Journal of Digital Law and Policy
Volume 3 Number 1, September 2023
e-ISSN 2808-3458 p-ISSN 2808-3652
https://ejournal.sidyanusa.org/index.php/jdlp

An Examination of Cybercrimes Leading to Vulnerabilities in Energy, Transportation, and Financial Systems

Ni Ketut Tri Srilaksmi[1], Moh. Erkamin[2], Naylah Dzakiah[3], Ngakan Kompiang Adi Suardana[4], Ni Kadek Sri Devi Putri Swambini[5]

[2]*Sekolah Tinggi Agama Hindu Negeri Mpu Kuturan, Singaraja, Indonesia*
[2]*Universitas Tunas Pembangunan, Surakarta, Indonesia*
[3,4,5]*Institut Bisnis dan Teknologi Indonesia, Denpasar, Indonesia*

Email: [1]gektrisrilaksmi@gmail.com, [2]erkamim@lecture.ac.id, [3]naylahdzzakiah@gmail.com, [4]ngakankompyang72@gmail.com, [5]deviswambini@gmail.com

Received on	*Revised on*	*Accepted on*
30 06 2023	*27 08 2023*	*15 09 2023*

Abstract

The commencement of the current decade is the primary milestone in the progression from Industry 4.0 to Society 5.0. The contemporary period necessitates the ability of individuals from all strata of society to effectively acclimate to the rapid advancements in technology. In the context of Society 5.0, which emphasizes the central role of human beings in generating novel value through technical advancements, there exists the potential to mitigate future disparities among individuals and address economic challenges. The potential risks that may emerge are diverse, intangible in tangible terms, and characterized by uncertainty. The aforementioned threat is a cyber threat that possesses the capacity to inflict significant losses upon a nation. One potential future development of significant consequence involves the occurrence of cyberattacks against essential national assets or critical infrastructure, including but not limited to renewable energy facilities, transportation networks, and financial institutions. Hence, it is imperative for all nations to possess the capability to effectively organize training programs, establish fresh military units, and enhance their individual national defense capabilities. In brief, the text elucidates the prevailing societal transition towards Society 5.0, which underscores the vital role of humans in technology progress. This highlights the potential advantages of this transition, such as the mitigation of inequalities and economic difficulties, while also stressing the importance of implementing strong cybersecurity protocols to prevent possible cyber risks in this dynamic technological environment.

Keywords: *renewable energy, cyberattacks, cyber prevention.*

INTRODUCTION

In the context of Indonesia, it is imperative to recognize the significance of digital literacy, particularly in relation to digital safety, due to the vulnerability of the education sector to cyber assaults. The prevalence of

cyber risks or cybercrime has grown in tandem with the advancement of Information and Communication Technology (ICT) over the past decade. This correlation can be attributed to the increased interconnectedness of many entities, such as businesses, governmental organizations, and society as a whole, with cyberspace.

In light of the findings of digital literacy monitoring and government studies, it is imperative for higher education service providers to prioritize digital security measures. Specifically, their focus should be on safeguarding vital information infrastructure from cyberattacks, such as web defacement, as stipulated by Presidential Decree Number 82 of 2022, which pertains to the protection of Vital Information Infrastructure (IIV). The primary objective of this Presidential Decree is to establish comprehensive regulations and enhance the existing legal structure pertaining to the protection of information and infrastructure vulnerabilities (IIV). This includes measures to heighten consciousness and readiness in effectively addressing cyber assaults. The issuance of Presidential Decree Number 82 in 2022 aims to establish a robust and efficient safeguarding mechanism for the protection of critical information infrastructure against potential cyber threats. In the year 2019, Indonesia witnessed a significant number of cyber security assaults, with reports indicating a total of 290 million cases. According to the study conducted by[1], The concept of cyber, as documented by the Agency, refers to the realm of computer-based systems, networks, and digital technologies. It encompasses the interconnectedness of these systems and the associated risks and vulnerabilities that arise from their use. The Agency's records provide insights into the multifaceted nature the number of reported instances pertaining to Cyber and National Cryptography (BSSN) had a 25% increase compared to the previous year. These incidents resulted in a financial loss amounting to 34.2 million US Dollars.[2] According to the BSSN, a total of 88 million cyberattack cases were registered between January and April 2020, coinciding with the COVID-19 pandemic. The two documented incidents encompass notable instances of phishing, virus spam, and ransomware.

The COVID-19 pandemic has expedited the transition of nearly all social media platforms into the digital domain. For instance, the implementation of remote work policies, sometimes referred to as "work from home" or "work from anywhere" arrangements. In January 2022, the total number of internet users in Indonesia amounted to 204.7 million individuals, which accounts for around 73.7% of the country's overall population. Based on Kepios' analysis, there is projected to be a growth of 2.1 million internet users from 2021 to 2022. The frequency at which digital work is being conducted is steadily rising, resulting in a growing accumulation of data from individuals, corporations, and state agencies. However, there is a growing trend of heightened vulnerabilities in the realm of digital information technology, namely in the domain of cyber security.

