 p-ISSN: 2548-9267 | e-ISSN : 2549-2365, Open Access at : *http://unramlawreview.unram.ac.id/index.php/ulrev*

Cyber Insurance as a Risk Mitigation Tool and Company Compliance Instrument with Indonesia's Personal Data Protection Law

Farras Achmad Joenaedi
Universitas Pembangunan Nasional Veteran Jakarta
2110611231@mahasiswa.upnvj.ac.id

Dwi Desi Yayi Tarina
Universitas Pembangunan Nasional Veteran Jakarta
dwidesiyayitarina@upnvj.ac.id

ABSTRACT

The rapid advancement of Information and Communication Technology (ICT) has revolutionized how individuals and businesses interact, but it has also increased the risk of data breaches, leading to serious financial and reputational consequences. In Indonesia, several high-profile data breach incidents, such as those involving Bank Syariah Indonesia (2023), BPJS Kesehatan (2021), and Tokopedia (2020), have exposed sensitive personal information, highlighting the need for stronger data protection mechanisms. The Indonesian government has responded by enacting the Law Number 27 of 2022 on Personal Data Protection (UU PDP) to safeguard citizens' data and ensure accountability for violations. However, many companies struggle to comply with these regulations due to inadequate data security measures. This paper aims to examine the role of cyber insurance as an effective risk mitigation tool to help businesses manage financial losses from data breaches and comply with the UU PDP. The research uses a normative legal approach, analyzing primary and secondary legal materials. It also adopts a comparative approach by exploring how California's AB 2320 mandates cyber insurance and assesses its applicability in Indonesia. The findings suggest that cyber insurance provides a safety net for businesses, covering costs related to legal liabilities, data recovery, and regulatory fines. Introducing mandatory cyber insurance in Indonesia similar to California's model could enhance corporate compliance with data protection laws while simultaneously reducing the financial burden of cyberattacks.

Keywords**: **Cyber Insurance, Personal Data Protections, and Risk Mitigation.

INTRODUCTION

The development of information and communication technology (ICT) over the past few decades has fundamentally transformed how people interact, work, and live. With the advent of the internet, smart devices, and digital applications, nearly every aspect of human life is now digitally interconnected.[1] This digital revolution has brought numerous benefits, including easier access to information, increased business efficiency, and innovations across various fields. ICT has advanced rapidly since the emergence of the internet in the late 20th century.[2] Sophisticated hardware and software, such as computers, smartphones, and cloud-based applications, have enabled people to access and share information quickly and efficiently. Social networks, mobile banking services, and e-commerce are just a few examples of how ICT has become integrated into our daily lives. However, as technology usage continues to grow, the

[1]Sulianta, F., 2020, Literasi digital, riset dan perkembangannya dalam perspektif social studies. Feri Sulianta, Jakarta, P. 20.

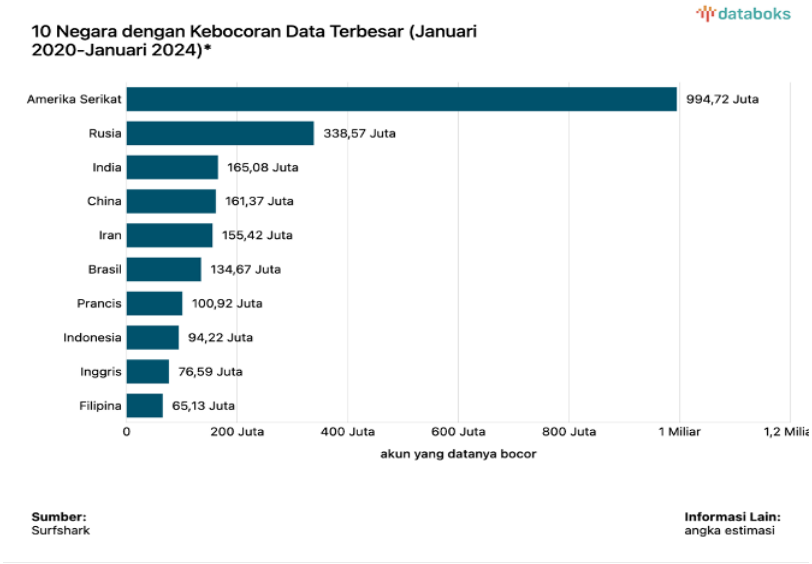
[2]Tanjung, F., Dania, A. P., Saputri, A. D., Sumbayak, D., Ramadhani, N., Bangun, S. K. B., & Nainggolan, L. B, 2024, Pengaruh Keberadaan Amerika Di Akhir Abad Ke-20 Sampai Awal Abad Ke-21, Holistik Analisis Nexus, Vol 1 No. 6, https://doi.org/10.62504/zt1wra81

DOI: https://doi.org/10.29303/ulrev.v8i2.380

volume of data generated and stored has increased exponentially. This data encompasses not only general information but also sensitive personal details, such as names, addresses, phone numbers, financial records, and medical history. Frequently stored on servers connected to the internet, this personal information is susceptible to unauthorized access and data breaches.[3]

Personal data, as outlined in Article 1, paragraph (1) of Law No. 27 of 2022 on Personal Data Protection (PDP Law), refers to information about an individual that can be identified, either directly or indirectly, on its own or in conjunction with other data, through both electronic and non-electronic systems.[4] The right to personal data protection is guaranteed to Indonesian citizens under Article 28G, paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which ensures that every person is entitled to the protection of their personal identity, family, honor, dignity, and property, as well as the right to feel safe and free from threats when exercising or refraining from actions related to their fundamental rights.[5] The need for personal data security has become more pressing due to the increase in data breaches.

Chart 1. The Ten Countries with the Largest Data Breaches



Sources: Databoks Katadata.

According to a report by Surfshark, a Dutch virtual private network (VPN) company, approximately 3.96 billion digital accounts experienced data breaches globally between January 2020 and January 2024.[6] The United States recorded the highest number of data breaches, with an estimated 994.72 million compromised accounts, while Indonesia ranked eighth with 94.22 million breached accounts.[7] These data breaches often involve sensitive personal information, such as full names, gender, geographical locations, email addresses, account passwords, and phone numbers. Unauthorized access to such data can have severe consequences for both individuals and companies. Individuals may suffer from identity theft, fraud, and financial loss. For companies, data breaches can damage their reputation, erode customer trust, and result in significant financial losses.

