Identifying the Prevalence of Cybercrime in Indonesian Corporations: A Corporate Legislation Perspective

by Djoni Sumardi Gozali

Submission date: 16-Jun-2023 01:10AM (UTC+0700)
Submission ID: 2116778828
File name: Final--Djoni_IJCC-1.pdf (445.07K)
Word count: 5473
Character count: 33484

International Journal of Cyber Criminology
Vol 17 Issue 1 January – June 2023

Identifying the Prevalence of Cybercrime in Indonesian Corporations: A Corporate Legislation Perspective

***Djoni Sumardi Gojali*[1]**
Universitas Lambung Mangkurat, Banjarmasin, Indonesia

Abstract

The continuous development and improvement of information and technology have prompted businesses to implement various technological techniques to complete daily tasks efficiently. This strategy has effectively reduced costs and time; however, excessive internet and online media use have resulted in various challenges for the associated businesses, such as hacking, defamation, unlawful transactions, etc. These offenses are referred to as cybercrimes. Since the turn of the century, the number of cybercrimes committed against Indonesian corporations has risen sharply, causing concern for the Indonesian government. Thus, the present study focuses on the prevalence of cybercrimes in Indonesian corporations, particularly on corporate law. Legal research was conducted for this study, and data were collected from various primary and secondary sources. Based on the findings of this study, the legal framework for cybercrimes in Indonesia consists primarily of the "Electronic Information and Transactions (ITE) Law" and the "Indonesian Criminal Code" (KUHP), which are currently restricted to defamation, online threats, and other individual cybercrimes. However, other crimes relating to corporations, such as data protection, unlawful transactions, and others, are not highlighted in this legal framework, resulting in various obstacles to implementing cyber laws in Indonesia. This has also affected consumers' purchasing performance, influencing the affiliated businesses' social image. Nonetheless, this study has also provided various practical and theoretical implications. To safeguard data, privacy, and transactions in Indonesia, it is also suggested that a cybersecurity law be drafted.

Keywords: Cybercrimes; Indonesia; Corporations; Corporate Legislation; Business Law; KUHP

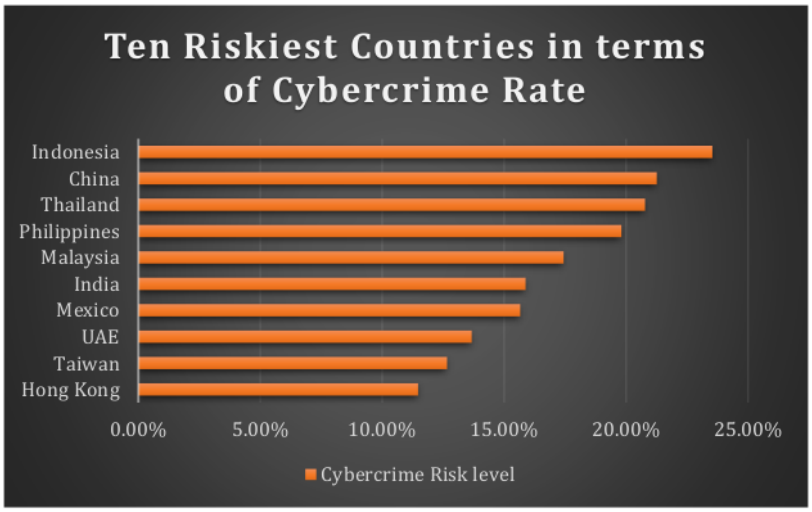
1. Introduction

In Indonesia, a country governed by civil law, cybercrime at the corporate level is increasing daily, necessitating the formulation of frameworks and laws that could be beneficial in preventing cybercrime at the corporate level. Indonesia has experienced

[1] Study Program of Law, Universitas Lambung Mangkurat, Banjarmasin, Indonesia.
Email: djoni.gozali@ulm.ac.id

a rise in cybercrime due to the daily advancement of technology in the current era. To eliminate the prevalence of cybercrime at the corporate level, adhering to enacted and enforced laws is necessary. Recent research (Akdemir, Sungur, & Başaranel, 2020) indicates that cybercrime can be defined in two distinct ways, as described by Loader and Thomas (2013) and Gordon and Ford (2006). Thomas and Loader define cybercrime as "illegal computer-mediated activities that can be carried out via a global network of electronic technologies." In contrast, Gordon and Ford define cybercrime as a "crime that has been committed by using a hardware device or computer network" (Phillips et al., 2022).