The proliferation of data theft, unauthorized access to government-owned websites, network disruption, and other illicit activities pose significant risks of both tangible and intangible damages. Indeed, it is evident that the frequency of cyberattacks has the potential to escalate annually. In the year 2021, the National Cyber and Crypto Agency (BSSN) documented an estimated total of 1.6 billion instances of cyberattacks. Additionally, they forecasted probable economic ramifications, estimating potential damages of up to 14.2 trillion.

---

[1] W. W. Soewoeh, C. A. J., Tenda, E., Ketaren, E., & Kalengkongan, "ANALISA KERENTANAN WEBSITE FMIPA UNSRAT BERDASARKAN OPEN WEB APPLICATION SECURITY PROJECT TOP 10 FRAMEWORK," *Journal of Engineering, Computer Science and Information Technology*, 2022.

[2] BSSN, "Peraturan Presiden Nomor 53 Tahun 2017 Tentang Badan Siber Dan Sandi Negara" (2017), https://peraturan.bpk.go.id/Home/Details/72920/perpres-no-53-tahun-2017.

A cyberattack, also known as a cyberattack, refers to an offensive tactic employed by nations, individuals, groups, or organizations to target computer information systems, infrastructure, computer networks, and/or personal computer devices. These attacks involve the use of various malicious actions, typically originating from anonymous sources, with the intention of stealing, modifying, or destroying a specific target by exploiting vulnerabilities within a system through hacking techniques.[3]

Previous research studies on the national cyber security strategy have indicated that the Indonesian government has made efforts to address the rising issue of cybercrime. These efforts involve a comprehensive strategy that encompasses five key aspects: legal, technical and procedural, organizational structure, capacity building, and international cooperation. However, it is worth noting that the implementation of this strategy has not fully met the anticipated outcomes, as highlighted by Setiadi.[4] Moreover, the successful execution of cyber security measures necessitates the harmonious collaboration of government entities, private sector engagement, and community participation.

Cyberspace presents multifaceted challenges, encompassing dangers, weaknesses, and concerns over security. This demonstrates that cybercrime can be classified as a type of transnational crime, characterized by its lack of geographical boundaries, absence of physical violence, absence of direct personal interaction, and anonymity of perpetrators. As per Smith's analysis, the aforementioned threats might emanate from various sources such as governmental bodies, organizations, individuals, or businesses, with or without deliberate intent, with the aim of achieving financial, military, political, or other objectives.[5][6]

Renewable energy projects in the United States were the initial recipients of the awareness of the potential risks posed by cyber assaults on critical infrastructure. sPower, a corporate entity specializing in the ownership and operation of solar and wind power plants, encountered a sequence of disruptions in the communication linkages connecting its central control center with its geographically dispersed power producing facilities. The brief and sporadic instances of system unavailability were purportedly attributed to a Distributed Denial of Service (DDoS) assault. In 2015/2016, a comparable incident occurred within the energy network of Ukraine, wherein hackers employed remote control of SCADA and substation technology. While the recent incident did not target renewable energy infrastructure, it instead focused on conventional energy systems. However, the attack successfully exploited flaws within a comparable system.[7]

---

[3] Miko Aditiya Suharto and Maria Novita Apriyani, "Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional," *Risalah Hukum* 17 (2021): 98–107, https://doi.org/10.30872/risalah.v17i2.705.

[4] Ahmad Setiadi, "Pemanfaatan Medsos Untuk Efektifitas Komunikasi," *Jurnal AMIK BSI Karawang* 12, no. 15 (2020): 25–30.

[5] Hino Samuel Jose, "Politisasi Agenda Keamanan Siber Pada Era Industri 4.0 Di Forum Multilateral," *Populika* 9, no. 2 (2021): 70–85, https://doi.org/10.37631/populika.v9i2.390.

[6] Rasa Bruzgiene and Konstantinas Jurgilas, "Securing Remote Access to Information Systems of Critical Infrastructure Using Two-Factor Authentication," *Electronics (Switzerland)* 10, no. 15 (2021), https://doi.org/10.3390/electronics10151819.

[7] Juan Garay and Aggelos Kiayias, "SoK: A Consensus Taxonomy in the Blockchain Era," in *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12006 LNCS, 2020, https://doi.org/10.1007/978-3-030-40186-3_13.

The economic growth of Indonesia is significantly impacted by the expansion of the e-commerce sector. An increasing number of dealers are assuming the role of producers and engaging in the online advertising of commercial products in this context. The proliferation of e-commerce producers has led to a corresponding expansion in the availability of e-commerce goods and services.[8] Consequently, he proceeded with the further development of the firm he had established. The rise of regional economic added value, as measured by GDP, is influenced by the increase in e-commerce intensity. This is due to the direct relationship between economic activity intensity and the economic added value of the regional economy. According to Galindo et al. (2009), the study examines the impact of the number of internet users on the economic growth of Indonesia. The aforementioned figures indicate a positive correlation between the quantity of Internet users in Indonesia and the country's economic expansion. According to the findings of the regression analysis, the coefficient estimate for the variable representing internet users is 105794.0. This implies that for every 1% rise in the number of internet users, there is an associated increase of 105794.0 in the outcome variable.[9]

The internet is expected to foster a substantial increase in economic growth, estimated at 2500.0%. This observation aligns with the empirical study conducted by Aula and Nur (2019) titled "The Influence of E-commerce on Indonesia's Gross Domestic Product (GDP)".[10] The study reveals that the quantity of individuals who have been utilizing the internet for an extended period of time has both a substantial positive and bad effect on Indonesia's overall revenue.