[3]APA ITU Perlindungan Data?: Microsoft security. Apa itu Perlindungan Data? | Microsoft Security. (n.d.). https://www.microsoft.com/id-id/security/business/security-101/what-is-data-protection accessed on September 3, 2024.

[4]Article 1 of Law Number 27 of 2022 concerning Protection of Personal Data.

[5]Article 28G of The 1945 Constitution of the Republic of Indonesia.

[6]Indonesia masuk 10 Negara dengan kebocoran data terbesar: Databoks. Pusat Data Ekonomi dan Bisnis Indonesia. (2024, June 28). https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/cc5473708a4f8dc/indonesia-masuk-10-negara-dengan-kebocoran-data-terbesar accessed on September 3, 2024.

[7]*Ibid.*

Companies that handle millions of customer records are highly vulnerable to data breaches.[8] One notable case of a data breach in Indonesia involved Bank Syariah Indonesia (BSI) in May 2023. The attack was carried out by a ransomware group known as Lockbit 3.0, which successfully stole 1.5 TB of data, including 15 million customer and employee records.[9] This data encompassed sensitive personal information such as phone numbers, addresses, names, account balances, account numbers, and transaction histories. Additionally, the stolen data included financial documents, legal documents, Non-Disclosure Agreements (NDAs), and passwords for both internal and external access to BSI's systems.

Another significant data breach occurred at BPJS Kesehatan in May 2021. Personal data belonging to approximately 279 million Indonesian citizens, including deceased individuals, was allegedly hacked and sold on online forums.[10] The compromised data included sensitive information such as card numbers, policyholder names, taxpayer identification numbers (NPWP), birthdates, and phone numbers. In May 2020, Tokopedia, one of Indonesia's leading e-commerce platforms, suffered a significant data breach. The personal information of 91 million user accounts and 7 million merchant accounts was compromised and later sold on the dark web.[11] The leaked information included user IDs, email addresses, full names, birthdates, gender, phone numbers, and encrypted passwords.

The Indonesian government has taken steps to protect citizens' personal data by enacting the Personal Data Protection Law (UU PDP). One of the primary objectives of this law is to safeguard personal data from various threats, such as unauthorized access, misuse, and data breaches.[12] Article 12, paragraph (1) of the UU PDP grants individuals the right to file lawsuits and receive compensation for violations in the processing of their personal data, in accordance with legal regulations.[13] This provision underscores that individuals whose data has been misused or leaked can take legal action against the companies responsible for such breaches.

Article 57 paragraph (2) of the UU PDP stipulates that violations of the law may result in administrative fines.[14] If a company is required to pay compensation to affected individuals and is also subjected to administrative fines, its financial situation may be severely impacted. The costs incurred would not only include direct compensation but also operational expenses related to enhancing security systems, legal fees, and potential revenue losses due to reputation damage. These financial burdens can significantly strain the company and threaten its business continuity. Therefore, effective risk mitigation measures are necessary to anticipate and manage potential losses arising from data breaches.

One of the insurable objects, as stated in Article 1 of Law No. 40 of 2014 on Insurance, is legal liability.[15] This legal liability encompasses the obligation of companies or individuals to provide compensation for losses arising from their activities that impact third parties. In the digital realm, this legal liability has become increasingly relevant due to the growing incidence

[8]Husna, A. H. (2024). Corporate Communication Literacy in Protecting Consumer's Privacy Data. JURNAL SIMBOLIKA Research and Learning in Communication Study, Vol. 10 No. 1, doi.org/10.31289/simbolika.v10i1.10763

[9]Asmaaysi, A. (2023, May 14). Kronologi Nasabah BSI Kehilangan Tabungan RP378,25 Juta Hingga konfirmasi bris. Bisnis.com. https://finansial.bisnis.com/read/20230514/90/1655744/kronologi-nasabah-bsi-kehilangan-tabungan-rp37825-juta-hingga-konfirmasi-bris accessed on September 3, 2024.

[10]Sari, N. P. (n.d.). Data BPJS Kesehatan Diduga Bocor, menteri Tjahjo Dukung kemkominfo usut tuntas. Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi. https://www.menpan.go.id/site/berita-terkini/data-bpjs-kesehatan-diduga-bocor-menteri-tjahjo-dukung-kemkominfo-usut-tuntas accessed on September 3, 2024.

[11]Kronologi Lengkap 91 Juta Akun Tokopedia Bocor Dan Dijual. teknologi. (2020, May 3). https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual accessed on September 3, 2024.

[12]Yudistira, M., & Ramadani, R. (2023). Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 oleh KOMINFO. UNES Law Review, Vol. 5, No. 4, https://doi.org/10.31933/unesrev.v5i4.698

[13]Article 12 of Law Number 27 of 2022 concerning Protection of Personal Data.

[14]*Ibid.*

[15]Article 1 of Law Number 40 of 2014 concerning Insurance.

of personal data breaches. Companies that store or manage customers' personal data may be held legally accountable in the event of a data breach.[16]

Cyber insurance is a form of protection designed to safeguard companies against risks related to cyberattacks and data breaches.[17] This type of insurance serves as a safety net for businesses facing increasingly complex digital threats, such as hacking, ransomware, and the theft of users' personal data. A cyber insurance policy covers various aspects, including the costs of incident investigation, data recovery, regulatory fines, and compensation to third parties harmed by data breaches.[18] In dealing with these unpredictable situations, cyber insurance helps companies mitigate the financial impact of data breaches, which can potentially reach billions of rupiah. This makes cyber insurance an effective risk mitigation tool, as the costs associated with managing cyber incidents can quickly deplete a company's budget.[19]

The role of cyber insurance in risk mitigation is increasingly recognized globally, as evidenced by regulations like California's AB 2320, which mandates companies to have cyber insurance to reduce the financial burden on the public caused by cyberattacks.[20] This bill encourages businesses to be more cautious in managing personal data and ensures they have adequate protection in the event of a data breach. In Indonesia, with the implementation of the Personal Data Protection Law (UU PDP), companies face similar challenges. They must ensure compliance with stringent data protection standards to avoid potential severe penalties, which may include substantial financial fines. Many companies struggle to meet these requirements, particularly in areas related to personal data governance and weak security systems.