It has been observed that cybercrime has increased in Indonesia. As a result, policymakers have enacted telematic laws to combat the increase in cybercrime and regulate the occurrence of telecommunication accidents in the country (Amin & Huda, 2021). Moreover, in 2019, the government reported 290 million cyberattack cases, a 25 percent increase compared to previous years, and the country's loss due to cybercrime exceeded $34.2 billion U.S. dollars (as shown in Graph 1 below).



Graph 1: 10 riskiest countries in terms of Cybercrime Rate (Source: Author generated)

As is evident from the preceding diagram, Indonesia's cybersecurity laws were implemented within the constitutional framework. The first law thus implemented for cybersecurity in Indonesia was Electronic Information and Transaction Law (EIT) No. 11/2008, which was revised as law No. 19/2016, but it was deemed inapplicable for cybersecurity because it only applied to offenses prohibited in Indonesia, such as corporate content theft (Sunkpho, Ramjan, & Ottamakorn, 2018). Although it provided substantial legal protection for electronic transactions, it was modified by GR 71/2019, which, in addition to ensuring the security of transactional systems, protected organizations' personal information and data (Tapsell, 2020). In addition, this law assured the authenticity of websites to prevent any scams or fraudulent activities involving websites (Amin & Huda, 2021).

The current study is founded on the prevalence of corporate-level cybercrime in Indonesia. The researcher will focus on two primary objectives: the prevalence of cybercrime within Indonesian corporations and the impact of cybercrime on Indonesian corporate law. In many countries, including Indonesia, whistleblowers are essential in fostering cybersecurity. It refers to the mechanism of corporate governance that ensures transparency and accountability and detects wrongdoings, such as bribery and corruption (Mehrotra et al., 2020). As it has been observed that cybercrime is increasing in the Indonesian business sector and there is no robust cybersecurity framework in Indonesia, the current research will enable the Indonesian constitution to promote effective cybersecurity laws.

In addition, it will have substantial practical and theoretical implications. The current investigation is organized into several sections. The first section explains the background of the research, the need for cybersecurity in Indonesian corporations, and the constitutional laws enforced by the policymakers for the prevention of cybercrime in the country. This is followed by a literature review that explains the prevalence of cybercrime within corporations worldwide and the role of corporate legislation on cybercrime, i.e., it will explain the impact of corporate legislation on cybercrime. In addition, the study's methodology describes the relevant method employed by the researcher, followed by the results and the researcher's interpretation of them. To provide an opportunity for future researchers, the researcher has concluded, explained the study's implications, and highlighted the study's limitations.

2. Method

Research methodology is required for conducting and analyzing research to obtain generalizable results from a particular study. In addition, the research methodology clarifies the objectives, focusing on the researcher and playing a crucial role in achieving the study's purpose. The researcher chose the qualitative inductive approach for the data collection of the current research because it enables the researcher to easily analyze large amounts of data collected, as the present study focuses on the prevalence of cybercrime within Indonesian corporations and the assessment of legislative rules and regulations enforced by various countries to eradicate cybercrime at the corporation level. The researcher has used both primary and secondary sources to collect data. The researcher collected preliminary data from various primary legal resources, including legal documents, laws, legislation, and case laws. The researcher has gathered secondary data from various sources, including journal articles, books, and online databases such as Hein Online, Taylor & Francis, Wiley online library, JSTOR, and Google Scholar. In addition, the shortcomings of the current study's methodology will aid the researcher in providing recommendations for future research, and it will provide a solid legislative law framework that could be enforced to eliminate the prevalence of cybercrime within Indonesian corporations.

