik Belum Gunakan Layanan Cloud, Apa Alasannya?* Databoks. https://databoks.katadata.co.id/datapublish/2022/08/24/banyak-lembaga-publik-belum-gunakan-layanan-cloud-apa-alasannya

Annur, C. M. (2022b). *Pelindungan Data Pribadi Warga RI Masih Tergolong Rendah*. Databoks. https://databoks.katadata.co.id/datapublish/2022/08/09/pelindungan-data-pribadi-warga-ri-masih-tergolong-rendah

Ariyaningsih, S., Andrianto, A. A., Kusuma, A. S., & Prastyanti, R. A. (2023). Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia. *Justisia: Jurnal Ilmu Hukum*, *1*(1), 1–11.

Databoks. (2017). *Indonesia Rentan Terkena Serangan Malware - Negara-negara yang Rentan Terkena Serangan Malware 2016*. Katadata Insights Center.

Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5–32.

Efthymiopoulos, M. P. (2019). A cyber-security framework for development, defense and innovation at NATO. *Journal of Innovation and Entrepreneurship*, *8*(1). https://doi.org/10.1186/s13731-019-0105-z

Fauzi, A. H., Rizal, M., & Arifianti, R. (2019). Corporate entrepreneurship in SMEs: A systematic mapping study. *Jurnal Manajemen Pelayanan Publik*, *2*(1), 55.

Fichtner, L. (2018). What kind of cyber security? Theorising cyber security and mapping approaches. *Internet Policy Review*, *7*(2). https://doi.org/10.14763/2018.2.788

Finne, T. (2000). Information Systems Risk Management: Key Concepts and Business Processes. *Computers & Security*, *19*(3), 243–242.

Gerber, M., & Von Solms, R. (2005). Management of risk in the information age. *Computers & Security*, *24*(1), 16–30. https://doi.org/10.1016/J.COSE.2004.11.002

Gojali, D. S. (2023). Identifying the Prevalence of Cybercrime in Indonesian Corporations: A Corporate Legislation Perspective. *International Journal of Cyber Criminology*, *17*(1), 1–11. https://doi.org/10.5281/zenodo.4766600

Hajj, R. A., Muta, A., & Mamoto, B. J. (2022). *Data and Information Security Management : Preparing Data in the Cyber Era in Indonesia*. 19165–19171.

Harkin, D., & Molnar, A. (2023). Exploring the social implications of buying and selling cyber security. *Crime, Law and Social Change*, *79*(1), 83 – 100. https://doi.org/10.1007/s10611-022-10037-y

Hill, R. (2015). Dealing with cyber security threats: International cooperation, ITU, and WCIT. *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, 119–134.

Indah, F., & Sidabutar, A. Q. (2022). Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka). *Jurnal Bidang Penelitian Informatika*, *1*(1), 1–8.

Jenab, K., & Moslehpour, S. (2016). Cyber Security Management: A Review. *Business Management Dynamics*, *5*(11), 16–39. www.bmdynamics.com

Kadek, I., Jaya, N. A., Ayu, I., & Dewi, U. (2021). Regulasi Keamanan Data Pribadi Pengguna pada E-commerce di Indonesia. *Jurnal Sistem Informasi Akuntansi*, 1–8.

Kalogiannidis, S., Paschalidou, M., Kalfas, D., & Chatzitheodoridis, F. (2023). Relationship between Cyber Security and Civil Protection in the Greek Reality. *Applied Sciences (Switzerland)*, *13*(4). https://doi.org/10.3390/app13042607

Kusmiarto, K., Aditya, T., Djurdjani, D., & Subaryono, S. (2021). Digital transformation of land services in indonesia. *A Readiness Assessment. Land*, *10*(2), 1–16.

Kusnandar, V. B. (2022a). *ITU: Keamanan Siber Indonesia Kalah dari Singapura dan Malaysia*. Databoks. https://databoks.katadata.co.id/datapublish/2022/01/27/itukeamanan-siber-indonesiakalah-dari-singapura-dan-malaysia

Kusnandar, V. B. (2022b). *Pemerintah Pangkas 60% Anggaran Badan Siber dan Sandi Negara pada 2022*. Databoks. https://databoks.katadata.co.id/datapublish/2022/01/26/pemerintah-pangkas-60-anggaran-badan-siber-dan-sandi-negara-pada-2022

Limba, T., Plėta, T., Agafonov, K., & Damkus, M. (2017). CYBER SECURITY MANAGEMENT MODEL FOR CRITICAL INFRASTRUCTURE. *The International Journal ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES*, *4*(4), 559–573.

