Vol. 2 No. 3 Edisi Juli 2025 **E. ISSN. 3032-2472**

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com

CYBER RISK MANAGEMENT IN THE DIGITAL ERA: AN ANALYSIS OF MITIGATION STRATEGIES AND PREVENTIVE INNOVATIONS AGAINST CYBERCRIME IN INDONESIA

MANAJEMEN RISIKO SIBER DI ERA DIGITAL: ANALISIS STRATEGI MITIGASI DAN INOVASI PENCEGAHAN CYBER CRIME DI INDONESIA

Chalifa Luthfiyya Nadhifa[1], Ova Novi Irama[2], Anggia Sari Lubis[3], Junita Putri Rajana Harahap[4]
[1] Accounting Study Program, Faculty of Economics and Business, Al Washliyah Muslim Nusantara University, Email : *chalifaluthfiyya01@gmail.com*
[2] Accounting Study Program, Faculty of Economics and Business, Al Washliyah Muslim Nusantara University, Email : *novi12345za@gmail.com*
[3] Accounting Study Program, Faculty of Economics and Business, Al Washliyah Muslim Nusantara University Email : *anggiasarilubis@gmail.com*
[4] Accounting Study Program, Faculty of Economics and Business, Al Washliyah Muslim Nusantara University, Email : *junitaputrirajanaharahap@umnaw.ac.id*

*email Koresponden: *chalifaluthfiyya01@gmail.com*

DOI: https://doi.org/10.62567/micjo.v2i3.869

Article info:

Submitted: 04/06/25 Accepted: 13/07/25 Published: 30/07/25

Abstract

Cyber risk management has become a critical issue as the number of cybersecurity incidents continues to rise each year. This study aims to analyze the trends in cyber incidents, the most prevalent types of cybercrimes, and the efforts in mitigation and cyber risk management in Indonesia. According to data from the National Cyber and Crypto Agency (BSSN) for the period 2019 to 2023, the number of incidents increased significantly from 290,000 cases in 2019 to 1,031,389 cases in 2023. The dominant types of cybercrime shifted each year, starting with phishing in 2019, malware in 2020, ransomware in 2021, DDoS attacks in 2022, and data breaches in 2023. This surge in incidents reflects the growing complexity of cyber threats faced by various sectors in Indonesia. In response, the government and private sector have strengthened regulations through the enactment of the Personal Data Protection Law and have adopted technologies such as artificial intelligence (AI) and blockchain to enhance detection and prevention of cyberattacks. Effective cyber risk management requires integrated preventive, detective, and corrective measures to safeguard information systems and sensitive data from increasingly sophisticated attacks. Through collaboration among the government, private sector, and the public, Indonesia's digital ecosystem is expected to become more secure and resilient in the face of cybercrime threats..

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com

Keywords **:** Cyber Risk Management, Cybercrime, Digital Security Incidents, Cyber Threat Mitigation, Government and Private Sector Collaboration

Abstrak

Manajemen risiko siber menjadi isu krusial seiring dengan meningkatnya jumlah insiden keamanan siber dari tahun ke tahun. Penelitian ini bertujuan menganalisis tren insiden siber, jenis kejahatan siber yang dominan, serta upaya mitigasi dan pengelolaan risiko siber di Indonesia. Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN) periode 2019 hingga 2023, jumlah insiden meningkat signifikan dari 290.000 kasus pada 2019 menjadi 1.031.389 kasus pada 2023. Jenis kejahatan siber yang mendominasi mengalami pergeseran setiap tahunnya, dimulai dari phishing pada 2019, malware pada 2020, ransomware pada 2021, serangan DDoS pada 2022, dan kebocoran data pada 2023. Peningkatan jumlah insiden ini mencerminkan semakin kompleksnya ancaman siber yang dihadapi oleh berbagai sektor di Indonesia. Dalam upaya mitigasi, pemerintah bersama sektor swasta memperkuat regulasi melalui Undang-Undang Perlindungan Data Pribadi serta mengadopsi teknologi kecerdasan buatan (AI) dan blockchain untuk meningkatkan deteksi dan pencegahan serangan. Pengelolaan risiko siber memerlukan langkah-langkah preventif, detektif, dan korektif yang terintegrasi guna melindungi sistem informasi dan data sensitif dari serangan yang semakin canggih. Dengan kolaborasi antara pemerintah, swasta, dan masyarakat, diharapkan ekosistem digital Indonesia dapat menjadi lebih aman dan tangguh dalam menghadapi ancaman kejahatan siber.