3. Literature Review

3.1. Prevalence of Cybercrime in Corporations

Within corporations and the business world, cybercrime is an outsider crime that impedes the safe completion of transactions by corporations around the globe. According to research (Williams et al., 2019), external business cybercrime aims to

illegally transfer all money or valuables to themselves, resulting in economic or political surveillance. Despite the outsiders, there is another type of cybercrime known as insider business cybercrime, in which the perpetrator is accused of assessing the company's personal data in a manner that compromises the confidentiality, integrity, and availability of the organizational data. The United Kingdom's corporations have applied the Routine Activities Theory by analyzing the Cardiff University UK Business Cybercrime Survey to evaluate corporate insider crime. In addition, it has been determined that cybercrime is the greatest threat to the United Kingdom's business community (Devanny, 2015). To eradicate cybercrime in the country, the United Kingdom Government has invested £2 billion in cybersecurity from 2016 to 2021, which includes resources for businesses to protect themselves from becoming victims. According to the Information Security Breaches Survey (ISBS), from 1998 to 2015, the United Kingdom's business community was subjected to high levels of business cybercrimes, including hacking, fraud, virus infection, and insider cybersecurity breaches (Williams et al., 2019).

On the other hand, Malaysia has begun its path to becoming a developed nation by advancing the information technologies utilized by Malaysian organizations, resulting in cybercrime and larceny. With the aid of a survey conducted by PricewaterhouseCoopers Malaysia (PWC, 2016), it was discovered that nearly 42% of Malaysian organizations were at risk of increasing cyber threats. For instance, the country's investments in information technology security pave the way for electronic theft due to poor investment decisions (Abidin, Nawawi, & Salin, 2019; Sen & Borle, 2015). Research has demonstrated that such investments worsen the organization's condition when implementing the security feature requires a substantial investment, and a single incorrect decision increases cybercrime within the organization. This assures that technological advancements have increased the prevalence of cybercrime in the modern world. In the current business environment, evaluating the laws and regulations designed to combat cybercrimes and promote cybersecurity is necessary.

3.2. Cybercrime in Corporate Legislation

Corporate law is essential to formulating a nation's rules, regulations, and enforcement of legal frameworks and laws. In Nigeria, for instance, the prevalence of cybercrime has increased alongside technological development (Awotoye & Akinola, 2022). Nigeria's corporate legislation has enacted several laws prohibiting activities in Nigerian cyberspace. These laws include the Economic and Financial Crime Commission Act of 2004, the penal code, the criminal code, the Money Laundering (Avoidance and Exclusion) Act of 2022, and the Cybercrime Act of 2015. The Nigerian corporations that drafted these cybercrime laws provided justice and a deterrent to cyber criminals. This impacts the significance of corporate laws for averting cybercrime in the business world.

The researcher provided a similar illustration of cybercrime in which there was a high risk of stealing consumer data from Malaysian organizations (Abidin et al., 2019). Malaysia has enacted numerous laws, including the Personal Data Protection Act 2010, to eliminate the loss of consumer data and reduce cybercrime in the country's business environment. This Act is also known as Act 709, and it applies to all individuals within an organization who are capable of assessing the personal

information of consumers or who have access to such information about commercial transactions in Malaysia. This law enforcement in Malaysia contributed to the eradication of cybercrimes and the protection of the economy.

Various international laws have been implemented within the framework of the Philippines to eliminate corporate cybercrimes and safeguard the economy and politics of the nation (Pamela, Fabe, & Zarcilla-Genecela, 2021). The European Union Cybersecurity Act, which entered into force on June 27, 2019, is one of these international cybersecurity laws. This act was quite effective in regulating cybercrimes in the Philippines, as its effects include: Also created were 1) the European Union Cybersecurity Agency and 2) a cybersecurity certification framework. This framework was instrumental in establishing compliance standards for EU member states. In addition, Philippine companies that operate within the EU framework will prevent cybercrime and promote effective cybersecurity within the country, thereby enhancing the Philippines' economic standing. Therefore, corporate legislation is the researcher's primary concern, as it significantly affects cybercrime worldwide.