Previous studies on cyber insurance have highlighted its role in managing cyber risks and assisting companies in complying with privacy regulations. Talesh found that cyber insurance functions as an external compliance manager,[21] while Tsohou et al. (2023) analyzed the challenges and trends in the implementation of cyber insurance. Trang (2017) proposed mandatory cyber-liability insurance to enhance data security standards. However, there is a gap in research specifically examining the legal context of Indonesia, particularly concerning compliance with Law No. 27 of 2022 on Personal Data Protection (UU PDP) through cyber insurance. This study aims to fill that gap by focusing on the role of cyber insurance in risk mitigation and compliance with the UU PDP in Indonesia.

Cyber insurance not only helps mitigate the effects of risks but also assists companies in adhering to the requirements of the Personal Data Protection Law (UU PDP). It offers legal and financial protection in the event of a data breach, helping to reduce the likelihood of sanctions and financial losses.[22] Therefore, there is a strong urgency to make cyber insurance a mandatory requirement for businesses vulnerable to data breaches in Indonesia, similar to the model implemented in California. With such a mandate, companies would be more motivated to enhance their security protocols and ensure full compliance with applicable regulations, thus protecting not only their businesses but also the interests of consumers and the public at large.

---

[16]Muhammad D., 2023, *Pertanggungjawaban Hukum PT Tokopedia Terhadap Kebocoran Data Pribadi*, Doctoral dissertation, Institut Agama Islam Negeri (IAIN) Polopo, Sulawesi Selatan, P.. 58

[17]Talesh, S. A., 2018, Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers" for businesses. Law & Social Inquiry, Vol. 43 No. 2, https://doi.org/10.1111/lsi.12303

[18]Heath, B. (2018). Before the Breach: The Role of Cyber Insurance Incentivizing Data Security. Geo. Wash. L. Rev., Vol. 86 No. 4.

[19]Coburn, A., Leverett, E., & Woo, G., 2018, Solving cyber risk: protecting your company and society. John Wiley & Sons. P.. 47.

[20]Assembly Privacy and Consumer Protection Committee, 2020, Personal information: contractors: cyber insurance, California, P. 1.

[21]Talesh, S. A. (2018). Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers" for businesses. Law & Social Inquiry, 43(2), 417-440. https://doi.org/10.1111/lsi.12303.

[22]Gavėnaitė-Sirvydienė, J., 2019, Evaluation of cyber insurance as a risk management tool providing cyber-security. In Social transformations in contemporary society (STICS 2019): proceedings of an annual international conference for young researchers. Vilnius: Mykolas Romeris university, No. 7.

METHOD

The research conducted in this study is classified as normative legal research. This type of research involves the systematic inventory and analysis of legal documents, which primarily relies on secondary data such as laws, court decisions, legal theories, and scholarly opinions related to the subject matter being studied. The focus of this research is on understanding and interpreting the relevant legal frameworks, norms, and regulations that govern the issue at hand. The approach adopted in this research includes a statute approach, which involves analyzing the structure of norms within legal regulations, with a focus on the hierarchy and the relationship between general and specific rules within the legal framework. Additionally, the research employs a conceptual approach, aiming to develop theoretical concepts regarding the role of cyber insurance as a risk mitigation tool and its compliance with personal data protection laws. The study also stresses the importance of making cyber insurance a mandatory requirement for companies that handle personal data. Furthermore, a comparative approach is utilized to evaluate the implementation of cyber insurance in other countries, such as California, which has proposed AB 2320 as a foundation for mandatory cyber insurance, and explores how such an approach could be applied in Indonesia.

The data sources for this research comprise secondary data, which are divided into two main categories of legal materials: primary legal materials and secondary legal materials. Primary legal materials comprise relevant laws and regulations that directly pertain to the research topic, such as Law No. 27 of 2022 on Personal Data Protection and Law No. 40 of 2014 on Insurance. Secondary legal materials offer explanations and interpretations of primary legal materials and include research findings, scholarly works, textbooks, scientific journals, and draft laws. In addition, tertiary legal materials, such as dictionaries and encyclopedias, are used to provide guidance and clarification on the primary and secondary legal materials. The data collection technique employed in this research is library research, which involves a thorough review of books, literature, notes, and reports that are relevant to the research problem. This method allows for a comprehensive exploration of the existing legal and theoretical materials related to the subject. For data analysis, the study adopts a descriptive-analytical method, aiming to present and interpret the data in a clear and systematic manner, providing a detailed understanding of the legal issues discussed in the research.

ANALYSIS AND DISCUSSION

A. The Losses Suffered by Companies Due to Data Breaches under Indonesia's Personal Data Protection Law

Data breaches are one of the primary issues faced by companies in Indonesia as digital technology rapidly evolves. In recent years, Indonesia has encountered a number of data breach incidents involving various sectors, including e-commerce, fintech, and government institutions. Such incidents not only have serious implications for individual privacy but also threaten public trust in the ability of companies and institutions to protect personal data. Data breaches in Indonesia can occur due to several factors. Technical factors, such as weaknesses in a company's cybersecurity systems, often serve as the primary cause of data breaches. Many companies in Indonesia still rely on outdated technology or lack adequate security systems to face the ever-evolving cyber threats.[23] Additionally, human factors, such as negligence or

[23]Yudistira, M., & Ramadani, R. (2023). Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 oleh KOMINFO. UNES Law Review, 5(4), 3917-3929. https://doi.org/10.31933/unesrev.v5i4.698

errors in handling sensitive data, also contribute significantly to data breach incidents. For example, lax internal practices in data management or insufficient employee training on data security can greatly increase the risk of breaches.[24]

The risk profile of data breaches in Indonesia is also influenced by the low level of compliance among companies with personal data protection regulations. Although Indonesia has enacted the Personal Data Protection Law (UU PDP), its implementation still faces various challenges, particularly for small and medium-sized enterprises (SMEs) that lack the infrastructure or resources to comply with the regulations.[25] As a result, these companies become more vulnerable to cyberattacks targeting user data. Furthermore, the increasing number of internet users and the proliferation of digital transactions also heighten the risk of data breaches, as more personal data is stored and processed by companies.