Users of online media who lack awareness of safety often exhibit a careless attitude when it comes to uploading sensitive information, including official documents and defense assets. The disclosure of this information has resulted in the dissemination of classified government information to the general public. It is imperative to rectify this prevailing mindset and establish governmental restrictions and policies to prevent indiscriminate placement of secret and strategically significant papers and information on the internet. In relation to the potential risk posed by cyber warfare, a policy has been established which mandates that computers employed for operational and classified purposes must remain disconnected from the internet.[11]

Hence, it is imperative to devise strategies to safeguard critical national assets, such as New Renewable Energy (EBT), by first recognizing the escalating risk posed by cyberattacks, promptly addressing them, and implementing policies that foster future cyber security. This study aims to elucidate the imperative nature of

---

[8] Luh Anastasia et al., "ANALISIS EKONOMI TERHADAP HUKUM DALAM KEGAGALAN PERLINDUNGAN DATA PRIBADI PENGGUNA E-COMMERCE ECONOMIC ANALYSIS OF LAW IN FAILURE TO PERSONAL DATA PROTECTION OF E-COMMERCE USERS I Dewa Gede Dana Sugama," *Jurnal IUS Kajian Hukum Dan Keadilan* 9, no. 3 (2021), http://jurnalius.ac.id/ojs/index.php/jurnalIUSDOI:http://dx.doi.org/10.29303/ius.v9i3.978.

[9] Budi. Mudrikah, Azizah, Aulia Hubara, Zsasa Dharma, "Pengaruh Nilai Transaksi E-Commerce Terhadap Pertumbuhan Ekonomi Di Indonesia Tahun 2017-2021," *Jurnal Publikasi Sistem Informasi Dan Manajemen Bisnis (JUPSIM)* 1, no. 3 (2022): 260–66.

[10] K D Pratiwi, "E-Commerce and Economic Growth in Indonesia: Analysis of Panel Data Regression," Jurnal *Manajemen Dan Kebijakan* 7 (2022): 171–86, https://ejournal.undip.ac.id/index.php/gp/article/view/44116%0Ahttps://ejournal.undip.ac.id/index.php/gp/article/download/44116/21211.

[11] Ni Putu Suci Meinarni and Happy Budyana Sari, "Analisis Potensi Kejahatan Di Dalam Dunia Maya Terkait Data," *Kertha Wicaksana* 14, no. April 2019 (2020): 9–15, https://doi.org/https://doi.org/10.22225/kw.14.1.1530.9-15.

cyber security for renewable energy assets, highlighting its role in detecting cybercrimes and identifying infrastructure vulnerabilities that manifest during crises. Until recently, the susceptibility of vital national objects to cyber threats has been a concern. This has prompted the exploration of potential dangers and threats that could compromise the security of these objects. In response, the concept of an ideal defense posture has been proposed as a solution to counter asymmetric threats, specifically cyber technology attacks, targeting vital national objects in the field of new and renewable energy.

METHODS

The present composition was crafted through the utilization of qualitative research methodologies, incorporating mixed approaches and extensive library study.[12] The research methodology employed in this study is a qualitative technique, specifically utilizing a literature review conducted in a library setting. The library research methodology involves gathering a diverse range of pertinent reading materials related to the research problem, followed by a thorough and meticulous examination of these sources to derive meaningful research outcomes. Data gathering strategies employ several sources of information that can be verified, and the reliability of the information can be assessed.[13]

The concept of hypothesis-driven threat defense. One commonly accepted interpretation of a hypothesis can be defined as an initial supposition or proposed explanation that is created based on minimal facts, serving as a foundation for subsequent inquiry. The important phrase in this context pertains to the scarcity of proof available for cybersecurity professionals. Threat detection technologies offer restricted evidential support as they may identify certain indicators of compromise (IoCs), yet fail to deliver a comprehensive evaluation of the extent or sophistication of the compromise. There is a possibility that they may not be able to perceive the presence of the threat.

The integration of these assumptions into a unified framework, known as hypothesis-driven threat defense, serves as the foundation for a risk management program. Threat assessment, threat simulation, and hypothesis-driven threat hunting constitute the fundamental components of hypothesis-driven security and form a trinity essential for effective threat mitigation. In order to thrive in a period characterized by swiftly developing dangers and emerging technologies, which therefore lead to a dearth of actionable evidence and a lack of certainty, the act of hypothesizing is the most comparable approach to making predictions.[14]

---

[12] Soerjono Soekanto, *Faktor-Faktor Yang Mempengaruhi Penegakan Hukum* (Jakarta: PT Rajawali Pers, 2015).

[13] Agung Sutriyawan, Universitas Bhakti Kencana, and Agung Sutriyawan, "Studi Mixed Method : Gambaran Epidemiologi Dan Analisis Sistem Surveilans Demam Berdarah Dengue (DBD) Di Kota Bandung Dinas Kesehatan Kota Bandung Dan" 8, no. 2 (2021): 15–29.