Manik, L. P., Akbar, Z., Yaman, A., & Indrawati, A. (2022). Indonesian Scientists' Behavior Relative to Research Data Governance in Preventing WMD-Applicable Technology Transfer. *Publications*, *10*(4). https://doi.org/10.3390/publications10040050

Michalec, O., Milyaeva, S., & Rashid, A. (2022). When the future meets the past: Can safety and cyber security coexist in modern critical infrastructures? *Big Data and Society*, *9*(1). https://doi.org/10.1177/20539517221108369

Miner, M. (2021, March 16). *What is the Difference between Data Security and Cyber Security?* SSI NET. https://insider.ssi-net.com/insights/what-is-the-difference-between-data-security-and-cyber-security

Mirna, M., Judhariksawan, & Maskum. (2023). Analisis Pengaturan Keamanan Data Pribadi di Indonesia. *Jurnal Ilmiah Living Law*, *15*(1), 16–30.

Mizan, N. S. M., Ma'arif, M. Y., Mohd Satar, N. S., & Shahar, S. M. (2020). CNDS-Cybersecurity: Issues and Challenges in ASEAN Countries. *International Journal of Advanced Trends in Computer Science and Engineering*, *8*(June), 1965–1968.

Muhamad, N. (2023). *Mayoritas Masyarakat Tidak Yakin dengan Tingkat Keamanan Siber di Indonesia*. Databoks. https://databoks.katadata.co.id/datapublish/2023/08/10/mayoritas-masyarakat-tidak-yakin-dengan-tingkat-keamanan-siber-di-indonesia

Nurhaqiqi, H., Mustikasari, R. P., & Kusnarto. (2023). Data Security in Indonesia: Bibliometric Analysis of the Development of Personal Data Regulatory. *Jurnal Spektrum Komunikasi (JSK)*, *11*(1), 85–93.

Pal, D., Zhang, X., & Siyal, S. (2021). Prohibitive factors to the acceptance of Internet of Things (IoT) technology in society: A smart-home context using a resistive modelling approach. *Technology in Society*, *66*. https://doi.org/10.1016/j.techsoc.2021.101683

Panahi Rizi, M. H., & Hosseini Seno, S. A. (2022). A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city. *Internet of Things (Netherlands)*, *20*(August), 100584. https://doi.org/10.1016/j.iot.2022.100584

Persadha, P. D., Waskita, A. A., & Yazid, S. (2016). Comparative Study of Cyber Security Policies among Malaysia, Australia, Indonesia: A Responsibility Perspective. *Proceedings - 4th International Conference on Cyber Security, Cyber Warfare, and Digital Forensics, CyberSec 2015*, *July 2018*, 146–150. https://doi.org/10.1109/CyberSec.2015.36

Priyambodo, T. K., & Prayudi, Y. (2016). A Proposed Strategy for Secure and Trusted Environment in e-Government. *Lecture Notes in Electrical Engineering*, *362*, 891–902. https://doi.org/10.1007/978-3-319-24584-3

Raul, A. C. (2021). *The privacy, data protection and cybersecurity law review*. Law Business Research Limited.

Rofii, M. S. (2020). Strengthening Digital Ecosystems for Sustainable Development in Indonesia: Anticipating Cyber Threats. *IOP Conference Series: Earth and Environmental Science*, *436*(1). https://doi.org/10.1088/1755-1315/436/1/012026

Rosyda, S. S., & Raharja, S. J. (2020). Privatization in State-Owned Enterprises: A Systematic Literature Review. *Jurnal Manajemen Pelayanan Publik*, *3*(2), 107–118.

Rumata, V. M., & Sastrosubroto, A. S. (2019). The Indonesian Law Enforcement Challenges over Encrypted Global Social Networking Platforms. *2018 International Conference on Computer, Control, Informatics and Its Applications: Recent Challenges in Machine Learning for Computing Applications, IC3INA 2018 - Proceeding*, *November*, 199–203. https://doi.org/10.1109/IC3INA.2018.8629528

Sakban, A., Sahrul, Kasmawati, A., & Tahir, H. (2020). The role of Indonesian National Cyber Bureau in monitoring mining business companies. *IOP Conference Series: Earth and Environmental Science*, *413*(1). https://doi.org/10.1088/1755-1315/413/1/012032

