International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838, Print ISSN: 2664-682X
Received: 19-04-2024, Accepted: 10-05-2024, Published: 03-06-2024
Volume 6, Issue 2, 2024, Page No. 108-114

Mitigating cyber security risks through the principle of subrogation in cyber insurance in Indonesia

Purgito[1*], Ratna Januarita[2], Neni Ruhaeni[2], Toto Tohir Suriaatmadja[2]
[1] Faculty of Law, Universitas Islam Bandung, Bandung, Indonesia
[2] Lecturers, Faculty of Law, Universitas Islam Bandung, Bandung, Indonesia

Abstract
The absence of adequate legal regulations regarding Cyber Security Risks through the application of the subrogation principle in the Cyber Insurance industry can create legal uncertainty in protecting against threats to cyber security in the cyber insurance industry. This research aims to explore the role of the state in mitigating Cyber Security Risks in the Cyber Insurance Industry. The method used is normative legal analysis to assess the extent of the state's role in establishing rules to provide legal protection and legal certainty in the cyber insurance industry. The research results indicate that existing legal regulations have not been able to provide adequate legal protection, which may disrupt or hinder the growth of the cyber insurance industry. It is important to establish legislation that can provide legal protection for the sustainability of the cyber insurance industry, particularly in the application of the subrogation principle.

Keywords: Mitigation, cyber security risk, cyber insurance

Introduction

Currently, technology is advancing rapidly, leading us to become highly reliant on it. The technology that plays the most significant role is information technology and data processing. The phenomenon of digital transformation and digitalization is changing how businesses and organizations operate [1]. With the help of interconnected information processes and technologies, companies can achieve their goals by generating added value and balancing the benefits and risks of information technology [2].

Alongside this, there is also an increase in risks resulting from the operation of such technology. Many risks can arise from the implementation of digital technology. The rapid digitization of the economy and social interactions is the primary reason why issues like cyber risks, cyber threats, and cyber security continue to grow in importance. The digitization of the economy and social interactions brings new opportunities and serious threats, but it is not the only source of development and innovation opportunities. Unintentional or intentional cyber incidents can lead to the loss of availability, integrity, and confidentiality of digital data [3]. There are important and influential factors in explaining cyber risk incidents and the amount of losses, namely size, contagion risk, and legal responsibility. The importance of these three factors is not only applicable to the financial industry but also to other industries exposed to cyber risks [4].

Cyber risks resulting from the use of technology pose the biggest new threat faced by businesses and consumers, manifesting in losses related to the use of electronic equipment, computers, information technology, and virtual reality. The security of consumer, financial, and health information is increasingly crucial. Identity theft and the theft of personal, financial, and health information can occur due to hackers, malware, viruses, tracking software, eavesdropping, robocalls, and requests. Almost all major industries are affected by these breaches; these include financial services, healthcare, government, entertainment, sales, insurance, social networking, credit card processing, and legal sectors [5]. Because cyber insurance is a crucial component of the digital world, cyber risk management is highly important and at the core of the digital realm. Therefore, the insurance industry must ensure and provide facilities for the cyber insurance market to continue growing and developing robustly [6]. Cyber insurance promotes internet security and is an integral part of digital risk management [7]. Every new technology brings new opportunities and risks. These risks do not disappear but evolve with technological advancements [8].

Heuristics and the availability of protective tools, such as firewalls and passwords, are typically the foundation of cyber risk management [9]. Cyber risks are generally associated with financial loss, disruption, or damage to an organization's reputation caused by failures in its information technology systems. Cyber risks can manifest in various ways, such as operational IT risks due to factors like poor system integrity. Additionally, cyber risks can arise from cybercrime. Smart technology, digitization, and globalization have increased the propensity and intensity of cybercrimes [10]. The insurance business is currently embracing opportunities to make technological breakthroughs. This has accelerated the digitization of the insurance market [11]. The insurance industry has become more vulnerable to cyber threats due to the increased use of digital technology by industry players. This can include disruptions to business operations and data theft. Therefore, the progress of digitization in the insurance industry must be accompanied by improved governance and risk management of information technology. IT supervision is crucial to prevent the negative effects of IT use on consumers and industry stability [12].