Kata Kunci : Manajemen Risiko Siber, Kejahatan Siber, Insiden Keamanan Digital, Mitigasi Ancaman Siber, Kolaborasi Pemerintah dan Swasta

1. INTRODUCTION

Cyber risk management is a crucial aspect in the digital era marked by the rapid development of information technology. Digital transformation has changed the way individuals, organizations, and governments interact and carry out daily operations. These changes provide easy access to information, efficiency of business processes, and increased productivity. However, behind these benefits, new threats have emerged in the form of cybercrime. Cybercrime includes various actions aimed at stealing data, damaging systems, and disrupting digital services. Therefore, cyber risk management is an urgent need that must be faced seriously by all parties in Indonesia (Zunit & Zora, 2024) .

Indonesia as one of the countries with an increasing number of internet users faces increasingly complex cybercrime risks. Increasing internet penetration in various sectors, including government, banking, education, and the private sector, opens up opportunities for cybercriminals. Various hacking incidents, data leaks, and ransomware attacks have occurred and caused major losses, both in terms of finance, reputation, and national security. This condition encourages the need to strengthen mitigation strategies and innovation in efforts to prevent cybercrime. (Liddin & Pulansari, 2024) .

Cyber risks not only affect large organizations, but also small and medium enterprises (SMEs) and individuals. Many small business owners are unaware of the importance of data security, making them easy targets for cybercriminals. In addition, individuals are also targets of phishing, malware, and social engineering attacks. This phenomenon shows that cybercrime is not discriminatory, but targets anyone who has a security gap. Therefore, cyber risk mitigation efforts must cover all levels of society. (Budi et al., 2021) .

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com

Cyber risk mitigation efforts in Indonesia face various challenges. One of the main challenges is the low awareness of the importance of cybersecurity among the general public, business actors, and government institutions. Many parties still consider cybersecurity as a technical aspect that is only relevant to information technology experts. In fact, cyber threats can attack anyone without discrimination. In addition, another challenge lies in the limited human resources who have special expertise in the field of cybersecurity. The number of professionals in this field is still relatively small compared to the high need for security in various sectors.

In the context of regulation, Indonesia already has a legal framework to handle cybercrime, one of which is through the Electronic Information and Transactions Law (UU ITE). However, the implementation of this regulation still faces various obstacles, ranging from aspects of implementation, supervision, to legal evidence in court. Many cases of cybercrime cannot be revealed due to limited forensic technology and minimal cross-agency cooperation. Therefore, more adaptive policies and collaboration between institutions are needed in managing cyber risk. (Angel Siti Fatimah & Aini Rahmah, 2022) .

Cyber risk mitigation strategies involve implementing comprehensive technology, policies, and education. On the technology side, organizations need to adopt security software such as firewalls, intrusion detection systems (IDS), and data encryption. Companies also need to build a vulnerability management system that allows early detection of security gaps. In addition to technology, internal policies governing data protection and system access must also be strengthened. These policies include user access management, role-based access restrictions, and strong password management. Increasing cyber literacy through employee education and training is also part of efforts to prevent cybercrime.

Cybercrime prevention innovation requires the development of new approaches that are proactive and based on artificial intelligence (AI) and machine learning (ML). AI and ML technologies enable prediction of cyber attacks before they occur, as well as detecting suspicious patterns that cannot be recognized by humans. The use of this technology provides advantages in more effective cyber risk management. In addition, the development of blockchain-based security systems can also provide additional layers of security, especially in the management of transaction data and digital identities. (Novita et al., 2023) .