[14] Shinta Nurul, Shynta Anggrainy, and Siska Aprelyani, "Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi : Keamanan Informasi , Teknologi Informasi Dan Network (Literature Review Sim)," *Jurnal Ekonomi Manajemen Sistem Informasi (Jemsi)* Vol. 3, no. No. 5 (2022): 564–73.

RESULT AND DISCUSSION

Cybercrime and Infrastructure Vulnerabilities

1) Cyber Crime

Cybercrime or cybercrime is a crime involving computers and networks. Computer technology can be misused to commit crimes or become the target of crime. Cybercrime can endanger a person's security and finances. Some examples of cybercrime are online auction fraud, check forgery, credit card fraud, confidence fraud, identity fraud, child pornography, and so on. In this era of continuously developing technology, you have to be extra careful about cybercrime.

There are many privacy issues surrounding cybercrime when confidential information is stolen or disclosed lawfully or otherwise. Internationally, both government and non-government actors are involved in cybercrime, including espionage, financial theft, and other cross-border crimes. Cybercrime that crosses international borders and involves the actions of at least one nation state is sometimes referred to as cyberwar. Warren Buffett describes cybercrime as "humanity's number one problem" and "poses a real risk to humanity." Cybercrime based on its motives can be divided into several things as follows.[15][16]

a. Cybercrime as a pure crime can be interpreted as where a person commits a crime intentionally and premeditatedly to carry out damage, theft, anarchic acts against an information system or computer system.
b. Cybercrime as a gray crime can mean that this crime is not clear whether it is a criminal crime or not because it commits a burglary but does not damage, steal, or commit anarchic acts against the information system or computer system.
c. Cybercrime that attacks individuals is a crime committed by other people with the motive of revenge or for fun which aims to damage a good name, try or play with someone to gain personal satisfaction such as pornography, cyberstalking, etc.
d. Cybercrime which attacks property rights, namely crimes committed against someone's work with the motive of duplicating, marketing, changing for the purpose of personal/public interests or for material/non-material purposes.
e. Cybercrime which attacks the government in the form of crimes committed with the government as the object with the motive of committing terror, hijacking, or destroying the security of a government with the aim of disrupting the government system, or destroying a country.

To tackle increasingly widespread computer crime or cybercrime, awareness is needed from each country regarding the dangers of internet misuse.

2) Infrastructure Vulnerabilities

The utilization of Information and Communication Technology (ICT), encompassing the internet network that was initially established under the auspices of the United States Department of Defense as a strategic

[15] I. D. K. K. Marufah, N., Rahmat, H. K., & Widana, "Degradasi Moral Sebagai Dampak Kejahatan Siber Pada Generasi Millenial Di Indonesia.," *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial* 7, no. 1 (2020): 191–201.

[16] Hardianto Djanggih, "KEBIJAKAN HUKUM PIDANA DALAM PENANGGULANGAN TINDAK PIDANA CYBER CRIME DI BIDANG KESUSILAAN" I, no. 2 (2013).

medium for communication and data interchange, has progressively permeated various facets of contemporary human existence. It has emerged as an integral component of social, economic, and governmental domains on a global scale. The aforementioned phenomenon is also observed in Indonesia, a country with a current population of over 250 million individuals. Indonesia has experienced a significant increase in internet users, characterized by a rapid growth rate.

Critical infrastructure refers to the essential systems, networks, and assets that are vital for the functioning of a society, economy, or nation the susceptibility of cybersecurity to assaults is frequently heightened in comparison to other domains due to the prevalent utilization of outdated software in SCADA (Supervisory Control and Data Acquisition) systems. The NIS Regulations (Networks and Information Systems Regulations 2018) impose obligations on operators of critical services within the energy, transport, health, water, and digital infrastructure sectors in the United Kingdom, as well as digital service providers. In addition to various other stipulations, it is imperative for national policy to incorporate technical security measures aimed at safeguarding critical national assets, governmental bodies, ministries, and establishments, with the primary objective of effectively managing the security of their data.[17]

Case Study of Cyber Attacks on Energy

The transition to more environmentally sustainable energy sources has the potential to give rise to several challenges. The focus lies not on the costliness of technology or the magnitude of power generated, but rather on the realm of cyber security. The increasing significance of the renewable energy sector is evident as nations strive to transition away from fossil fuels. However, it is crucial to acknowledge the imperative of integrating cybersecurity measures into the sector's continued expansion. Concerns have been raised regarding potential vulnerabilities in various components, ranging from power plants to smart meters, which could potentially result in their compromise or destruction. The act of manipulation is anticipated to result in significant disruption to the grid or microgrid infrastructure of Renewable Energy.[18]

The vulnerability of cyber security in the field of Renewable Energy (EBT) extends to a wide range of systems, including industrial systems and Internet of Things (IoT) metering systems.

Presently, the energy sector has emerged as a primary focal point for cyber attackers, including individuals seeking to engage in espionage through the utilization of ransomware. There have been instances were attacks have been carried out with the intention of deliberately undermining the system in order to disrupt the supply of electricity. The vulnerabilities of renewable energy technology arising from the potential risk of cyberattacks are delineated as follows:

1) The enhancement of cybersecurity during the design phase is not given significant emphasis in the majority of contemporary renewable energy sectors.