Salim, L., Harjono, S., Gunawan, F., Moniaga, J., & Rianto, I. (2022). A Literature Review on the Impact of Effective Management in Cyber Security System Performance. *Proceedings - 4th International Conference on Informatics, Multimedia, Cyber and Information System, ICIMCIS 2022*, 172–177. https://doi.org/10.1109/ICIMCIS56303.2022.10017933

Sandjojo, N., Zuhriyanto, M., & Pradnyana, I. W. W. (2020). The Effects of Fear of Cybercrime and Information Systems Security Policy on National Vigilance. *Proceedings - 2nd International Conference on Informatics, Multimedia, Cyber, and Information System, ICIMCIS 2020*, *November 2020*, 195–200. https://doi.org/10.1109/ICIMCIS51567.2020.9354283

Saputra, P. N., Sudirman, A., Sinaga, O., Wardhana, W., & Hayana, N. (2019). Addressing Indonesia's Cyber Security through Public-Private Partnership (PPP). *Central European Journal of International & Security Studies*, *13*(4).

Septi Jayanti, C., & Suraji. (2022). The Issues Of Data Protection Against Leaking Of Personal Data in Security Health Services (A Comparison Between Indonesia and Other Countries Regulations). *International Journal of Business, Economics and Law*, *26*(1), 1.

Setiadi, F., Sucahyo, Y. G., & Hasibuan, Z. A. (2012). An overview of the development indonesia national cyber security. *International Journal of Information & Computer Science*, *6*, 108.

Shedden, P., Smith, W., & Ahmad, A. (2010). Information Security Risk Assessment: Towards a Business Practice Perspective. *Proceedings of the 8th Information Security Management Conference*.

Silva, K. e. (2013). Europe's fragmented approach towards cyber security. *Internet Policy Review*, *2*(4).

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. *Nist Special Publication*, *800*(30), 800–830.

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. *International Journal on Informatics Visualization*, *4*(4), 225–230.

Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020). Analysis of Cybersecurity Standard and Framework Components. *International Journal of Communication Networks and Information Security*, *12*(3), 417–432. https://doi.org/10.17762/ijcnis.v12i3.4817

Syarief, E. (2022). Security Concerns in Digital Transformation of Electronic Land Registration: Legal Protection in Cybersecurity Laws in Indonesia. *International Journal of Cyber Criminology*, *16*(2), 32–46. https://doi.org/10.5281/zenodo.4766565

Thompson, M., Tiwari, A., Fu, R., Moe, E., & Buckley, D. I. (2012). A Framework To Facilitate the Use of Systematic Reviews and Meta-Analyses in the Design of Primary Research Studies. *Research White Paper: AHRQ Publication No. 12-EHC009-EF.*, 30.

Tvaronavičienė, M., Plėta, T., Della Casa, S., & Latvys, J. (2020). Cyber security management of critical energy infrastructure in national cybersecurity strategies: Cases of USA, UK, France, Estonia and Lithuania. *Insights into Regional Development*, *2*(4), 802–813.

Utomo, R. G., Wills, G., & Walters, R. (2020). A framework for factors influencing the implementation of information assurance for e-Government in Indonesia. *International Journal on Advanced Science, Engineering and Information Technology*, *10*(3), 1025–1034. https://doi.org/10.18517/ijaseit.10.3.9186

von Maltzan, S. (2019). No Contradiction Between Cyber-Security and Data Protection? Designing a Data Protecton Compliant Incident Response System. *European Journal of Law and Technology*, *10*(1).

Yuadi, I., & Khusniah, L. (2022). Pemetaan Penelitian Terkait Keamanan Data di Indonesia. *Petir*, *15*(2), 253–263. https://doi.org/10.33322/petir.v15i2.1586

Yuliana, R., & Hasibuan, Z. A. (2022). Best practice framework for information technology security governance in Indonesian government. *International Journal of Electrical and Computer Engineering*, *12*(6), 6522–6534. https://doi.org/10.11591/ijece.v12i6.pp6522-6534

Yusni, M., & Sigalingging, B. (2021). Encryption as The Legal Protection Against Cybercrimes Associated with Digital Land Certificates in Indonesia. *International Journal of Cyber Criminology*, *15*(2), 124–134. https://doi.org/10.5281/zenodo.4766551

Yusuf, M. Y., Kurniasih, D. K., & Setyoko, P. I. (2023). The Record Management: Upcoming Challenges and Key Components to Enhancing Better Public Services. *Jurnal Manajemen Pelayanan Publik*, *7*(1), 61. https://doi.org/10.24198/jmpp.v7i1.47337