Collaboration between institutions is a strategic step in managing cyber risk in Indonesia. The government, private sector, and civil society organizations need to work together to create a stronger cybersecurity ecosystem. The government has an important role in setting policies, providing security infrastructure, and raising public awareness. The private sector needs to be actively involved in implementing security systems in their work environments, especially in the financial sector, e-commerce, and cloud-based services. Civil society organizations can play a role in advocacy and socialization regarding the importance of cybersecurity to the wider community.

The government's role in managing cyber risk is further strengthened by the establishment of the National Cyber and Crypto Agency (BSSN) which is responsible for national cyber security. BSSN is tasked with protecting national critical infrastructure from cyber threats that could disrupt national stability. In addition, the government is also encouraging the establishment of cyber security operation centers (SOC) in various institutions, including government agencies and large companies. This step aims to improve the response to cyber threats in real time.

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com

In terms of financing, cyber risk management requires adequate budget allocation. Organizations need to invest funds in developing security infrastructure, updating systems, and training human resources. The costs incurred for preventing cyber threats are much smaller compared to the losses caused by cybercrime incidents. Therefore, investment in cybersecurity should not be considered as an expense, but rather as a long-term investment that protects the continuity of organizational operations. (Yulanderi, 2020) .

The development of cybercrime in Indonesia shows that criminals continue to develop more sophisticated attack methods. In facing this challenge, collective efforts are needed from various parties. A collaborative approach, technological innovation, and strengthening regulations will create a more resilient cybersecurity system. Public awareness of the importance of cybersecurity must also be increased through educational campaigns and digital literacy.

management in the digital era requires a holistic approach that involves strengthening regulations, implementing advanced technologies, and cross-sector collaboration. The success of cybercrime prevention mitigation and innovation strategies in Indonesia will depend on the synergy between the government, private sector, and society. With an integrated approach, the threat of cybercrime can be minimized, thus creating a safe, trusted, and productive digital environment.

2. RESEARCH METHODS

The research method aims to provide systematic guidelines in collecting, analyzing, and interpreting data relevant to the topics of cyber risk management, cyber threat mitigation, and cybercrime. The selection of the right research method ensures the accuracy of the results and the validity of the conclusions obtained. The research approach used in this study is descriptive with a qualitative approach. This approach was chosen because it allows for in-depth information mining related to the phenomenon of cybercrime, mitigation strategies, and cyber risk management policies implemented in Indonesia. (Supriyanto et al., 2024) . Qualitative research aims to understand the meaning, experiences, and views of research subjects in a particular context. Data collection techniques used include documentation studies and field observations.

Documentation study aims to collect data from various documents relevant to the research topic. The documents analyzed include laws and regulations related to cybercrime, reports from national and international institutions, and previous research results. These documents provide an empirical basis for identifying cyber threat patterns, mitigation strategies, and regulatory policies. Document analysis is carried out systematically by tracing relevant themes and recording key information that can support data analysis. (V, 2024) .

Field observation aims to directly observe the implementation of cyber risk management and mitigation measures in the field. Observations are carried out in organizations that are the object of research, such as companies, government agencies, or other related institutions. Observations include observations of user access management, data security systems, and emergency response processes when cyber incidents occur. Observation data

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com

provides a real picture of the implementation of cyber security policies and the obstacles faced by organizations in managing cyber risk.

Data analysis was conducted thematically using the content analysis method. Data obtained from documentation studies and field observations were analyzed through the process of coding, categorization, and identification of main themes. Coding aims to group data into smaller units according to certain themes. Categorization aims to group codes that have similar meanings into broader categories. From this process, the main themes relevant to cyber risk management, cyber threat mitigation, and cybercrime can be identified. The themes that emerge are analyzed in depth to understand significant patterns, interrelationships between themes, and their influence on the research context. (Jaringan et al., 2023) .