The enactment of Law No. 27 of 2022 on Personal Data Protection brings significant legal implications regarding data breaches, including breaches of customer data by companies that store millions of customer records. According to data, several large companies in Indonesia that collect millions of customer records operate in sectors such as telecommunications, e-commerce, banking, and technology. For example, telecom operator Telkomsel had over 160 million customers in 2023.[26] Additionally, e-commerce giants like Tokopedia and Shopee report millions of active users each month, with Tokopedia having around 40 million active users and Shopee exceeding 103 million active users in the same year.[27] Digital banks like Bank Jago and GoTo Financial also manage millions of customer records from various financial services they offer. This illustrates the immense potential impact of data breaches in Indonesia, especially with the implementation of the UU PDP, which requires companies to take greater responsibility in managing and protecting personal data.

Referring to Article 74 of the Personal Data Protection Law (UU PDP), companies acting as Data Controllers and Data Processors are required to align their personal data processing practices with the provisions of this law by October 17, 2024.[28] The two-year transition period, following the enactment of the law, provides companies with time to ensure compliance with these regulations. If companies fail to meet these obligations within the specified period, they will face strict legal sanctions after that date. The UU PDP contains regulations regarding personal data processing by data controllers, outlined in Articles 30 to 50. These provisions cover various aspects of data processing, including the fundamental principles of data collection, storage, and deletion. These articles require companies to implement cautionary measures and protection for the personal data they manage. Non-compliance with these rules can result in administrative sanctions, as stipulated in Article 57 of the UU PDP. The administrative sanctions include:[29]

a. Written warnings;
b. Temporary suspension of personal data processing activities;
c. Deletion or destruction of personal data; and/or
d. Administrative fines.

[24]Radiansyah, A., Baroroh, N., Fatmah, F., Hulu, D., Syamil, A., Siswanto, A. & Nugroho, F. (2023). Manajemen Risiko Perusahaan: Teori & Studi Kasus. PT. Sonpedia Publishing Indonesia.

[25]Samosir, I. H. (2024). Perlindungan Hukum Terhadap Data Pribadi Dalam UU Nomor 27 Tahun 2022 dan Tantangan Implementasinya Dalam Era Teknologi Informasi, Tesis Universitas HKBP Nommensen, Sumatera Utara, P. 45.

[26]Telkomsel, operator Seluler Terbesar Dengan Layanan Digital terdepan. ekonomi. (2024, July 9). https://www.cnnindonesia.com/ekonomi/20240708153421-97-1118865/telkomsel-operator-seluler-terbesar-dengan-layanan-digital-terdepan accessed on September 21, 2024.

[27]Ginanjar, R. P. A. (2024, August 30). Jejak Persaingan Shopee Dengan Tokopedia, Siapa Penguasa Pasar e-commerce Ri Saat Ini?. Tempo. https://bisnis.tempo.co/read/1910326/jejak-persaingan-shopee-dengan-tokopedia-siapa-penguasa-pasar-e-commerce-ri-saat-ini accessed on September 21, 2024.

[28]Article 47 of Law Number 27 of 2022 concerning Protection of Personal Data.

[29]Article 57 of Law Number 27 of 2022 concerning Protection of Personal Data.

For administrative sanctions in the form of fines, these penalties can amount to up to 2% of a company's annual revenue or receipts, depending on the severity of the violation. [30] Beyond administrative penalties, the Personal Data Protection Law (UU PDP) also grants individuals (data subjects) the right to seek compensation in cases of personal data processing violations. Article 12 of the UU PDP clearly states that data subjects are entitled to file lawsuits and receive compensation for breaches related to their personal data. [31] This holds companies directly accountable, requiring them to compensate users affected by data breaches as part of their responsibility to protect personal information. In terms of enforcement, the Personal Data Protection Authority (Lembaga PDP) has the power to impose administrative sanctions on Data Controllers and/or Data Processors who violate the regulations. Under Article 60 letter c of the UU PDP, the Lembaga PDP is specifically authorized to enforce these sanctions in response to such violations. [32]

The legal theory of responsibility, as proposed by Austrian legal scholar Hans Kelsen, states that an individual is legally accountable for a specific act or holds legal responsibility when they are subject to sanctions for actions that violate legal norms.[33] Kelsen emphasizes that legal responsibility arises when there is a breach of a legal norm, and in this case, data breaches constitute a violation of the norms outlined in the Personal Data Protection Law (UU PDP). According to Kelsen, legal responsibility is rooted in the obligation to comply with legal norms, and when these norms are violated, the perpetrator—in this case, the company—must face appropriate legal sanctions. In the context of data breaches, these sanctions can take the form of administrative penalties, as regulated in Article 57 of the UU PDP, and compensation to the data subject in accordance with Article 12 of the UU PDP.

The application of Hans Kelsen's theory to data breaches demonstrates that a company's responsibility extends beyond merely preventing data leaks; it also encompasses the obligation to compensate affected users. In this context, the company's responsibility operates on two levels: first, the company must comply with the legal norms set forth in the Personal Data Protection Law to avoid data breaches, and second, if a violation occurs, the company must bear the responsibility of providing fair compensation to the affected users. This reflects the core principle of Hans Kelsen's theory that legal responsibility is a direct consequence of violating legal norms, and such violations must be accompanied by remedies or sanctions to restore justice.[34]

According to the annual Global Digital Trust Insights survey conducted by PwC, one in four companies globally (27%) has experienced a data breach that cost them between US$1 million and US$20 million or more in the past three years.[35] In North America, this figure is even higher, with one in three companies (34%) reporting similar losses, while only 14% of companies globally reported that they had not experienced a data breach during this period.[36] These figures highlight the widespread impact of data breaches on companies worldwide. When a data breach occurs, the consequences can be highly damaging and vary depending

[30]Prasetyo, T., & Sinambela, J. S. (2023). Penerapan Sanksi Administrasi Dan Sanksi Pidana Terhadap Pencurian Data Pribadi Perspektif Teori Keadilan Bermartabat. Spektrum Hukum, 20(1), 58-69. http://dx.doi.org/10.56444/sh.v20i1.3663

[31]Article 12 of Law Number 27 of 2022 concerning Protection of Personal Data.