---

[17] Sahat Parulian, Devi Anassalifa Pratiwi, and Meiliya Cahya Yustina, "Ancaman Dan Solusi Serangan Siber Di Indonesia," *Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT)* 1, no. 2 (2021): 85–92, http://ejournal.upi.edu/index.php/TELNECT/.

[18] Svetlana M. Mironova and Svetlana S. Simonova, "Protection of the Rights and Freedoms of Minors in the Digital Space," *Russian Journal of Criminology* 14, no. 2 (2020): 234–41, https://doi.org/10.17150/2500-4255.2020.14(2).234-241.

2) The prevailing trend within the renewable energy sector is to employ cost-effective, readily available SCADA systems and CCTV systems of lower grade.
3) The selection of key components is conducted without due consideration for Cybersecurity.
4) In the renewable energy sector, there is currently a lack of established norms or regulations pertaining to the adherence of cyber security measures.
5) In the renewable energy business, it is observed that buyers and technical advisors often overlook the aspect of cybersecurity throughout the entire process, starting from transactional activities to installation, completion, and acceptance stages.
6) One of the primary challenges confronting the renewable energy industry is to the potential cyber security vulnerabilities inside its supply chain.

Renewable energy providers should adopt a more cautious strategy when managing their supply chain. Renewable energy operators are required to engage in extensive inquiry with suppliers and other stakeholders within the renewable energy industry. Regular maintenance should be conducted as needed. There is a growing trend among energy providers worldwide to promote the adoption of smart meters and other sensor technologies among their customers. Nevertheless, smart meters and other Internet of Things (IoT) devices are susceptible to cyber threats. The promise of IoT lies in its capacity to establish pathways into networks and facilitate the construction of botnets, which can be exploited by hackers.[19]

According to the annual report of CyberRes, a business line of Micro Focus, it is advised that Indonesia exercise caution in relation to cyberattacks that specifically target the energy industry. For a minimum duration of 12 months. According to this yearly assessment, the energy industry in Indonesia is identified as being among the industries with a high degree of vulnerability. The primary focus of attacks in 2021 has been directed at Indonesia's energy sector.

Additionally, it was indicated that the sub-sectors that experienced the greatest impact were oil and gas, nuclear energy, pipelines, and natural gas. The majority of the attacks were perpetrated by many threat actor groups, namely Energetic Bear, APT28, APT10, Lazarus, APT34, Maze, Fin7, FIN8, and MuddyWater.

Nevertheless, as per his perspective, the Southeast Asian region retains a substantial potential to rectify the prevailing circumstances, owing to its adept comprehension of the present environment, adept utilization of strategies, and anticipation of potential threats. The nations situated in Southeast Asia continue to experience the repercussions of cyberattacks that occurred in the previous year, resulting in enduring consequences for both entities and persons within the region. Concurrently, this prevailing pattern is anticipated to persist until the year 2022. Currently, the prevailing practice in the field of energy sector cybersecurity is the implementation of system updates as a means of fortifying defenses against potential assaults. However, it is worth noting that a significant number of network energy providers rely on outdated methods.

The primary determinant contributing to the susceptibility of the sector to cyber security risks is the rising population of hackers and cybercriminals. In addition to this, the energy sector is susceptible to risks arising from geographical factors. The nation of Indonesia exhibits a notable degree of geographic complexity,

[19] Zhanna Pavlenko, "LAW IN DIGITAL REALITY," *The Bulletin of Yaroslav Mudryi National Law University. Series:Philosophy, Philosophies of Law, Political Science, Sociology* 2, no. 49 (May 26, 2021), https://doi.org/10.21564/2663-5704.49.229779.

resulting in a highly decentralized system of control. Frequently, a disparity arises between the management at the central level and that at the branch level. This is the factor that afterwards creates a vulnerability in security.

Case Study of Cyberattacks on Financial Systems

The proliferation of plastic card-based payment systems has had a significant impact on transactional convenience. These systems encompass a range of cards, such as credit cards, Automatic Teller Machine (ATM) cards, debit cards, prepaid cards, and similar variants. The following instances exemplify various cyberattacks, serving as instructive examples to prevent their recurrence.

1) PT BFI Finance Indonesia Tbk (BFIN)[20]

   The latest case of cyberattack occurred on the finance company, PT BFI Finance Indonesia Tbk (BFIN). Management announced in its official statement on May 21 2023. "We hereby inform you that on May 21 2023 the company experienced a cyberattack," said BFI Finance Indonesia Corporate Secretary, Sudjono Until now there has been no indication of consumer data leakage and as a precautionary measure the company is carrying out a temporary switch off on several main systems which has caused disruption to customer service and company operational activities.