4. Findings and Discussion

This section focuses primarily on the findings and discussion of the legal study. This section consists of three subsections. The first section examines cybercrime laws in Indonesia that have been formulated with the prevalence of cybercrime in mind; the second section examines corporate cybercrime legislation in Indonesia; and the third section discusses the impact of cybercrime and corporate legislation on businesses in Indonesia.

4.1 Section I: Cybercrimes Laws in Indonesia

Utilizing the internet and digital media has become crucial in today's technologically advanced society, often resulting in a variety of cybercrimes. Even in Indonesia, the number of cybercrimes continues to rise, particularly in the business sector, resulting in inadequate outcomes. Different laws and regulations have been devised and implemented over the years to combat cybercrime (Hasbullah, 2022). Typically, the essence of cybercrimes changes occasionally, resulting in alterations to the associated laws and acts. Different varieties of cyberattacks have arisen due to technological advancements. At the beginning of the 20th century, Advanced viruses, Malicious Code, and Morris Code were the most frequently observed cyber-related issues (Stevani & Disemadi, 2021). Moreover, due to the continuous development of technology, cyber warfare, and espionage have emerged as the primary threats to various institutions and organizations in Indonesia. Consequently, cyber laws are formulated to promote ethical cyber activities and impose various punishments on those who commit cybercrimes.

In Indonesia, the development of Cyber Law is focused on three areas: Informatics Law, Telecommunications Law, and Media Law (Koto, 2021). These three statutes are believed to be responsible for establishing the limitations and conditions of cyber security. The "Electronic Information and Transactions (ITE) Law" and the "Indonesian Criminal Code" (KUHP) comprise the majority of Indonesia's legal framework about cybercrimes. Nonetheless, the ITE law is the most commonly utilized cyber security law in Indonesia, despite its challenges and issues. Different

acts (such as the Black Law) have been devised in the context of this law that are insignificant in promoting cyber security (Wijaya & Arifin, 2020). Approximately eleven UU ITE articles are used to evaluate cybercriminals. These articles present more than twenty-two categories of cybercriminal behavior. This law defines cyberspace activities and imposes certain restrictions in Article 27. In addition to highlighting the defamation charges, this article emphasizes the unlawful transfer of confidential information through digital means.

In contrast, article 28 of this law penalizes individuals who misuse confidential information and commit a cybercrime (Mauladi, Laut Mertha Jaya, & Esquivias, 2022). However, article 29 of this law addresses the unlawful disclosure of sensitive residential details. It also concentrates on threatening document leakage, commonly called security misconduct at the micro level. The violations of such cybercrimes are emphasized in articles 45 to 51 of the UU ITE.

In 2014, the Indonesian government enacted "Law Number 11/2008" to define the nature of cybercrime and its associated penalties (Siregar & Lubis, 2020). In this regard, the "Intellectual Property Right Act of 2002" was also concerned with reducing cybercrimes. However, the escalating number of cybercrimes in Indonesia has prompted various law enforcement agencies to take significant steps to promote cyber security. Revision of non-punitive policies is crucial to reducing the number of cybercrimes in Indonesia at this critical time (Amin & Huda, 2021). However, Indonesia's corporate sector is heavily impacted by cybercrime, affecting the overall credibility of Indonesia's law enforcement agencies.