Based on data from the Institute of Internal Auditors (IIA), the Financial Services Authority (OJK) recorded losses due to cybercrime worldwide in 2023 amounting to 8 trillion US dollars. According to Sophia Wattimena, Chair of the Audit Board of OJK, losses due to ransomware worldwide are estimated to reach 265 billion US dollars in 2031. According to data from the National Cyber and Crypto

Agency (BSSN), there were 361 million cyber attacks in Indonesia from January to October 2023. Therefore, these figures are quite significant [13]. Because cyber risks can affect business activities as a whole, they can have a significant impact. The larger the company, the greater the risk [14]. All stakeholders agree that cyber threats continue to increase, as evidenced by constantly evolving cyber threats. This occurs even though there are no agreed-upon standards. Special insurance for cyber risks is needed as a solution, using insurance types related to cyber risk. The insurance industry is one of the businesses impacted by technological advancements. The development of a separate market for cyber insurance is driven by the need to address cyber risks and the challenges of digital transformation [15]. However, this market is hindered by information asymmetry, data scarcity, and moral hazard issues, highlighting the need for better risk assessment.

Cyber insurance is an insurance product specifically designed to protect businesses from threats in the digital era, such as data breaches or harmful cyber intrusions into computer systems. Recently, computer network attacks have occurred both domestically and internationally. The high risk of cyber attacks presents an opportunity for the insurance industry to offer cyber insurance products, especially in terms of policy design that promotes network security enhancement [16]. Despite the sharp increase in insurance premiums, demand for cyber protection as part of risk mitigation has grown rapidly. The high demand for coverage has attracted new players to the cyber market, expanding its market share. Factors such as technological advancements and cyber-related loss activity have driven the growth of the cyber insurance market [17].

In 2022, the top ten cyber insurers in the US controlled 52% of the market share. Conversely, leading data and analytics companies like GlobalData project that the global cyber insurance market will increase from US$16.7 billion in direct written premiums (DWP) in 2022 to US$33.4 billion in 2027 [18]. However, in Indonesia, there aren't many insurance companies offering policies in this field. One player in the Indonesian cyber insurance industry is AIG Indonesia through its CyberEdge® insurance. AIG's website states that this insurance provides several protection features specifically designed to help manage and reduce the effects of data breaches and the consequences of company information loss [19]. Every business is responsible for its own risks. Risk transfer, such as purchasing insurance, is a strategy for managing risks. The demand for cyber insurance products continues to increase as a result of these emerging risks [20]. By having a cyber insurance policy, one has the assurance of proper cyber insurance, which can provide crucial support to help businesses survive. In the event of a cyber attack, a cyber insurance policy will cover financial costs, financial risks, and reputational risks for both first and third parties if data or electronic systems are lost, damaged, stolen, or corrupted. The insurance policy covers expenses for cybercrime investigations, data recovery in security breaches, computer system restoration, lost income due to business closure, reputation management, ransom payments demanded by hackers, and notification costs if required to inform affected third parties.

In the digital era, it's undeniable that the virtual world has become crucial in all activities. This makes business owners vulnerable to cybercriminals in terms of the security of customers' or consumers' personal data. It necessitates cyber insurance designed to protect vulnerable parties. The study of how law and technology interact is now more important than ever. To cite a few examples, advancements in technology such as artificial intelligence, information communication, biological and chemical techniques, and space travel technology have forced us to reconsider what we know about basic concepts in litigation law and insurance [21]. Given the crucial role of insurance companies in the insurance industry in maintaining customer trust, insurance companies in Indonesia must be extremely cautious in protecting personal data. Failure to protect personal data can jeopardize the company's reputation and integrity [22]. However, this vigilance remains vulnerable to the emergence of cyber risks. Cyber risks arising from cyber attacks can lead to losses. These losses become the responsibility of the insurance company, which in this case acts as the Underwriter for the arising cyber risks.

In insurance law, there is a legal relationship between the Insurer and the Insured regarding risk management. This legal relationship arises from an insurance agreement known as the insurance policy. The policy outlines the rights and obligations of the parties based on general contract principles such as the principle of consensus, good faith, and freedom to contract. Additionally, insurance agreements adhere to insurance principles such as insurable interest, utmost good faith, indemnity, and subrogation. Insurance companies and policyholders have a legal relationship with each other as a result of the contract they sign, which is stipulated in the agreement. In this agreement, each party has rights and obligations that must be adhered to and implemented in accordance with the law [22]. The legal relationship between the insurer and the insured arises from an insurance agreement made by the parties [23]. In this context, our case study examines the application of the subrogation principle in cyber insurance policies. Generally, in every loss insurance policy, there is always a clause about subrogation. For example, the subrogation clause is included in the Allianz cyber insurance policy. The policy states that the insurer will receive subrogation rights over all recovery rights held by the insured for all losses reimbursed by the insurer or all amounts insured in this policy. The insured must make all necessary efforts to obtain all these rights, including signing all required documents so that the insurer can effectively pursue claims on behalf of the insured, whether such actions are crucial to be taken either before or after payments are made by the insurer.