[32]Article 60 letter C of Law Number 27 of 2022 concerning Protection of Personal Data.

[33]Kelsen, H. (2005). General Theory of Law and State (1st ed.). Routledge. https://doi.org/10.4324/9780203790960

[34]*Ibid.*

[35]PricewaterhouseCoopers. (n.d.). One in four companies globally have suffered a data breach that cost them US$1 - 20 million or more in the past three years. PwC. https://www.pwc.com/id/en/media-centre/press-release/2022/english/one-in-four-companies-globally-have-suffered-a-data-breach-that-cost-them-usd-1-20-million-or-more-in-the-past-three-years.html accessed on October 25, 2024.

[36]*Ibid.*

on the type and scale of the breach. The following table categorizes the potential costs of data breach losses for companies, divided by timeframes: short-term, medium-term, and long-term.[37]

Table 1. Costs Incurred Due to Data Leaks for Companies.

	Short-term	**Medium-term**	**Long-term**
Direct Cost	• Consultant expenses • Cyber ransom and extortion damages • Financial fraud • Insurance excess • Overtime pay for staff • Costs for contracting external staff for response efforts	• Modifications in cybersecurity practices • Compensation or discounts • External complaints • Penalties • External investigations • Legal expenses • External PR and marketing efforts • Recruitment expenses • Third-party liability	• Credit rating and insurance premium changes • Cybersecurity enhancements • Loss of investment, donations, or funding • Long-term staff expenses • Training expenses • External training costs • Shareholder value
Indirect Cost	• Containment efforts • Loss of data and software • Theft of intellectual property • Disruption of staff's regular business activities (opportunity cost) • Damage to IT equipment • Notification expenses (authorities) • Notification expenses (customers) • Damage to physical equipment (excluding IT equipment) • Service disruption	• Complaints (internal) • Investigation (internal) • Post-breach customer protection • PR/marketing activities (internal)	• Loss of customers • Cybersecurity enhancements (opportunity cost) • Long-term productivity impact • Supply chain losses • Internal training expenses • Training costs (opportunity cost)

Sources: Furnell, S., Heyburn, H., Whitehead, A., & Shah, J. N. (2020).

The costs incurred due to a data breach can vary significantly, encompassing both direct and indirect aspects related to the incident. One of the most common costs is the change in cybersecurity practices, where companies may need to switch internet service providers or invest in new security products to enhance their protection.[38] Additionally, companies often have to provide compensation or discounts to affected customers, as well as handle an increase in complaints, both externally and internally, which may require allocating additional staff or third-party services. Consultancy fees can also arise, as companies frequently need to hire external consultants to respond to the incident.

In some cases, companies may be forced to pay a ransom or face extortion related to blocked services due to a cybersecurity breach. Additionally, costs related to cybersecurity system repairs, data recovery, and the loss of software, along with other financial losses from

[37]Furnell, S., Heyburn, H., Whitehead, A., & Shah, J. N. (2020). Understanding the full cost of cyber security breaches. Computer fraud & security, 2020(12), 6-12. https://doi.org/10.1016/S1361-3723(20)30127-5

[38]Silalahi, F. D. (2022). Keamanan Cyber (Cyber Security). Jakarta: Yayasan Prima Agus Teknik.

asset theft, are significant components of the potential costs. Companies may also face fines from regulators, as well as internal and external investigation costs to determine the source of the breach.[39] Furthermore, reputational damage caused by a data breach can lead to loss of investors, funding, and stock value, while the costs of repairing the brand image through PR and marketing campaigns further increase the financial burden.[40] All of this, coupled with long-term productivity losses due to heightened fears of future cybersecurity risks, makes the costs of a data breach one of the most financially and operationally damaging risks for companies.

Companies facing the risk of data breaches should consider cyber insurance as a mitigation strategy to protect themselves from potential significant losses. Cyber insurance offers financial protection against various costs that may arise from a data breach incident, such as recovery expenses, compensation to affected customers, and fines that may be imposed by regulators. By having cyber insurance, companies can minimize the financial impact of breaches and enhance their resilience against cyberattacks. This also allows companies to focus more on remediation efforts and strengthening their security systems without being burdened by financial uncertainty due to data breaches.

B. The Role of Cyber Insurance in Assisting Companies to Comply with the Indonesia's Personal Data Protection Law

Cyber insurance is designed to protect companies from financial losses due to cybersecurity incidents, such as data breaches, malware attacks, ransomware, or identity theft. A range of cyber insurance providers have emerged, offering various coverage options to meet the growing demand for protection amidst increasing cyber risks.

Table 2. General Coverage of Cyber Insurance.

Type of Protection	Description
Data Breach Liability	Covers legal costs and compensation arising from personal data breaches.
Network Security Liability	Covers claims caused by network security breaches, such as malware or ransomware attacks.
Business Interruption	Covers financial losses due to operational disruptions due to cyber incidents.
Incident Response Costs	Costs for rapid response such as forensic investigations, notification to affected parties, and public relations costs.
Regulatory Fines	Covers fines imposed by regulators for breaches of data protection laws.
Crisis Management	Costs for reputation restoration services and public relations due to the impact of cyber incidents.
Cyber Extortion (Ransomware)	Covers costs associated with ransomware threats or attacks, including ransom payments.
Legal Defense Costs	Covers legal costs in facing third-party lawsuits or class-action lawsuits related to cyber incidents.

[39]Priliasari, E. (2023). Perlindungan Data Pribadi Konsumen Dalam Transaksi E-Commerce. Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional, 12(2). P. 20 http://dx.doi.org/10.33331/rechtsvinding.v12i2.1285

[40]Dancor. (2023, June 24). Dampak Besar kebocoran data TERHADAP Reputasi Perusahaan. Hypernet. https://www.hypernet.co.id/id/2023/06/24/dampak-besar-kebocoran-data-terhadap-reputasi-perusahaan/ accessed on September 26 2024.

Data Recovery Costs	Covers the cost of restoring data damaged or lost due to cyber security incidents.
Multimedia Liability	Covers claims arising from copyright infringement or defamation in electronic media.