4.2 Section II: Corporate Legislation Regarding Cybercrimes in Indonesia

Social, cultural, and economic changes have predominantly resulted from the development and expansion of technology. Even though information and technology have proven effective in various spheres of work and life, they also produce insufficient outcomes that have negligible effects on society and the business world. To reduce and prevent cybercrimes, the Indonesian government has made numerous endeavors to develop and implement significant laws and regulations in this area (Hasbullah, 2022). Cyber law in Indonesia is divided into public and private law categories. However, cyber law emphasizes consumer privacy and public data protection. Cyberlaw concentrates on intellectual property (IP), e-commerce, electronic contracts, and cybersquatting in the private sector. People who use, interact, and communicate online are held accountable by the law. In Indonesia, the media and informatics laws have not been recognized, whereas the concept of cyber law has been introduced in the context of an already substantial law dispute. However, media laws and law informatics deal with intellectual property rights related to telecommunication and press laws (Sukayasa & Suryathi, 2018).

The ITE law is one of Indonesia's primary pillars of cyber law. This law is responsible for combating cybercrime in Indonesian businesses. Additionally, "Law No. 36 of 1999 on Telecommunications" has emphasized data and privacy protection in electronic communications (Sirait et al., 2020). This law is also effective at preventing unlawful information exchange via electronic means. Nonetheless, the absence of a precise cyber law in Indonesia in 2008 increased the urgency to develop and implement an effective cyber law. Later, significant amendments to the 2008 Law

were made in 2016, and the resulting document was titled "Law No. 19 of 2016 on Amendments to Law No. 11 of 2008 on ITE. Under this law, cybercriminals were subject to severe penalties. However, ITE's primary focus has shifted from online transactions and information to wagering, hate speech, and defamation, affecting this law's compatibility. Currently, the "law of the Government Regulation Concerning Electronic Systems and Transaction Providers (82/2012)" and ITE (11/2008) are the main components of the legal framework of cybercrimes in Indonesia; however, they are inadequate to promote cyber security in Indonesian corporations, resulting in insignificant outcomes (Agustiwi, Nugraha, & Pratiwi, 2020). Consequently, there is an urgent need to develop and implement an effective legal framework in the context of cybercrimes in Indonesian corporations, resulting in effective results.

4.3 Section III: Impact of Cybercrimes and Corporate Legislation on Businesses in Indonesia

Cybercrimes also affect businesses by influencing their clients and consumers, resulting in sometimes insurmountable financial losses. After the Covid-19 pandemic, numerous businesses have promoted their digital presence to reach customers more readily. However, according to Lubis et al. (2023), such online enterprises effectively reduce costs and save time and resources. In addition, online enterprises result in other issues for Indonesian businesses, such as increased cybercrime. Customer confidence is the most effective strategy for increasing revenues and obtaining high market shares, thereby contributing to the company's competitive advantage. Therefore, the persistent prevalence of cybercrime in Indonesian corporations has significantly eroded customer confidence, resulting in ineffective results (Hasbullah, 2022). It has been observed that cybercrimes frequently violate the confidentiality provisions between companies and customers, resulting in negative outcomes for all parties involved. These crimes also have a negative effect on the company's social image.

Cybercrimes are believed to be capable of compromising the stability of businesses, resulting in negligible effects for the affected businesses. To safeguard the privacy and data of customers, the development and implementation of effective cyber laws and acts are deemed essential. In addition, cybercriminals have a direct and significant impact on customers and business laws (Hasibuan & Tobing, 2022). It has been observed that cybercrimes frequently influence consumers' purchasing decisions. In this regard, the legal practices of the affiliated businesses are deemed crucial. However, Indonesia's legal framework regarding cyber laws is ineffective. As a consequence, cyber crimes have a significant impact on the corporate world in Indonesia, leading to ineffective results. Thus, the present research has successfully highlighted the various business laws and regulations applicable to Indonesian corporations.