2) Bank Syariah Indonesia (BRIS)[21]

   Bank Syariah Indonesia (BRIS) had a cyber assault, resulting in the unavailability of ATM and mobile banking services from May 8, 2023. This prolonged disruption in financial services caused significant inconvenience to clients and raised concerns among them. The BSI service system has reportedly experienced a ransomware attack perpetrated by the Lockbit gang. The aforementioned information was disclosed on the gang's webpage, which was accessed through the dark web. The webpage said that the group successfully obtained 15 million client records, amounting to a total of 1.5 terabytes of data. Furthermore, the group issued a ransom demand of US$ 20 million. Consequent to the aforementioned attack, BSI underwent a reorganization of its board of directors and commissioners, which encompassed the Director of Information Technology and the Director of Risk Management.

3) Asuransi BRI Life[22]

   The BRI Life insurance firm was implicated in a hacking incident in July 2021, which led to the unauthorized disclosure of 2 million customer records, amounting to around 250 gigabytes of data. According to reports, the compromised data was allegedly traded on the internet for a sum of US$ 7,000. The data was presented in a structured PDF format, encompassing various personal documents such as KTPs (Indonesian identification cards), financial accounts, NPWPs (tax identification numbers), birth certificates, and medical records. BRI Bank has implemented stringent rules aimed at upholding the security of customer data and information. BRI Bank remains committed to allocating resources towards the

[20] CNBC Indonesia, "BFI Finance Diserang Hacker, Nasabah Takut Tagihan Menggunung," 25 May, 2023, https://www.cnbcindonesia.com/market/20230525151416-17-440614/bfi-finance-diserang-hacker-nasabah-takut-tagihan-menggunung.

[21] Info Bank News, "Belajar Dari Kasus Bank Syariah Indonesia (BSI)," 1 Agustus, 2023, https://infobanknews.com/belajar-dari-kasus-bank-syariah-indonesia-bsi/.

[22] Tempo, "Kebocoran Data Nasabah BRI Life Bukti Lemahnya Proteksi Dan Regulasi," 29 Juli, 2021, https://fokus.tempo.co/read/1488710/kebocoran-data-nasabah-bri-life-bukti-lemahnya-proteksi-dan-regulasi.

advancement of information security technologies, as well as enhancing the overall efficacy of its systems and networks. These efforts are undertaken with the primary objective of safeguarding client data and information, thereby ensuring their utmost protection. BRI Bank, as the foremost financial institution in Indonesia, faces a considerable vulnerability in terms of potential cyberattacks that could compromise the security of consumer data. The topic of discussion is security. Hence, the function of security management at BRI bank assumes significant importance in safeguarding and preserving client data against such risks.[23] The security management at BRI bank is obligated to consistently upgrade security technology and effectively maintain the accessibility of client data while fulfilling their responsibilities. In addition to this, it is imperative for security management to possess the capability to effectively execute suitable and prompt tactics when confronted with cyber security threats.[24]

4) BPJS Kesehatan Indonesia[25]

The website bpjs-kesehatan.go.id, operated by the Health Social Security Administering Agency (BPJS), was allegedly subjected to a hacking incident in May 2021. The aforementioned incident resulted in the compromise and subsequent sale of around 279 million records containing personal information of the Indonesian populace on the Raid Forums online platform. The responsible party behind this act operated under the pseudonym "Kotz". In order to mitigate the potential risks associated with the broadcast of personal data, the Ministry of Communication and Information Technology (Kominfo) has ultimately put out a proposition to cease access to links facilitating the download of such data, as well as implementing measures to ban Raids Forums.

There are various basic techniques for obtaining information using social engineering methods, there are three (2) most common ones, namely:

1) Phishing, phishing techniques are used by perpetrators to trick or manipulate bank account holders so that they provide data and information that can be used to access customers' banking accounts. Phishing is carried out to obtain confidential information such as passwords by posing as a trusted person or business in electronic communication. Channels used as email, instant messaging services (SMS), or the spread of fake links on the internet to direct victims to websites that have been designed to deceive.
2) Impersonation, namely an attempt by a fraudster to pretend to be someone else with the aim of obtaining confidential information.[26]

Universally, what is defined as computer crime or crime in the cyber world (cybercrime) is an attempt to penetrate another person's computer network without that person's knowledge with the aim of identifying things that are of a privacy nature that can cause changes to the computer. tried directly where the computer is located

---

[23] Jangirala Srinivas et al., "Managing Cybersecurity Risk in Government: An Implementation Model," *Computers and Security* 8, no. 1 (2018).

[24] Edy Soesanto et al., "Peranan Manajemen Sekuriti Dalam Mengamankan Dan Memecahkan Masalah PT SK Keris Indonesia," *Jurnal Manajemen Riset Inovasi* 1, no. 3 (2023): 46–57, https://doi.org/10.55606/mri.v1i3.1259.

[25] Detik News, "Polri Identifikasi Profil Pelaku Kebocoran Data BPJS Kesehatan Di Raid Forum," 15 Juni, 2021, https://news.detik.com/berita/d-5606800/polri-identifikasi-profil-pelaku-kebocoran-data-bjps-kesehatan-di-raid-forum.