The subrogation principle is regulated in Article 284 of the Commercial Code (KUHD), which states: "The insurer who has paid for the insured goods losses acquires all rights that the insured would have against third parties regarding those losses; and the insured is responsible for any actions that may harm the insurer's rights against those third parties." The replacement of such position in civil law is called subrogation. Based on the provisions of this article, it can be understood that for subrogation to occur in insurance, two conditions are required: (a). The insured has rights against the insurer and third parties. (b). These rights arise due to losses caused by the actions of third parties [24]. In insurance law, if the insured has received compensation for their loss from the insurer, they cannot then claim rights from the third party who caused the loss. The rights against the third party are transferred to the insurer who has paid compensation to the insured. The purpose of this provision is to prevent the insured from receiving double

compensation, which would contradict the principle of balance or unjust enrichment. This principle is actually a logical consequence of the indemnity principle, which is to provide compensation to the insured only for the losses they have suffered. If the insured still has claims against others after receiving compensation, they are not entitled to receive them, and these rights are transferred to the insurer [25].

In practice, subrogation rights must not prejudice the insurer's rights, such as when the insured releases a third party from the obligation to pay compensation or provides compensation for their debts. Thus, when the insurer exercises its subrogation rights against a third party, the insured no longer has a relationship with the third party, and the insured is responsible for any actions that harm the insurer. Subrogation is a legal right held by insurance companies to recover the money paid to the insured from the party at fault. Until now, subrogation has been a somewhat difficult, complex process requiring a lot of communication and physical inspection between the insurance company and the insured [26]. The application of the subrogation principle is always related to the principle of indemnity or the principle of balance, which states that compensation must be in line with the actual loss incurred. In insurance law, the principle of indemnity states that the insured is entitled to full compensation for their losses, neither more nor less [27].

If the insured receives compensation from both the insurer and the third party responsible for the loss, then the insured's position becomes enriched or receives payment exceeding the actual loss value. Therefore, the insured who has received compensation from the insurer cannot claim compensation from the third party who caused the loss. Thus, based on the subrogation principle, the insured who has received compensation from the insurer transfers their right to claim compensation to the insurer. Both the insurer claiming subrogation and the claimant seeking compensation have one similarity: their claims are solely related to financial losses [28]. In accordance with the insurance agreement, the insurance company acquires all rights of the insured from the responsible party for the damage. The insurer takes on the insured's role and utilizes its right to subrogate the insured's rights. For the insurer, subrogation is not an obligation but a right [29]. The need to manage cybersecurity threats faced by cyber insurance companies is one of the main challenges in the cyber insurance industry. In this industry, the implementation of the subrogation principle has become a highly important topic for addressing these risks. In cyber insurance, the subrogation principle can be used to reduce the financial losses borne by insurance companies due to successful cyber attacks. Insurance companies can take over the insured's rights to pursue other parties responsible for the losses. Subrogation action has two advantages: reducing risk for companies collecting consumer data and encouraging vendors to maintain better data security. In other words, subrogation action specifically provides dual benefits, namely risk mitigation for companies collecting consumer data and incentives for better data security among data-storing vendors [30].

The right of subrogation arises due to the actions of a third party that cause damage to the insured object. For the resulting damage, the third party can be claimed for compensation. According to Article 1365 of the Civil Code, any act that violates the law and causes harm to others obliges the person responsible for the harm due to their fault to compensate for the loss. In this regard, the insurer as the owner of the object has the right to claim compensation from the third party responsible for the loss. However, in the context of insurance, after the insurer compensates the insured, the right to claim compensation shifts to the insurer. In conventional insurance, identifying the third party causing the loss is not difficult because the insured can directly ascertain the risk when it occurs. However, it becomes a different issue when the insured object is related to cyber insurance, specifically cyber security risk. The third party causing the loss is often challenging to identify, and even if known, they may be outside the jurisdiction of Indonesia, making it difficult to exercise the right of subrogation.