5. Conclusion

Continued growth and technological advancement have led to increased cybercrime in the modern digital world, particularly in the corporate sector. Different governments and international organizations have developed and implemented significant laws and policies to combat cybercrime to achieve effective results. However, in some developing nations, corporate law is still underdeveloped, which hinders the incorporation of cybercrimes into the corporate world. This study has also emphasized the corporate legislation about cybercrimes in Indonesia,

highlighting significant gaps in the associated framework that may affect the overall performance of companies by affecting their social image. It has been observed that cybercriminals frequently use customers' confidential information for unlawful transactions and other purposes, which negatively affects customers' purchasing behavior and results in a variety of financial losses for the associated businesses. Developing cyber laws and acts is crucial to preventing cybercrimes in this regard. In Indonesia, however, the private and public spheres of cyber laws are not delineated, preventing law enforcement agencies from taking significant action against cybercriminals and imposing severe penalties. Nonetheless, in the current study, recommendations have been made to improve the corporate legislation regarding cybercrimes in the Indonesian corporate world to achieve effective results, resulting in significant practical implications that add value to the current study.

6. Recommendations

Cyber laws have received a great deal of attention in recent years due to the consistently rising number of cybercrimes worldwide. These cybercrimes are not limited to cyberbullying, defamation, and other individual offenses; they have also significantly impacted the business world. Numerous cybercriminals hack the confidential information of the consumers and clients of various businesses, resulting in illegal transactions. Due to certain unavoidable gaps, the legal framework of Indonesia regarding cyber laws is insufficiently effective and robust; consequently, the following recommendations can be considered to enhance corporate legislation to reduce cybercrimes in associated corporations:

- The government of Indonesia should establish a cybersecurity law that prioritizes the protection of people's data, privacy, and transactions. This law should also be accountable for determining corporate cybercrimes, and cyber criminals who commit them should face severe penalties. This will help promote a secure corporate environment, reducing the risk of cyber-attacks.
- Businesses should develop and implement a cyber-security system to detect cybercriminal activity. Effective innovation techniques and strategies should be encouraged to achieve the desired results. This strategy will also effectively introduce crucial cyber-security standards essential for attaining successful outcomes.
- Significant modifications should be made to the KUHP and the ITE to incorporate essential data protection laws to safeguard the confidential information of customers and clients of various corporations. Such amendments should also emphasize the promotion of telecommunications law to ensure the secure use of various online media to prevent cybercrimes that could harm the social image of the associated company.

7. Research Implications

This research has both practical and theoretical significance. This study has emphasized cybercrime issues within the context of Indonesian corporations, which have not been addressed extensively in previous research. In addition, this study has effectively identified the difficulties law enforcement agencies face in implementing cyber laws. In addition, the present study has presented an effective legal framework

of cyber laws in Indonesia, which can enhance the knowledge of associated individuals regarding cybercrimes and their impact on businesses. In the context of Indonesian corporate law, the current study has effectively filled research gaps left by previous studies. It has been observed that most previous studies have focused on cyber laws in the context of developed countries such as the United Kingdom, Canada, and the United States; however, little attention has been paid to developing and under-developed countries in this context, leaving a gap in the legal research regarding corporate legislations in the context of cybercrimes. In this regard, the present investigation has demonstrated its effectiveness. In addition to highlighting the effects of cybercrimes on cultural, economic, and social changes, this study asserts that cybercrimes have a significant impact on the corporate world.

In addition to its theoretical significance, the present study provides practical implications that significantly enhance its overall value. For example, the findings of this study effectively identify the gaps in Indonesia's cyber laws, encouraging the government of Indonesia and other affiliated organizations to make significant amendments to these laws to safeguard businesses from cybercrimes. This study is also useful for enhancing the public's understanding of the potential effects of cybercrime on the performance of businesses, encouraging them to play their part in combating cybercrime to promote a secure and healthy working environment for all. This study can also effectively motivate policymakers to develop and implement vital cyber security policies to reduce and prevent cybercriminal activity. Effective outcomes can also be attained with the assistance of this study by encouraging the management of various companies to implement a cyber-security system to ensure the safety of their customers and other stakeholders.