[26] Febrian Kwarto and Madya Angsito, "Pengaruh Cyber Crime Terhadap Cyber Security Compliance Di Sektor Keuangan," *Jurnal Akuntansi Bisnis* 11, no. 2 (2018): 99–110, https://doi.org/10.30813/jab.v11i2.1382.

or tried remotely via an information communications network. Cybercrime takes quite a number of victims, especially from a financial perspective. Most victims can only regret what has happened. They hope to learn a lot from the experience, what must be tried now is to take precautions against possibilities that could be detrimental to us as IT actors can take the form of:[27]

a. Educate Users (share new insights about Cyber Crime and the internet).
b. Use of a Hacker's Perspective (using a hacker's point of view to secure your system)
c. Patch System (patching deficiencies and weaknesses in the system).
d. Rules (ensuring procedures and regulations that protect your system from parties who do not have authority) IDS (Intrusion Detection System) combined with IPS (Intrusion Prevention System).
e. Firewalls
f. Anti-virus application

CONCLUSION

A cyberattack, also known as a cyberattack, refers to an offensive tactic employed by nations, individuals, groups, or entities to target computer information systems, infrastructure, computer networks, and/or personal computer devices. These attacks involve the use of various malicious actions, typically originating from unidentified sources, with the intention of stealing, altering, or destroying a specific target by exploiting vulnerabilities in a system through hacking techniques. Cyberspace presents multifaceted challenges, encompassing dangers, weaknesses, and issues of vulnerability. This evidence substantiates the assertion that cybercrime constitutes a type of transnational criminal activity that transcends geographical boundaries, lacks physical aggression, avoids direct interpersonal interactions, and operates anonymously. As per Smith's analysis, the aforementioned threats might originate from various sources such as governmental bodies, organizations, individuals, or businesses, irrespective of their deliberate or inadvertent intentions, with the aim of achieving financial, military, political, or other objectives. The transportation and logistics sector is widely recognized as one of the largest and most lucrative industries on a global scale. This phenomenon is appealing to meticulously structured cybercriminal organizations driven by monetary incentives. Furthermore, the extensive use of this technology has resulted in fleet operators sharing a greater amount of data with their partners and vendors than in previous times.

[27] Ni Komang Novia Widiasari and Emmy Febriani Thalib, "The Impact of Information Technology Development on Cybercrime Rate in Indonesia," *Journal of Digital Law and Policy* 1, no. 2 (2022): 73–86, https://doi.org/10.58982/jdlp.v1i2.165.

REFERENCES

Anastasia, Luh, Trisna Dewi, Magister Kenotariatan, Ni Putu, and Suci Meinarni. "ANALISIS EKONOMI TERHADAP HUKUM DALAM KEGAGALAN PERLINDUNGAN DATA PRIBADI PENGGUNA E-COMMERCE ECONOMIC ANALYSIS OF LAW IN FAILURE TO PERSONAL DATA PROTECTION OF E-COMMERCE USERS I Dewa Gede Dana Sugama." *Jurnal IUS Kajian Hukum Dan Keadilan* 9, no. 3 (2021). http://jurnalius.ac.id/ojs/index.php/jurnalIUSDOI:http://dx.doi.org/10.29303/ius.v9i3.978.

Bruzgiene, Rasa, and Konstantinas Jurgilas. "Securing Remote Access to Information Systems of Critical Infrastructure Using Two-Factor Authentication." *Electronics (Switzerland)* 10, no. 15 (2021). https://doi.org/10.3390/electronics10151819.

BSSN. Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (2017). https://peraturan.bpk.go.id/Home/Details/72920/perpres-no-53-tahun-2017.

Detik News. "Polri Identifikasi Profil Pelaku Kebocoran Data BPJS Kesehatan Di Raid Forum." 15 Juni, 2021. https://news.detik.com/berita/d-5606800/polri-identifikasi-profil-pelaku-kebocoran-data-bjps-kesehatan-di-raid-forum.

Dharma, Budi. Mudrikah, Azizah, Aulia Hubara, Zsasa. "Pengaruh Nilai Transaksi E-Commerce Terhadap Pertumbuhan Ekonomi Di Indonesia Tahun 2017-2021." *Jurnal Publikasi Sistem Informasi Dan Manajemen Bisnis (JUPSIM)* 1, no. 3 (2022): 260–66.

Djanggih, Hardianto. "KEBIJAKAN HUKUM PIDANA DALAM PENANGGULANGAN TINDAK PIDANA CYBER CRIME DI BIDANG KESUSILAAN" I, no. 2 (2013).

Edy Soesanto, Alifah Jiddal Masyruroh, Ganis Aliefiani Mulya Putri, and Srirahayu Putri Maharani. "Peranan Manajemen Sekuriti Dalam Mengamankan Dan Memecahkan Masalah PT SK Keris Indonesia." *Jurnal Manajemen Riset Inovasi* 1, no. 3 (2023): 46–57. https://doi.org/10.55606/mri.v1i3.1259.

Garay, Juan, and Aggelos Kiayias. "SoK: A Consensus Taxonomy in the Blockchain Era." In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Vol. 12006 LNCS, 2020. https://doi.org/10.1007/978-3-030-40186-3_13.

Indonesia, CNBC. "BFI Finance Diserang Hacker, Nasabah Takut Tagihan Menggunung." 25 May, 2023. https://www.cnbcindonesia.com/market/20230525151416-17-440614/bfi-finance-diserang-hacker-nasabah-takut-tagihan-menggunung.