Therefore, a solution needs to be found to resolve this legal issue. In this regard, the involvement of the state is required to assist with this matter. Referring to various legal regulations that govern cybersecurity, including Law Number 19 of 2016 regarding Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), and Presidential Regulation Number 47 of 2023 regarding National Cyber Security Strategy and Cyber Crisis Management (PP 47/2023). These three legal regulations only regulate the protection of objects and legal subjects related to data security, but do not address how to assist insurance companies in the implementation of subrogation rights. In the ITE Law Article 26, it is stated that the use of any information through electronic media related to personal data must be done with the consent of the individual concerned, and any person whose rights are violated can file a lawsuit for damages caused. Regarding cyber risks, the ITE Law focuses on protecting information security and mitigating risks arising from cyber attacks or threats. As explained in Article 40, the government protects public interests from all types of disruptions due to the misuse of electronic information and transactions that disturb public order, conducts prevention of dissemination, interrupts access, and/or orders electronic system providers to interrupt access to electronic information and/or documents that contain illegal content. Legal protection in the PDP Law is regulated in Article 65, which mentions prohibitions on the use of personal data. It states that anyone is prohibited from unlawfully obtaining or collecting personal data that does not belong to them with the intention of benefiting themselves or others, which may result in harm to the data subject. Meanwhile, in PP 47/2023 Article 24, it includes risk mitigation which explains cyber crisis recovery. A Cyber Crisis is an emergency situation resulting from a cyber incident at the national level that impacts the safety, integrity, and sovereignty of the country. Cyber Crisis Recovery as referred to in Article 24 letter b is the effort to recover impacted electronic systems at the national level. On the other hand, recovery through the implementation of the subrogation principle is part of risk mitigation, aimed at reducing the financial losses borne by insurance companies due to partial cyber attacks.

Method

This research employs a juridical-normative research approach, which positions law as a normative system. Juridical-normative research delves into principles, norms,

rules, agreements, court decisions, and legal doctrines or teachings. The study connects a concept based on literature in the field of insurance law with factual contractual relationships observed in the practical realm of cyber insurance products. Based on the gathered data approach, this type of research is qualitative, generating descriptive data. It adopts a descriptive-analytical method, aiming to describe the application of the subrogation principle in insurance agreements within the practical context of the cyber insurance industry for risk mitigation purposes. In this qualitative study, the author seeks to explain actual facts within the practical framework of clauses in cyber insurance policies, then examines concepts in insurance agreements related to the principles of insurance agreements from a cyber insurance perspective. The research is conducted through a literature review. The methodological approach is intended to gather information from various aspects regarding legal issues to find answers, which include a conceptual approach based on expert opinions (doctrine) related to insurance law matters, a legal approach, and a comparative approach as part of the complementary approach to compare national law and foreign law related to insurance, particularly cyber insurance [31].

Result and Discussion

The Practice of Cyber Insurance and the Application of Subrogation

In Japan, cyber insurance has experienced rapid growth as a comparative study. The number of insurance policies used to protect users and businesses from cyber threats has increased in Japan. According to Asia Insurance Review, the number of cyber insurance policies increased from fiscal year 2016 to March 2017. Mitsui Sumitomo Insurance reported a 250% increase, Tokio Marine & Nichido Accident Insurance reported a threefold increase, AIU Insurance reported a 50% increase, and Sompo Japan Nipponkoa Insurance reported a 350% increase. The Yomiuri Shimbun reported these figures without specifying absolute numbers [32]. Furthermore, in 2021, cyber insurance sales in Japan increased by fifty percent, indicating a rising demand for cyber insurance that protects businesses from damage caused by cyberattacks [33].

Human life relies heavily on computer systems and networks. Hackers and anonymous attackers intimidate organizations, companies, and governments into creating security networks by providing budgets and taking steps to protect national secrets, trade secrets, and personal information. This includes Japan. Cyberattacks can cause significant damage to countries, governments, and companies when they steal and leak personal information. As a result, cyber insurance is needed to cover the damages and costs caused by cyberattacks. Cyber insurance consists of two categories: first-party insurance, similar to property insurance, and third-party insurance, similar to liability insurance. At least, original Japanese non-life insurance companies do not have specific insurance for cyberattacks. Cyber insurance in Japan shares similarities with traditional property insurance and liability insurance. Given that attackers and anonymous hackers target companies, organizations, and governments, it seems appropriate for its government to take preventive actions against these attacks and hacking incidents. According to the traditional understanding of first-party insurance, when an insurance company pays insurance money to the insured party, the insurance company has subrogation rights against the party at fault for the error and cancels the insured party's right to claim from the faulty party. However, in cyber insurance, subrogation rights are meaningless because the insurance company cannot identify the tortfeasor. This phenomenon raises the question of whether subrogation rights are an essential aspect of property insurance or not [34]. The term "tortfeasor" refers to a person who commits a wrongful act, where the law allows the aggrieved party to seek restitution or compensation.