To increase the validity and reliability of the data, this study uses triangulation techniques. Triangulation involves the use of different data sources, data collection methods, and different analysis perspectives. Data is validated by comparing it with data from documents and observation results. Thus, the accuracy and consistency of information can be ensured. Triangulation increases the reliability and validity of research results, so that research findings can be scientifically accounted for.

The research stages start from the problem formulation stage, data collection, data analysis, to the preparation of the final report. The problem formulation stage aims to determine the focus of the research and identify research questions. The data collection stage involves the process of collecting data from documentation studies and field observations. The data analysis stage includes coding, categorization, and identifying main themes. The final stage is the preparation of the research report, which includes findings, discussions, and conclusions obtained from the research process.

The advantage of the qualitative method in this study lies in its ability to explore deep meaning and provide a richer understanding of the phenomenon of cybercrime. The qualitative approach allows for more flexible analysis and is responsive to the research context. However, this approach also has limitations, such as the potential for bias from researchers and research subjects. To overcome these limitations, researchers apply triangulation techniques to ensure data accuracy and reduce potential bias.

method in this study uses a qualitative approach with data collection methods through documentation studies and field observations. Data are analyzed thematically through the process of coding, categorization, and identification of main themes. Data validity is guaranteed through triangulation techniques. This method aims to gain an in-depth understanding of cyber risk management, threat mitigation strategies, and cybercrime patterns that occur in Indonesia. With this method, research is expected to produce valid and useful findings for the development of policies and management of cybersecurity more effectively. (Zunit & Zora, 2024) .

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com

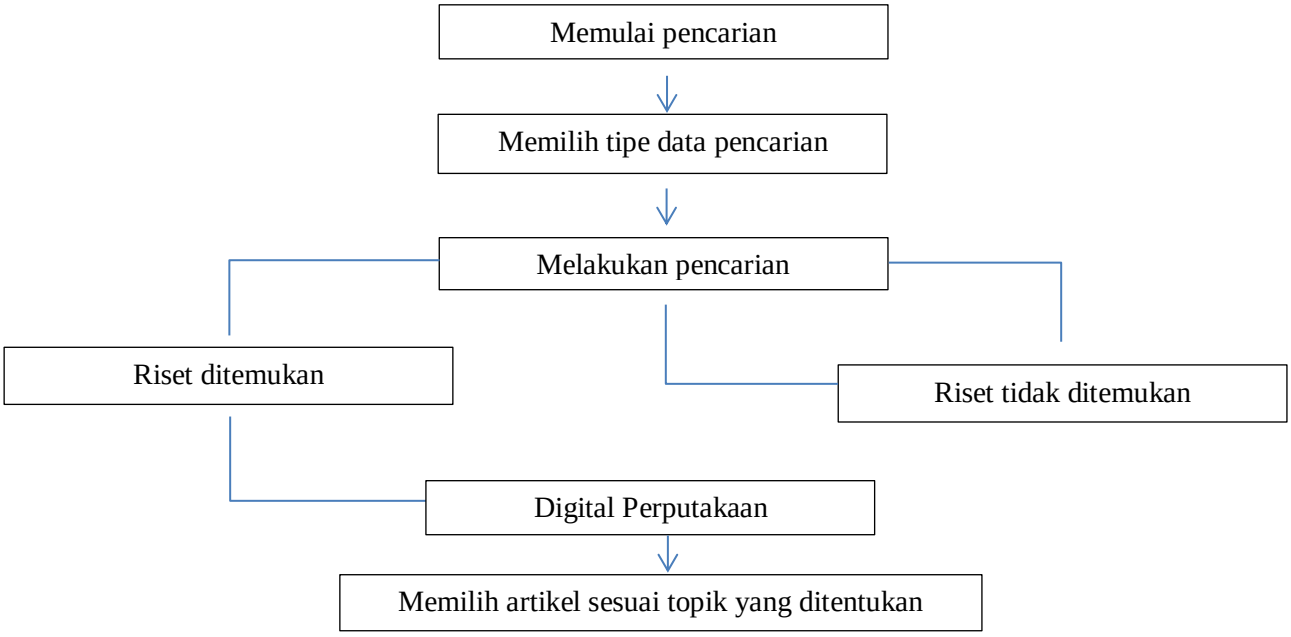

Figure 1: Literature Search Process

3. RESULTS AND DISCUSSION

Results

Table 1.