Jose, Hino Samuel. "Politisasi Agenda Keamanan Siber Pada Era Industri 4.0 Di Forum Multilateral." *Populika* 9, no. 2 (2021): 70–85. https://doi.org/10.37631/populika.v9i2.390.

Kwarto, Febrian, and Madya Angsito. "Pengaruh Cyber Crime Terhadap Cyber Security Compliance Di Sektor Keuangan." *Jurnal Akuntansi Bisnis* 11, no. 2 (2018): 99–110. https://doi.org/10.30813/jab.v11i2.1382.

Marufah, N., Rahmat, H. K., & Widana, I. D. K. K. "Degradasi Moral Sebagai Dampak Kejahatan Siber Pada Generasi Millenial Di Indonesia." *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial* 7, no. 1 (2020): 191–201.

Mironova, Svetlana M., and Svetlana S. Simonova. "Protection of the Rights and Freedoms of Minors in the

Digital Space." *Russian Journal of Criminology* 14, no. 2 (2020): 234–41. https://doi.org/10.17150/2500-4255.2020.14(2).234-241.

News, Info Bank. "Belajar Dari Kasus Bank Syariah Indonesia (BSI)." 1 Agustus, 2023. https://infobanknews.com/belajar-dari-kasus-bank-syariah-indonesia-bsi/.

Nurul, Shinta, Shynta Anggrainy, and Siska Aprelyani. "Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi : Keamanan Informasi , Teknologi Informasi Dan Network (Literature Review Sim)." *Jurnal Ekonomi Manajemen Sistem Informasi (Jemsi)* Vol. 3, no. No. 5 (2022): 564–73.

Parulian, Sahat, Devi Anassalifa Pratiwi, and Meiliya Cahya Yustina. "Ancaman Dan Solusi Serangan Siber Di Indonesia." *Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT)* 1, no. 2 (2021): 85–92. http://ejournal.upi.edu/index.php/TELNECT/.

Pavlenko, Zhanna. "LAW IN DIGITAL REALITY." *The Bulletin of Yaroslav Mudryi National Law University. Series:Philosophy, Philosophies of Law, Political Science, Sociology* 2, no. 49 (May 26, 2021). https://doi.org/10.21564/2663-5704.49.229779.

Pratiwi, K D. "E-Commerce and Economic Growth in Indonesia: Analysis of Panel Data Regression." *Jurnal Manajemen Dan Kebijakan* 7 (2022): 171–86. https://ejournal.undip.ac.id/index.php/gp/article/view/44116%0Ahttps://ejournal.undip.ac.id/index.php/gp/article/download/44116/21211.

Setiadi, Ahmad. "Pemanfaatan Medsos Untuk Efektifitas Komunikasi." *Jurnal AMIK BSI Karawang* 12, no. 15 (2020): 25–30.

Soekanto, Soerjono. *Faktor-Faktor Yang Mempengaruhi Penegakan Hukum*. Jakarta: PT Rajawali Pers, 2015.

Soewoeh, C. A. J., Tenda, E., Ketaren, E., & Kalengkongan, W. W. "ANALISA KERENTANAN WEBSITE FMIPA UNSRAT BERDASARKAN OPEN WEB APPLICATION SECURITY PROJECT TOP 10 FRAMEWORK." *Journal of Engineering, Computer Science and Information Technology*, 2022.

Srinivas, Jangirala, Ashok Kumar Das, Neeraj Kumar, Hans de Bruijn, Marijn Janssen, Rafał Leszczyna, Agnė Brilingaitė, et al. "Managing Cybersecurity Risk in Government: An Implementation Model." *Computers and Security* 8, no. 1 (2018).

Suci Meinarni, Ni Putu, and Happy Budyana Sari. "Analisis Potensi Kejahatan Di Dalam Dunia Maya Terkait Data." *Kertha Wicaksana* 14, no. April 2019 (2020): 9–15. https://doi.org/https://doi.org/10.22225/kw.14.1.1530.9-15.

Suharto, Miko Aditiya, and Maria Novita Apriyani. "Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional." *Risalah Hukum* 17 (2021): 98–107. https://doi.org/10.30872/risalah.v17i2.705.

Sutriyawan, Agung, Universitas Bhakti Kencana, and Agung Sutriyawan. "Studi Mixed Method : Gambaran Epidemiologi Dan Analisis Sistem Surveilans Demam Berdarah Dengue (DBD) Di Kota Bandung Dinas Kesehatan Kota Bandung Dan" 8, no. 2 (2021): 15–29.

Tempo. "Kebocoran Data Nasabah BRI Life Bukti Lemahnya Proteksi Dan Regulasi." 29 Juli, 2021. https://fokus.tempo.co/read/1488710/kebocoran-data-nasabah-bri-life-bukti-lemahnya-proteksi-dan-regulasi.

Widiasari, Ni Komang Novia, and Emmy Febriani Thalib. "The Impact of Information Technology

Development on Cybercrime Rate in Indonesia." *Journal of Digital Law and Policy* 1, no. 2 (2022): 73–86. https://doi.org/10.58982/jdlp.v1i2.165.