The cyber insurance market in Georgia has experienced significant impacts from the evolving cybersecurity threats. This is due to the fact that cyber threats continue to evolve and become more sophisticated, making companies in Georgia more vulnerable to cyber attacks, data breaches, and other cyber incidents. This has increased the demand from state insurance companies for cyber insurance protection. Georgia insurance companies have responded to this demand by offering stronger cyber insurance policies that protect against various cyber threats [35]. In contemporary legal literature, the term "subrogation" is used to describe substitution. This encompasses the process by which an insurer can claim against a third party for losses caused by their negligence. Georgia law includes the concept of subrogation, although the term "subrogation" is not explicitly used to refer to this relationship. Article 832 of the Georgia Civil Code defines the relationship as a claim for damages against a third party, which in this context is the institution of subrogation. Subrogation is based on principles of restitution for damages, prohibition of unjust enrichment, and restoration of the original condition. Insurers can request policyholders to reimburse losses under the institution of subrogation. After reimbursing the policyholder's losses, the insurer, in turn, has the right to claim against the third party [36].

Implementing the Principle of Subrogation as a Mitigation for Cyber Risk

The application of the principle of subrogation in Indonesia is related to the principle of indemnity. The principle of indemnity explains that compensation must be proportionate to the actual loss. Providing compensation is about restoring the situation to its original state. This can be interpreted as compensation being quantifiable in monetary terms. Additionally, the provision of subrogation does not apply to social insurance. In contrast, the principle of subrogation in America can apply to health insurance and social insurance. It is noted that subrogation provisions are a common feature of property insurance, liability insurance, health and medical insurance, and disability insurance in the United States. This can also apply to government-provided insurance, especially for Medicare, Medicaid, workers' compensation, and accident insurance [37]. The subrogation principle is also known as the principle of representation, transfer of rights, or in other terms, the subrogation principle. There are provisions in insurance law regarding subrogation, whereby if the insured has received compensation from the insurer, they cannot claim compensation from the third party. Once the insurer has provided compensation to the insured, the right to claim compensation from the third party transfers from the insured to the insurer. Therefore, the insured no longer has the right to seek compensation from the third party who caused the loss, as this right has transferred to the insurer upon payment of compensation. The subrogation

principle supports the principle of indemnity, especially in insurance against losses [38].

Furthermore, it is acknowledged that the biggest legal barrier is the contractual limitations that may have been included by some subrogation targets in their service contracts. However, before these limitations become an issue, factual barriers to cyber investigations themselves often create initial obstacles by preventing forensic analysts from fully understanding the extent and causes of the data breach [39]. Based on the description above regarding subrogation, the application of the subrogation principle can be applied in various data security contexts, such as:

1. **Damage or loss caused by the negligence of a third party:** The subrogation principle can be used if the damage or loss covered in the data management contract is caused by the negligence of a third party. For example, if a third party accesses data without the consent of the insured party, the insurer can obtain subrogation rights to claim against the third party that caused the damage.

2. **Damage or loss caused by tort (unlawful act):** The subrogation principle can be used if the insured property experiences damage or loss covered in the policy caused by the negligence of a third party. For instance, if a third party accesses data without permission, the insurer can obtain subrogation rights to claim against the third party that caused the damage.

3. **Damage or loss caused by insurance:** The subrogation principle can be used if the damage or loss covered in the data management contract is caused by insurance. For example, if a third party accesses data managed by the insurer, the insurer can obtain subrogation rights to claim against the third party that caused the damage.

4. **Damage or loss caused by the delay of a third party:** The subrogation principle can be used if the damage or loss covered in the data management contract is caused by the delay of a third party. For instance, if a third party fails to pay within the specified time in the contract, the insurer can obtain subrogation rights to claim against the third party.

5. **Damage or loss caused by improper data usage:** The subrogation principle can be used if the damage or loss covered in the data management contract is caused by improper data usage. For example, if a third party uses data provided in violation of the agreement, the insurer can obtain subrogation rights to claim against the third party that caused the damage.

Essentially, the principle of subrogation can be applied in the context of data security when the losses or damages covered in the data management contract are caused by third parties' errors/negligence, tort, insurance, delays, or unauthorized data use.

In the context of cyber insurance, several challenges can hinder the implementation of subrogation for risk mitigation:

1. **Difficulty in identifying third parties:** In the realm of data security, third parties can include individuals, companies, or other organizations that access data without the insured party's permission. However, locating and identifying these third parties can be challenging, especially if they are located overseas.