Year	Number of Security Incidents	Common Types of Cyber Crime (2023)
2019	290,000 incidents	- Phishing: 35%
2020	495,000 incidents	- Malware: 27%
2021	888,711 incidents	- Ransomware: 15%
2022	976,429 incidents	- DDoS attacks: 12%
2023	1,031,389 incidents	- Data Leakage: 11%

Source: BSSN (National Cyber and Crypto Agency) 2019–2023

Based on data from the National Cyber and Crypto Agency (BSSN) for the period 2019 to 2023, there has been a significant increase in the number of cybersecurity incidents in Indonesia. Table 1 shows that the number of cybersecurity incidents has been increasing from year to year. In 2019, there were 290,000 cybersecurity incidents recorded. This figure increased drastically to 495,000 incidents in 2020. This increase shows that during this period there was a significant spike in the number of cyber attacks.

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com

In 2021, the number of security incidents more than doubled compared to the previous year, reaching 888,711 incidents. This increase indicates that cyber threats are increasingly complex and targeted. 2022 recorded a total of 976,429 incidents, indicating that cyber threats have not decreased even though various mitigation efforts have been made. The peak occurred in 2023 with a total of 1,031,389 incidents recorded. This data indicates that cybercrime continues to grow both in terms of the number and types of attacks carried out.

The dominant type of cybercrime varies each year. In 2019, the most common type of cybercrime was phishing, with a percentage reaching 35% of the total incidents. Phishing is an attack method that aims to steal sensitive information through social engineering. Phishing is usually done by tricking victims into providing personal data through fake links or fake websites. This method is quite effective because it involves psychological manipulation of the victim.

In 2020, the dominant type of crime shifted from phishing to malware, accounting for 27% of total incidents. Malware, or malicious software, is designed to infect computer systems and steal data, disrupt operations, or control devices remotely. Malware attacks are often spread through email attachments, fake software downloads, or compromised websites. The shift in dominance from phishing to malware shows that cybercriminals are increasingly relying on more sophisticated and difficult-to-detect methods.

In 2021, ransomware was the most reported type of cybercrime, accounting for 15% of all incidents. Ransomware is a type of malware that encrypts the victim's data and demands a ransom to restore access. Ransomware attacks not only cause financial losses but also disrupt the operations of organizations, including government agencies, hospitals, and private companies. The increase in ransomware cases in 2021 indicates that cybercriminal groups are becoming more organized in exploiting existing security vulnerabilities.

In 2022, the dominant type of crime shifted to distributed denial of service (DDoS) attacks with a percentage of 12%. DDoS attacks aim to disrupt the availability of online services by flooding the target server with large amounts of data traffic, making the service inaccessible. These attacks commonly target e-commerce platforms, financial services, and government websites. DDoS attacks are often used as a form of protest or an attempt to create economic and social disruption. The increase in DDoS attacks in 2022 indicates that cybercriminals are starting to utilize more destructive attack strategies.

In 2023, data breaches will be the most common type of crime, accounting for 11% of all incidents. Data breaches involve the unauthorized disclosure of sensitive data, either intentionally or unintentionally. Leaked data can include personal information, financial data, or confidential organizational information. Data breaches are often caused by hacking, data mismanagement, or unauthorized access to systems. Data breaches involving personal information have a major impact on individual privacy, consumer trust, and organizational reputation. The shift in threat types from DDoS to data breaches reflects cybercriminals' focus on higher-value data on the black market.

Discussion

The increase in the number of cybersecurity incidents from 2019 to 2023 shows that cybercrime is becoming an increasingly serious threat. The development of digital technology, the wider adoption of the internet, and digital transformation in various sectors are factors that drive the increase in cyber threats. Although various mitigation efforts have been made, the

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com

number of incidents continues to increase. Factors such as low cybersecurity awareness, security gaps in digital infrastructure, and the inability of organizations to respond quickly to threats are the main causes.