8. Limitations and Future Research Directions

Even though the present study successfully determined the prevalence of cybercrimes within the context of Indonesian corporations, it has limitations that can be addressed in future studies. Due to data availability, this study focused exclusively on Indonesian business laws regarding cybercrimes. This strategy has significantly diminished the value of the study. Similarly, this study has only examined the impact of cybercrimes on businesses. Due to researcher bias, the relationship between cybercrimes and consumer behavior has received no attention. This has left a gap in the current research. In addition, no comparative analysis between civil law and common law systems has been conducted to comprehend the role of cybercrimes, limiting the effectiveness of this study.

Therefore, the limitations mentioned above effectively offer avenues for future research and encourage future research in the context of business laws about cybercrimes. Future research can concentrate on the corporate cybercrime laws of various nations to take a broader, more effective approach to the topic. Future research can also focus on the effect of cybercrimes on customer behavior, with a particular emphasis on the role of the social image of the associated companies. In addition, an effective comparative analysis between various civil law and common law countries in future research can help us better comprehend the limitations of corporate cybercrime legislation. This strategy will effectively provide significant solutions to the associated global cybercrime problems.

References

Abidin, M. A. Z., Nawawi, A., & Salin, A. S. A. P. (2019). Customer data security and theft: a Malaysian organization's experience. *Information & Computer Security, 27*(1), 81-100. https://doi.org/10.1108/ICS-04-2018-0043

Agustiwi, A., Nugraha, R. W., & Pratiwi, D. R. (2020). Implementation of Law Number 11 of 2008 on Electronic Information and Transactions Against the Rise of Hoax Culture During Covid-19 Pandemic in Indonesia. *Surakarta Law and Society Journal, 3*(1), 55-66. http://dx.doi.org/10.32019/slsj.v3i1.4781

Akdemir, N., Sungur, B., & Başaranel, B. (2020). Examining the Challenges of Policing Economic Cybercrime in the UK. *Güvenlik Bilimleri Dergisi*, 113-134. https://doi.org/10.28956/gbd.695956

Amin, M. E., & Huda, M. K. (2021). Harmonization of Cyber Crime laws with the Constitutional Law in Indonesia. *International Journal of Cyber Criminology, 15*(1), 79-94. https://doi.org/10.5281/zenodo.4766534

Awotoye, T., & Akinola, O. B. (2022). An Examination of the Corporate Criminal Liability Within the Nigerian Cyberspace. *Legal Network Series*, 1-26. https://www.researchgate.net/publication/366310582

Devanny, J. (2015). Co-ordinating UK Foreign and Security Policy: The National Security Council. *The RUSI Journal, 160*(6), 20-26. https://doi.org/10.1080/03071847.2015.1122977

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in computer virology, 2*, 13-20. https://doi.org/10.1007/s11416-006-0015-z

Hasbullah, M. A. (2022). Identifying the Effects of Cybercrime on Business Laws: Implications for Businesses and Consumers. *International Journal of Cyber Criminology, 16*(2), 119-130. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/112

Hasibuan, E. S., & Tobing, C. I. (2022). Prevention of Criminal Acts of the Drug Trade Through the Internet Media Based on Positive Law in Indonesia. *Journal of Law, Politic and Humanities, 3*(1), 208-2015. https://doi.org/10.38035/jlph.v3i1.151

Koto, I. (2021). Cyber Crime According to the ITE Law. *International Journal Reglement & Society (IJRS), 2*(2), 103-110. https://doi.org/10.55357/ijrs.v2i2.124

Loader, B. D., & Thomas, D. (2013). *Cybercrime: Law enforcement, security and surveillance in the information age*. Routledge. https://doi.org/10.4324/9780203354643

Lubis, F. S., Lubis, M., Hakim, L., & Fakhrurroja, H. (2023). The Text Mining Analysis Approach for Electronic Information and Transaction (ITE) Implementation Based on Sentiment in the Social Media. In *Intelligent Sustainable Systems: Selected Papers of WorldS4 2022, Volume 1* (pp. 263-271). Springer. https://doi.org/10.1007/978-981-19-7660-5_23

Mauladi, K. F., Laut Mertha Jaya, I. M., & Esquivias, M. A. (2022). Exploring the link between cashless society and cybercrime in Indonesia. *Journal of Telecommunications and the Digital Economy, 10*(3), 58-76. https://doi.org/10.18080/jtde.v10n3.533