Cyber insurance offers a range of protections for companies facing risks associated with cyber incidents. Referring to Table 3, one of the primary types of coverage is Data Breach Liability, which covers legal fees and compensation arising from personal data breaches.[41] Additionally, Network Security Liability protects companies from claims caused by network security breaches, such as malware or ransomware attacks.[42] Cyber insurance also provides protection for Business Interruption, covering financial losses resulting from operational disruptions due to cyber incidents.[43] Costs for rapid response, such as forensic investigations and notifying affected parties, fall under Incident Response Costs.

Other protections offered by cyber insurance include Regulatory Fines, which cover fines imposed by regulators due to violations of data protection laws, and Crisis Management Costs for reputation recovery.[44] Additionally, the insurance addresses Cyber Extortion (Ransomware), covering costs related to ransomware threats, and Legal Defense Costs, which cover legal expenses when facing third-party lawsuits.[45] Lastly, Data Recovery Costs cover the recovery of lost or damaged data, while Multimedia Liability protects against copyright violations or defamation claims.[46] These protections help companies manage risks more effectively and ensure business continuity in the digital era. With the obligations set by the UU PDP regarding compensation to data subjects and administrative fines for non-compliance, cyber insurance can serve as a highly effective risk mitigation tool. A cyber insurance policy can cover compensation payments to data subjects affected by data breaches and cover administrative fines imposed by the authorities for violations of the UU PDP.

Until now, no region or country has made cyber insurance mandatory. However, in the United States, the state of California is currently proposing a bill that would make cyber insurance compulsory under specific conditions. AB 2320, introduced by Assemblymember Ed Chau of the West San Gabriel Valley on February 14, 2020, is a significant bill aimed at strengthening data privacy protection for California residents, particularly through a requirement for entities working with government agencies to have adequate cyber insurance.[47] This bill highlights the growing importance of cybersecurity in an increasingly digital landscape, where contractors working with the government often have access to sensitive personal information. With the rising risk of cyberattacks, including data breaches, cyber insurance has become a vital tool for mitigating risks and protecting businesses and data subjects from potential losses resulting from such violations.

One of the key elements of AB 2320 is the requirement that any entity involved in a contract with California government agencies or departments, which has access to records containing

[41]Talesh, S. A. (2018). Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers" for businesses. Law & Social Inquiry, 43(2), 417-440 .https://doi.org/10.1111/lsi.12303

[42]Teichmann, F. M. J., & Wittmann, C. (2023). When is a law firm liable for a data breach? An exploration into the legal liability of ransomware and cybersecurity. Journal of Financial Crime, 30(6), 1491-1498. https://doi.org/10.1108/JFC-04-2022-009

[43]Shevchenko, P. V., Jang, J., Malavasi, M., Peters, G. W., Sofronov, G., & Trück, S. (2023). The nature of losses from cyber-related events: risk categories and business sectors. Journal of Cybersecurity, 9(1), tyac016. https://doi.org/10.1093/cybsec/tyac016

[44]Talesh, S. A. (2018). Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers" for businesses. Law & Social Inquiry, 43(2), 417-440. .https://doi.org/10.1111/lsi.12303

[45]*Ibid.*

[46]*Ibid.*

[47]Assembly Privacy and Consumer Protection Committee, 2020, Personal information: contractors: cyber insurance, California, P. 1.

personal information, must maintain adequate cyber insurance to cover losses arising from legal violations or disclosure of personal information.[48] In this context, "personal information" is broadly defined, encompassing details such as an individual's name, social security number, home address, education history, medical conditions, and employment history. This bill not only focuses on personal data protection but also creates a greater financial responsibility for contractors working with the government. Previously, in the event of a data breach, the financial burden often fell on the government and, ultimately, taxpayers. With AB 2320, this burden will be shifted to the contractors who have access to sensitive information. This change will force businesses to take stronger cybersecurity measures, as the financial risk of a data breach will now directly affect them. Additionally, this creates an incentive for contractors to enhance their security infrastructure, as insurance companies are likely to offer lower premiums to businesses that are considered lower risk.

An example of a company successfully claiming cyber insurance in the event of a data breach can be observed in several major incidents, such as the one experienced by Target in 2013. The data breach at Target exposed over 40 million credit card numbers and personal customer information.[49] In this case, Target held a cyber insurance policy worth $100 million, from which they successfully claimed approximately $90 million to cover a significant portion of the incurred costs, including legal fees, settlement claims, and security improvements.[50] The total costs incurred by the company related to the data breach amounted to around $292 million, but with the cyber insurance claim, the financial impact was significantly mitigated.[51] Another example is the Equifax data breach in 2017, which exposed the personal data of 147 million consumers.[52] Equifax filed a claim against its $125 million cyber insurance policy, which helped cover part of the substantial costs arising from the incident, including legal fees and security remediation, although the total losses exceeded $1.4 billion.[53]

If we refer to the Precautionary Principle, this principle emphasizes the importance of preventive measures, especially when there is uncertainty about the potential impact of cyber threats.[54] In the context of the Personal Data Protection Law (UU PDP), companies are obligated to protect personal data and are held accountable for legal consequences and administrative fines in the event of a data breach. This is where cyber insurance plays a crucial role. Cyber insurance acts as a risk mitigation instrument, ensuring that companies can mitigate potential financial and legal losses arising from cyber incidents. More than just a reactive measure, cyber insurance helps companies adopt a preventive approach in line with the precautionary principle, minimizing risks amid uncertainty, ensuring ongoing compliance with the UU PDP, and protecting business operations from significant disruptions.

The urgency of implementing mandatory cyber insurance for companies vulnerable to data breaches in Indonesia is becoming increasingly pressing, especially for companies that store millions of user data. In the current digital era, the threats of data breaches and cyberattacks are escalating, as large companies become more dependent on technology infrastructure for their daily operations. Data breaches can have widespread consequences, affecting a company's reputation, consumer trust, and causing significant financial losses. High-profile data breach cases involving e-commerce platforms, banking, and public services in Indonesia demonstrate

[48] *Ibid.*
[49] Shu, X., Tian, K., Ciambrone, A., & Yao, D. (2017). Breaking the target: An analysis of target data breach and lessons learned. arXiv preprint arXiv:1701.04940. https://doi.org/10.48550/arXiv.1701.04940
[50] *Ibid.*
[51] *Ibid.*
[52] Caitlin Kenny, The Equifax Data Breach and the Resulting Legal Recourse, 13 Brook. J. Corp. Fin. & Com. L. (2018).
[53] *Ibid.*
[54] van Asselt, M. B. A., & Vos, E. (2006). The precautionary principle and the uncertainty paradox. Journal of risk research, 9(4), 313-336. https://doi.org/10.1080/13669870500175063

that this risk is real and can happen at any time. Unfortunately, many companies in Indonesia have yet to prioritize cybersecurity optimally, making cyber insurance protection a crucial necessity.