2. **Difficulty in accessing information:** Concerning data security, the information required to identify third parties and proceed with the subrogation process can come from various sources such as information systems, security reports, and activity logs. An activity log is a digital record that logs every activity or event occurring within a system, application, or device. System administrators may face challenges in extracting relevant information from data related to log file attacks [40]. Therefore, excessive difficulty in accessing information can pose a hindrance to subrogation implementation.

3. **Difficulty in arranging affidavit creation:** In the context of data security, affidavits from third parties may be required to strengthen the case in the subrogation process. However, arranging for the appropriate creation of affidavits can be challenging, particularly if the third party is located overseas.

4. **Difficulty in arranging payments:** Concerning data security, payments required for subrogation may come from various sources such as insurance, patent holders, or third parties. However, difficulty in arranging appropriate payments can be a constraint in subrogation implementation.

5. **Difficulty in arranging contracts:** In the context of data security, suitable contracts may be necessary for subrogation. However, difficulty in arranging appropriate contracts can be a hindrance in subrogation implementation, especially if the third party is located overseas.

6. **Difficulty in managing data:** In the context of data security, proper data management can aid in subrogation implementation. However, difficulty in managing data appropriately can be a constraint in subrogation implementation.

7. **Difficulty in arranging communication:** In the context of data security, effective communication can aid in subrogation implementation. However, difficulty in arranging suitable communication can be a hindrance in subrogation implementation, especially if the third party is located overseas.

In the context of cyber insurance, insurance companies must possess the capability and discipline to address these challenges, enabling effective and efficient implementation of subrogation. Cyber subrogation responsibility is a relatively new aspect in insurance law. Therefore, it requires a keen expertise from subrogation attorneys to effectively subrogate claims in this field. Because the losses and actions involved are intangible, successfully reconstructing events and identifying responsible parties pose difficulties without lawyers focused on this complex area of insurance law [41].

The obstacles and challenges faced by the insurance industry in addressing recovery issues through the application of the subrogation principle for risk mitigation in the cyber domain are significant. Implementing

subrogation in cyber insurance encounters several hurdles in facilitating smooth cyber risk transfer. Issues such as data transparency, incident measurement, and reporting—making relevant data available to the public—are crucial in enabling stakeholders to make accurate pricing decisions (Skeoch & Ioannidis, 2024). These obstacles are undoubtedly difficult to overcome, necessitating the involvement of the state in resolving such issues. If there are indeed barriers hindering insurance companies' subrogation rights implementation for risk mitigation, it is also essential to consider involving the government actively in risk mitigation through subrogation implementation by formulating procedures and provisions in legislation. The partial and sectoral governance of cybersecurity in Indonesia has led to the lack of integrated cybersecurity management. This makes cyber threats increasingly real, especially when considering the cybersecurity threats faced by government and private sector entities. Therefore, cybersecurity management must be conducted comprehensively to protect the nation and its institutions from cyber attacks. The National Cyber and Crypto Agency (BSSN), as the government agency responsible for cybersecurity, is expected to help establish a legal framework for cybersecurity that must be adhered to by all stakeholders involved in cybersecurity implementation in Indonesia. Moreover, this legal framework should include regulations that enable the prosecution of cyber crimes, ensuring that violations committed in the cyber realm can be punished [42].

Conclusion

The cyber insurance industry in Indonesia takes cues from practices in several countries, yet it still lags behind in development. This is due in part to the lack of adequate legal frameworks for mitigating cyber risks. The use of provisions based on insurance laws has not been able to address the interests of stakeholders in the cyber insurance industry, given its unique characteristics that differ from conventional insurance practices. The implementation of the subrogation principle for mitigating cyber risks appears to face difficulties, not only in Indonesia but also in several other countries where challenges such as identifying third parties, accessing information, creating affidavits, and managing data have been acknowledged.

In Japan, for instance, in cyber insurance, subrogation rights hold little meaning because insurance companies cannot identify the tort-feasor. Meanwhile, in the United States, subrogation for cyber liability insurance has not matured well, although it is currently an interesting focus area. The biggest legal hurdle lies in contract limitations that may have been included by some subrogation targets in contracts and efforts to prevent forensic analysts from fully understanding the extent and causes of data breaches. Specifically in Indonesia, to mitigate cyber risks through subrogation, which faces numerous challenges, the involvement of the government is necessary. This entails encouraging the active participation of the government in risk mitigation through subrogation by establishing procedures and regulations formulated in legislation. This effort would have a positive impact, creating an increasingly advanced and thriving business climate, especially in the cyber insurance industry.