Mehrotra, S., Mishra, R. K., Srikanth, V., Tiwari, G. P., & Kumar, E. M. (2020). State of whistleblowing research: A thematic analysis. *FIIB Business Review, 9*(2), 133-148. https://doi.org/10.1177/2319714519888314

Pamela, A., Fabe, H., & Zarcilla-Genecela, E. (2021). The Philippines' Cybersecurity Strategy: Strengthening partnerships to enhance cybersecurity capability. In *Routledge Companion to Global Cyber-Security Strategy* (pp. 315-324). Routledge. https://doi.org/10.4324/9780429399718-29

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sciences, 2*(2), 379-398. https://doi.org/10.3390/forensicsci2020028

PWC. (2016). *Economic crime from the board to the ground: why a disconnect is putting Malaysian companies at risk*. Kuala Lumpur: PricewaterhouseCoopers Malaysia. https://www.pwc.com/my/en/assets/publications/gecs-report-2016.pdf

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems, 32*(2), 314-341. https://doi.org/10.1080/07421222.2015.1063315

Sirait, T., Sarjolo, A., Rajagukguk, M., & Sirait, G. (2020). Legal Protection of Electronic Data is approved by electronics as Regulated in Article 1 (one) Paragraph 9 (nine) of Law No. 19 of 2016 in Conjunction with Law No. 11 of 2008 Concerning Information and Electronic Transactions. In *Proceedings of the First Nommensen International Conference on Creativity & Technology, NICCT, 20-21 September 2019, Medan, North Sumatera, Indonesia*. EAI. http://dx.doi.org/10.4108/eai.20-9-2019.2296616

Siregar, G., & Lubis, M. A. (2020). The Effectiveness of The Imposition of Prison Sentences of Fines For Perpetrators of Electronic Technology Information Violations. In *Virtual Conference on Social Science in Law Political and Economic Development*. VCPSPILED 2020. http://dx.doi.org/10.2478/9788366675377-049

Stevani, W., & Disemadi, H. S. (2021). Urgency of Cryptocurrency Regulation in Indonesia: The Preventive Action for Ransomware Crime. *Hang Tuah Law Journal*, 52-66. https://doi.org/10.30649/htlj.v5i1.32

Sukayasa, I. N., & Suryathi, W. (2018). Law Implementation of Cybercrime in Indonesia. *Soshum: Jurnal Sosial dan Humaniora, 8*(2), 123-130. https://dx.doi.org/10.31940/soshum.v8i2.985

Sunkpho, J., Ramjan, S., & Ottamakorn, C. (2018). Cybersecurity policy in ASEAN countries. In *17th Annual Security Conference* (pp. 1-7). https://www.researchgate.net/publication/324106226

Tapsell, R. (2020). *Indonesia's Policing of Hoax News Increasingly Politicised*. ISEAS-Yusof Ishak Institute. https://www.iseas.edu.sg/images/pdf/ISEAS_Perspective_2019_75.pdf

Wijaya, M. R., & Arifin, R. (2020). Cyber Crime in International Legal Instrument: How Indonesia and International Deal with This Crime? *IJCLS (Indonesian Journal of Criminal Law Studies), 5*(1), 63-74. http://dx.doi.org/10.15294/ijcls.v5i1.23273

Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2019). Under the corporate radar: Examining insider business cybercrime victimization through an application of routine activities theory. *Deviant Behavior, 40*(9), 1119-1131. https://doi.org/10.1080/01639625.2018.1461786

Identifying the Prevalence of Cybercrime in Indonesian Corporations: A Corporate Legislation Perspective

ORIGINALITY REPORT

7%	6%	5%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Middle Georgia College Student Paper	5%
2	madoc.bib.uni-mannheim.de Internet Source	2%

Exclude quotes	On	Exclude matches	< 2%
Exclude bibliography	On		