Compared to the steps taken by California through AB 2320, Indonesia can draw valuable lessons from the regulatory model implemented there. AB 2320, introduced by California Assembly member Ed Chau, mandates that any company or contractor working with government agencies and having access to citizens' personal information must have adequate cyber insurance to cover losses resulting from data breaches. This measure aims to ensure that third parties involved in managing sensitive data have sufficient financial protection mechanisms in place in the event of a cyber incident. Furthermore, this regulation encourages companies to enhance their security practices, as there are incentives in the form of lower premiums if the risk of data breaches can be minimized. This approach can be seen as a combination of protecting public data and emphasizing better cyber security practices.

A similar urgency exists in Indonesia, especially considering that companies across various sectors manage millions of highly vulnerable user data. The e-commerce, fintech, telecommunications, and large financial institutions have a significant responsibility to protect consumer data. As a country with a rapidly growing and large internet population, Indonesia is also facing an increasing number of cyber threats year after year.[55] Data breaches involving personal information such as national ID numbers, banking data, and health information can lead to identity theft, fraud, and far greater losses on a national scale. Therefore, mandating companies in these sectors to have cyber insurance would help create stronger protection for users and also encourage companies to take more serious steps to bolster their digital security.

The implementation of cyber insurance as a mandatory program in Indonesia is crucial, considering the high risks of data breaches and the increasing frequency of cyberattacks, especially in companies managing sensitive data. Based on Article 1, paragraph 32 of Law No. 40 of 2014 on Insurance, a mandatory insurance program is defined as one required by legislation to provide protection against certain risks.[56] In this case, the government can establish cyber insurance as a mandatory program through further regulation. In accordance with Article 39A of Law No. 40 of 2014 on Insurance, as amended by the Financial Sector Development and Reinforcement Law (P2SK), the government has the authority to create mandatory insurance programs based on necessity.[57] This allows the government to tailor cyber insurance regulations to the evolving risks in the digital era. With clear legal grounds, the implementation of mandatory cyber insurance will not only enhance companies' compliance with the Personal Data Protection Law (UU PDP) but also provide the necessary financial protection to address the consequences of cyber incidents. In turn, this will strengthen the resilience of Indonesia's business sector in facing the challenges of the digital age.

CONCLUSION

Data breaches represent a serious issue for companies in Indonesia, often resulting from both technical and human factors. These breaches can lead to administrative sanctions, including fines of up to 2% of the company's annual revenue. The legal implications of data breaches extend beyond sanctions, also encompassing significant financial losses such as recovery costs, compensation, and sustained reputation damage. Therefore, implementing adequate security

[55]Ramadhani, F. (2023). Dinamika UU ITE Sebagai Hukum Positif Di Indonesia Guna Meminimalisir Kejahatan Siber. Kultura: Jurnal Ilmu Hukum, Sosial, Dan Humaniora, 1(1), 89-97. https://doi.org/10.572349/kultura.v1i1.98

[56]Article 1 of Law Number 40 of 2014 concerning Insurance.

[57]Article 39A Law Number 4 of 2023 on Development and Strengthening of the Financial Sector

systems and ensuring compliance with the Personal Data Protection Law (UU PDP) are crucial for safeguarding personal data and maintaining consumer trust.

Cyber insurance serves as an effective risk mitigation tool for companies facing cyber threats and complying with UU PDP. With coverage for legal fees, administrative fines, and data recovery, this insurance helps companies manage the financial consequences of cyber incidents and meet their obligations for compensation to data subjects. Although cyber insurance is not yet mandatory in Indonesia, regulatory models like California's AB 2320 highlight the urgency of adopting similar measures to enhance data security in Indonesia. The implementation of mandatory cyber insurance would strengthen compliance with UU PDP and improve the resilience of businesses in the increasingly data-vulnerable digital era.

BIBLIOGRAPHY

Books

Achmad Ali. (2012). *Menguak Teori Hukum (Legal Theory) dan Teori Peradilan (Judicialprudence) Termasuk Interpretasi Undang-Undang (Legisprudence)*. Jakarta: Kencana.

Coburn, A., Leverett, E., & Woo, G. (2018). Solving cyber risk: protecting your company and society. John Wiley & Sons, P.. 47.

Irwansyah. (2013). "Jejak Demokrasi Lingkungan dalam Undang-Undang Nomor 32 Tahun 2009" *Jurnal Ilmu Hukum Amanna Gappa*, 21(2): 121-131.

Muhammad D. (2023). Pertanggungjawaban Hukum PT Tokopedia Terhadap Kebocoran Data Pribadi. Doctoral dissertation, Institut Agama Islam Negeri (IAIN) Polopo, Sulawesi Selatan, P.. 58.

Radiansyah, A., Baroroh, N., Fatmah, F., Hulu, D., Syamil, A., Siswanto, A., & Nugroho, F. (2023). Manajemen Risiko Perusahaan: Teori & Studi Kasus. PT. Sonpedia Publishing Indonesia.

Sulianta, F. (2020). Literasi digital, riset dan perkembangannya dalam perspektif social studies. Feri Sulianta. Jakarta: Feri Sulianta, P.. 20.

Silalahi, F. D. (2022). Keamanan Cyber (Cyber Security). Jakarta: Yayasan Prima Agus Teknik.