References

1. Bencsik A, Hargitai DM, Kulachinskaya A. Trust in and risk of technology in organizational digitalization. Risks, 2022, 10(5). Available from: https://doi.org/10.3390/risks10050090
2. Erniwati S, Kurnia N. An analysis of information technology on data processing by using Cobit framework. Int J Adv Comput Sci Appl, 2015, 6(9). Available from: https://doi.org/10.14569/ijacsa.2015.060920
3. Strupczewski G. Defining cyber risk. Safety Sci, 2021, 135. Available from: https://doi.org/10.1016/j.ssci.2020.105143
4. Eling M, Jung K. Heterogeneity in cyber loss severity and its impact on cyber risk measurement. Risk Manag, 2022, 24(4). Available from: https://doi.org/10.1057/s41283-022-00095-w
5. Talesh SA. Data breach, privacy, and cyber insurance: how insurance companies act as "compliance managers" for businesses. Law Soc Inq, 2018, 43(2). Available from: https://doi.org/10.1111/lsi.12303
6. Fajrul Falah M. Tren risiko cyber insurance di 2023. Media Asuransi News, 2023 May 5. Available from: https://mediaasuransinews.co.id/asuransi/tren-risiko-cyber-insurance-di-2023/. Accessed 2024 Apr 2 at 8:20 PM WIB.
7. Bolot J, Lelarge M. Cyber insurance as an incentive for internet security.
8. Rawlings P. Cyber risk: insuring the digital age: updating the US cases. SSRN Electron J, 2021. Available from: https://doi.org/10.2139/ssrn.3769284
9. Pate-Cornell ME, Kuypers MA. A probabilistic analysis of cyber risks. IEEE Trans Eng Manag, 2023, 70(1). Available from: https://doi.org/10.1109/TEM.2020.3028526
10. Cremer F, Sheehan B, Fortmann M, Kia AN, Mullins M, Murphy F, *et al*. Cyber risk and cybersecurity: a systematic review of data availability. Geneva Pap Risk Insur Issues Pract,2022:47(3):698-736. Available from: https://doi.org/10.1057/s41288-022-00266-6
11. Mustafina AA, Kaigorodova GN, Alyakina PD, Velichko NY, Zainullina MR. Digital technology in insurance. Adv Intell Syst Comput, 2020, 908. Available from: https://doi.org/10.1007/978-3-030-11367-4_65
12. Financial Services Authority. Indonesia insurance roadmap 2023-2027, 2023.
13. Ghifari HR. OJK: Akibat kejahatan siber, dunia rugi 8 T Dolar AS pada 2023. Tirto.id. Available from: https://tirto.id/ojk-akibat-kejahatan-siber-dunia-rugi-8-t-dolar-as-pada-2023-gSPd. Accessed 2024 Apr 4 at 10:21 PM WIB.
14. Arifin MT. Apa itu cyber insurance? Liga Asuransi, 2021 Nov 30. Available from: https://ligaasuransi.com/en/apa-itu-cyber-insurance/. Accessed 2024 Apr 2 at 9:35 PM WIB.
15. Hatzivasilis G, Chatziadam P, Petroulakis N, Ioannidis S, Mangini M, Kloukinas C, *et al*. Cyber insurance of information systems: security and privacy cyber insurance contracts for ICT and healthcare organizations. IEEE Int Workshop Comput Aided Model Des Commun Links Netw CAMAD, 2019 Sep. Available from: https://doi.org/10.1109/CAMAD.2019.8858165