The shift in cybercrime types from *phishing* to *malware* , *ransomware* , DDoS, and data breaches reflects that cyberattack methods continue to evolve. Each method has different characteristics and impacts. *Phishing* leverages social engineering, while *malware* and *ransomware* are more technology-based. DDoS attacks target service availability, while data breaches impact information confidentiality. This shift in threat types shows that cybercriminals continue to exploit existing security gaps and adapt to changing technologies.

Increasing Cyber Threats in Indonesia

Cyber threats in Indonesia continue to increase along with rapid technological advances and digitalization. Data recorded by the National Cyber and Crypto Agency (BSSN) shows a significant spike in cybersecurity incidents, from 290,000 incidents in 2019 to more than 1 million incidents in 2023 (BSSN, 2023). This increase indicates that more individuals and organizations are being targeted by cyber attacks, whether in the form of personal data theft, system destruction, or financial attacks. The most common type of cybercrime is *phishing* (35%), indicating that attackers prefer social engineering to trick users into providing their personal information and credentials. In addition, *malware* and *ransomware attacks* , which accounted for 27% and 15% of total attacks respectively, are increasingly becoming a concern due to their impact on systems and threatening sensitive data (Sitorus et al., 2024).

Phishing and malware often target critical sectors such as banking, government, and technology companies, which hold highly valuable sensitive data. These attacks are usually accompanied by more complex tactics, such as the distribution of legitimate-looking phishing emails or malware hidden in legitimate applications. This shows the need for stronger defense systems and faster responses to reduce potential losses. With the increasing number of threats, it is important for Indonesia to prioritize strengthening cyber risk management, involving the latest technology and more comprehensive mitigation strategies.

Mitigation Strategies and Innovation in Cyber Risk Management

As cyber threats increase, the Indonesian government and the private sector have begun to introduce various innovations in cyber risk management. One significant step is the establishment of stricter regulations regarding data protection and information security, such as the recently passed Personal Data Protection Law. This regulation aims to provide stronger legal protection for data users, as well as encourage companies to comply with higher security standards (OJK, 2023). In addition, advanced technologies such as artificial intelligence (AI) and *blockchain* are increasingly being used to prevent cyber attacks. AI can help in automatically detecting suspicious attack patterns and providing early warnings to organizations so they can immediately respond to the threat. Meanwhile, blockchain, which is known for its security, has the potential to provide solutions to protect digital transactions and sensitive data from intruders. These technologies, if optimally implemented, can strengthen Indonesia's digital ecosystem and provide better protection against increasingly sophisticated cyber attacks.

Effective cyber risk management requires preventive, detective, and corrective measures. Preventive measures include implementing data security policies, role-based access management, and regular software updates. Detective measures include implementing an automated threat detection system based on artificial intelligence. Corrective measures include

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com

system recovery and security gap repair. With these measures, it is hoped that the number of cybersecurity incidents can be reduced and public trust in the digital ecosystem can be increased.

4. CONCLUSION

The increase in cyber threats in Indonesia recorded from 2019 to 2023 shows that cybercrime is growing rapidly, both in number and complexity. With more than 1 million cyber incidents recorded in 2023, Indonesia faces a major challenge in protecting critical data and systems from cyber attacks. The most common types of attacks, such as *phishing, malware, and ransomware* , require improved defense systems and faster responses. Therefore, more comprehensive cyber risk management and the implementation of technological innovation are a must to prevent the negative impacts of cyber attacks.