Articles

Furnell, S., Heyburn, H., Whitehead, A., & Shah, J. N. (2020). Understanding the full cost of cyber security breaches. Computer fraud & security, 2020(12), 6-12. https://doi.org/10.1016/S1361-3723(20)30127-5

Husna, A. H. (2024). Corporate Communication Literacy in Protecting Consumer's Privacy Data. JURNAL SIMBOLIKA Research and Learning in Communication Study, 10(1). https://doi.org/10.31289/simbolika.v10i1.10763

Kelsen, H. (2005). General Theory of Law and State (1st ed.). Routledge. https://doi.org/10.4324/9780203790960

Prasetyo, T., & Sinambela, J. S. (2023). Penerapan Sanksi Administrasi Dan Sanksi Pidana Terhadap Pencurian Data Pribadi Perspektif Teori Keadilan Bermartabat. Spektrum Hukum, 20(1), 58-69. http://dx.doi.org/10.56444/sh.v20i1.3663

Priliasari, E. (2023). Perlindungan Data Pribadi Konsumen Dalam Transaksi E-Commerce. Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional, 12(2), 20. http://dx.doi.org/10.33331/rechtsvinding.v12i2.1285

Ramadhani, F. (2023). Dinamika UU ITE Sebagai Hukum Positif Di Indonesia Guna Meminimalisir Kejahatan Siber. Kultura: Jurnal Ilmu Hukum, Sosial, Dan Humaniora, 1(1), 89-97. https://doi.org/10.572349/kultura.v1i1.98

Shu, X., Tian, K., Ciambrone, A., & Yao, D. (2017). Breaking the target: An analysis of target data breach and lessons learned. arXiv preprint arXiv:1701.04940. https://doi.org/10.48550/arXiv.1701.04940

Talesh, S. A. (2018). Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers" for businesses. Law & Social Inquiry, 43(2), 417-440. https://doi.org/10.1111/lsi.12303

Tanjung, F., Dania, A. P., Saputri, A. D., Sumbayak, D., Ramadhani, N., Bangun, S. K. B., & Nainggolan, L. B. (2024). Pengaruh Keberadaan Amerika Di Akhir Abad Ke-20 Sampai Awal Abad Ke-21, Holistik Analisis Nexus, 1(6). https://doi.org/10.62504/zt1wra81

Teichmann, F. M. J., & Wittmann, C. (2023). When is a law firm liable for a data breach? An exploration into the legal liability of ransomware and cybersecurity. Journal of Financial Crime, 30(6), 1491-1498. https://doi.org/10.1108/JFC-04-2022-009

van Asselt, M. B. A., & Vos, E. (2006). The precautionary principle and the uncertainty paradox. Journal of Risk Research, 9(4), 313-336. https://doi.org/10.1080/13669870500175063

Yudistira, M., & Ramadani, R. (2023). Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 oleh KOMINFO. UNES Law Review, 5(4), 3917-3929. https://doi.org/10.31933/unesrev.v5i4.698

Law

The Constitution of the Republic of Indonesia 1945.

Law Number 27 of 2022 on Personal Data Protection (Lembaran Negara Tahun 2022 Nomor 196, Tambahan Lembaran Negara Negara Nomor 6820).

Law Number 40 of 2014 on Insurance (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 337, Tambahan Lembaran Negara Republik Indonesia Nomor 5618).

Law Number 4 of 2023 on Development and Strengthening of the Financial Sector.

Websites

APA ITU Perlindungan Data?: Microsoft Security. Apa itu Perlindungan Data? | Microsoft Security. (n.d.). https://www.microsoft.com/id-id/security/business/security-101/what-is-data-protection accessed on 3 September 2024.

Asmaaysi, A. (2023, May 14). Kronologi Nasabah BSI Kehilangan Tabungan RP378,25 Juta Hingga konfirmasi bris. Bisnis.com. https://finansial.bisnis.com/read/20230514/90/1655744/kronologi-nasabah-bsi-kehilangan-tabungan-rp37825-juta-hingga-konfirmasi-bris accessed on 3 September 2024.

British Broadcasting Corporation. (2012). Noken Papua Mendapat Pengakuan UNESCO.

Available from: http://www.bbc.co.uk/indonesia/berita_indonesia/2012/12/121205_noken_unesco. accessed on 16 May 2015.

Dancor. (2023, June 24). Dampak Besar kebocoran data TERHADAP Reputasi Perusahaan. Hypernet. https://www.hypernet.co.id/id/2023/06/24/dampak-besar-kebocoran-data-terhadap-reputasi-perusahaan/ accessed on September 26, 2024.

Ginanjar, R. P. A. (2024, August 30). Jejak Persaingan Shopee Dengan Tokopedia, Siapa Penguasa Pasar e-commerce Ri Saat Ini?. Tempo. https://bisnis.tempo.co/read/1910326/jejak-persaingan-shopee-dengan-tokopedia-siapa-penguasa-pasar-e-commerce-ri-saat-ini accessed on September 21, 2024.

Indonesia masuk 10 Negara dengan kebocoran data terbesar: Databoks. Pusat Data Ekonomi dan Bisnis Indonesia. (2024, June 28). https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/cc5473708a4f8dc/indonesia-masuk-10-negara-dengan-kebocoran-data-terbesar accessed on 3 September 2024.

Kronologi Lengkap 91 Juta Akun Tokopedia Bocor Dan Dijual. Teknologi. (2020, May 3). https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual accessed on 3 September 2024.

PricewaterhouseCoopers. (n.d.). One in four companies globally have suffered a data breach that cost them US$1 - 20 million or more in the past three years. PwC. https://www.pwc.com/id/en/media-centre/press-release/2022/english/one-in-four-companies-globally-have-suffered-a-data-breach-that-cost-them-usd-1-20-million-or-more-in-the-past-three-years.html accessed on October 25, 2024.

Sari, N. P. (n.d.). Data BPJS Kesehatan Diduga Bocor, Menteri Tjahjo Dukung Kemkominfo Usut Tuntas. Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi. https://www.menpan.go.id/site/berita-terkini/data-bpjs-kesehatan-diduga-bocor-menteri-tjahjo-dukung-kemkominfo-usut-tuntas accessed on 3 September 2024.

Telkomsel, operator Seluler Terbesar Dengan Layanan Digital Terdepan. Ekonomi. (2024, July 9). https://www.cnnindonesia.com/ekonomi/20240708153421-97-1118865/telkomsel-operator-seluler-terbesar-dengan-layanan-digital-terdepan accessed on September 21, 2024.