5. REFERENCES

Amarullah, A. H., Josias, A., Runturambi, S., Amarullah, A. H., Josias, A., Runturambi, S., & Widiawan, B. (2021). *Jurnal Kajian Stratejik Ketahanan Nasional Analisis Ancaman Kejahatan Siber Bagi Keamanan Nasional Pada Masa Pandemi COVID-19 Analisis Ancaman Kejahatan Siber Bagi Keamanan Nasional Pada Masa Pandemi COVID-19*. *4*(2). https://doi.org/10.7454/jkskn.v4i2.10052

Angel Siti Fatimah, A., & Aini Rahmah, N. (2022). Sistem Informasi, Keuangan, Auditing Dan Perpajakan. *Journal of Comprehensive Science (JCS)*, *1*(3), 419–438. https://doi.org/10.36418/jcs.v1i3.66

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO)*, *3*(November), 223–234. https://doi.org/10.54706/senastindo.v3.2021.141

Harahap, N. M. (2024). Resiko Kejahatan Teknologi Informasi Dan Komunikasi Cyber Crime Dan Analisi Inovasi Pencegahan Resiko Cyber Crime Di Indonesia. *Jurnal Teknologi Dan Manajemen Sistem Industri*, *3*(1), 52–59. https://doi.org/10.56071/jtmsi.v3i1.483

Indonesia, B. D. I. (2023). *Jki 2.3.2023*. *2*(4), 1127–1147.

Jaggar, M., Salemba, J., No, R., Senen, K., Pusat, K. J., & Jakarta, D. K. I. (2021). *PERSPEKTIF GENDER DAN FILSAFAT POLITIK ALISON*.

Jaringan, T., Print, I., Online, I., Napitupulu, C. J., & Utara, U. S. (2023). *InfoTekJar : Jurnal Nasional Informatika dan Analisis Keamanan pada Cloud Computing*. *2*, 2–4.

Khoiriyah, N. M. (n.d.). *Pakta Keamanan Trilateral Aliansi Amerika Serikat , Australia , dan Inggris (AUKUS) Dalam Perspektif Neorealisme*.

Liddin, J. S., & Pulansari, F. (2024). Analisis dan Mitigasi Risiko Pada Supply Chain di PT XYZ Dengan Pendekatan House of Risk (HOR). *JURNAL Al-AZHAR INDONESIA SERI SAINS DAN TEKNOLOGI*, *9*(2), 164. https://doi.org/10.36722/sst.v9i2.2717

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com

Novita, A. P., Fatmanegara, F., Runtuwene, F. J. J., Samuela, J. T., & Syahbani, M. F. (2023). Cyber Security Threats; Analisis Dan Mitigasi Resiko Ransomware Di Indonesia. *Jurnal Ilmiah Sistem Informasi*, *3*(1), 160–169. https://doi.org/10.46306/sm.v3i1.91

Supriyanto, T., Wiyono, W., Yusgiantoro, P., & Midhio, I. W. (2024). *Strategi Keamanan Nasional Republik Indonesia Menghadapi Rivalitas Amerika Serikat - China di Laut China Selatan*. *06*(02), 12694–12711.

V, M. O. (2024). *Analisis Keamanan Siber pada Implementasi Sistem Informasi Rekam*. *7*(4), 824–833.

Yulanderi, E. B. (2020). Strategi Pencegahan Kejahatan Terorisme Di Indonesia Melalui Pembangunan Sosial (Crime Prevention Social Development). *Jurnal Pro Justitia (JPJ)*, *1*(1), 1–9. https://doi.org/10.57084/jpj.v1i1.288

Yuniarti, D. R., Alfarizy, H. F., Siallagan, Z., & Rizkyanfi, M. W. (2023). Analisis Potensi Dan Strategi Pencegahan Cyber Crim Dalam Sistem Logistik Di Era Digital. *Jurnal Bisnis, Logistik Dan Supply Chain (BLOGCHAIN)*, *3*(1), 23–32. https://doi.org/10.55122/blogchain.v3i1.714

Zunit, J. D., & Zora, Z. (2024). Analisis Hukum Internasional Terhadap Allowable Catch Dalam Upaya Pencegahan Praktik Overfishing Dan Penerapannya Di Indonesia. *Nagari Law Review*, *7*(3), 606. https://doi.org/10.25077/nalrev.v.7.i.3.p.606-615.2024