16. Khalili MM, Naghizadeh P, Liu M. Designing cyber insurance policies in the presence of security interdependence. NetEcon 2017 12th Workshop Econ Netw Syst Comput ACM EC 2017 18th ACM Conf Econ Comput, 2017. Available from: https://doi.org/10.1145/3106723.3106730
17. Cole CR, Fier SG. An empirical analysis of insurer participation in the U.S. cyber insurance market. North Am Actuar J, 2021, 25(2). Available from: https://doi.org/10.1080/10920277.2020.1733615
18. Aris A. Menilik prospek bisnis cyber insurance global. Media Asuransi News, 2021 Aug 2. Available from: https://mediaasuransinews.co.id/majalah/menilik-prospek-bisnis-asuransi-siber-global/. Accessed 2024 Apr 3 at 8:45 PM WIB.
19. Hidayat ASE. Cyber insurance di era 4.0, pentingkah? Datapolis.id. Available from: https://datapolis.id/asuransi-siber-di-era-4-0-pentingkah/. Accessed 2024 Apr 3 at 10:15 AM WIB.
20. Zeller G, Scherer M. A comprehensive model for cyber risk based on marked point processes and its application to insurance. Eur Actuar J, 2022, 12(1). Available from: https://doi.org/10.1007/s13385-021-00290-1
21. Lubin A. Insuring evolving technology. Conn Insur Law J, 2021, 28(1).
22. Januarita R, Alamsyah IF, Perdana A. Guardians of data: TruMe Life's continuous quest for data protection. J Inf Technol Teach Cases, 2024. Available from: https://doi.org/10.1177/20438869241242141
23. Syamsuddin M, Putri CS. Proteksi hukum bagi pemegang polis asuransi terhadap pailitnya perusahaan asuransi. SALAM J Sos Budaya Syar-i, 2022, 9(2). Available from: https://doi.org/10.15408/sjsbs.v9i2.25112
24. Sabrie HY, Amalia R. Karakteristik hubungan hukum dalam asuransi jasaraharja terhadap klaim korban kecelakaan angkutan umum. Yuridika, 2015, 30(3):387-406.
25. Muhammad AK. Hukum asuransi Indonesia. Bandung: Citra Aditya Bakti, 2006.
26. Parera BA, Tumanggor MS. Application of business principles insurance in Indonesia. J Law Polit Humanit, 2021, 2(1). Available from: https://doi.org/10.38035/jlph.v2i1.49
27. Bhadra O, Sahoo S, Kumar CM, Halder R. Decentralized insurance subrogation using blockchain. ACM Int Conf Proc Ser, 2022. Available from: https://doi.org/10.1145/3581971.3581972
28. Ginders K. Insurance law and the principle of indemnity in light of Ridgecrest NZ Ltd v IAG New Zealand Ltd. Victoria Univ Wellington Law Rev, 2016, 47(1). Available from: https://doi.org/10.26686/vuwlr.v47i1.4879
29. Weir T. Subrogation and indemnity. Camb Law J, 2012, 71(1). Available from: https://doi.org/10.1017/S0008197312000190
30. Dimov T. Subrogation in insurance contract. Knowledge Int J, 2018, 28(6). Available from: https://doi.org/10.35120/kij28061985t
31. Heath B. Before the breach: the role of cyber insurance in incentivizing data security. George Washington Law Rev, 2018, 86(4).
32. Hernoko AY. Hukum perjanjian asas proporsionalitas dalam kontrak komersial, 2nd ed. Jakarta: Kencana Prenadamedia Group, 2011.
33. Sari ADK. Asuransi cyber makin laris di Jepang. Finansial Bisnis, 2017 Jun 27. Available from: https://finansial.bisnis.com/read/20170627/215/666467/asuransi-cyber-makin-laris-di-jepang. Accessed 2024 Apr 5 at 10:32 AM WIB.
34. Agustina D. Asuransi cyber Jepang meningkat 50 persen. Tribun News, 2021 Aug 2. Available from: https://www.tribunnews.com/internasional/2021/08/02/asuransi-cyber-jepang-meningkat-50-persen-disebabkan-banyaknya-serangan-para-hacker. Accessed 2024 Apr 5 at 10:52 AM WIB.
35. Koezuka T. The cyber insurance in Japan. In: The "Dematerialized" insurance: distance selling and cyber risks from an international perspective. Springer International Publishing, 2016. p, 201-223. Available from: https://doi.org/10.1007/978-3-319-28410-1_9
36. Hong J. Cyber insurance market trends in Georgia. Finsurance Guide, 2024 Feb. Available from: https://www.finsuranceguide.com/insurance/cyber-insurance-market-trends-in-georgia/. Accessed 2024 Apr 8 at 01:27 AM WIB.
37. Kumsiashvili G, Chkhaidze K. Comparison of subrogation with cession and regression. Law World, 2021, 7(4). Available from: https://doi.org/10.36475/7.4.1
38. Polinsky AM, Shavell S. Subrogation and the theory of insurance when suits can be brought for losses suffered. J Law Econ Organ, 2018, 34(4). Available from: https://doi.org/10.1093/jleo/ewy008
39. Purgito P, Permana RAD. Penerapan prinsip indemnitas dan subrogasi dalam klaim asuransi umum. J Surya Kencana Satu: Dinamika Masalah Hukum Dan Keadilan, 2023, 14(2). Available from: https://doi.org/10.32493/jdmhkdmhk.v14i2.34982
40. NetDiligence. Cyber liability and subrogation, 2024 Apr 8. Available from: https://netdiligence.com/conferences/. Accessed 2024 Apr 8 at 00:11 WIB.
41. Cahyanto TA, Prayudi Y. Investigasi forensika pada log web server untuk menemukan bukti digital terkait dengan serangan menggunakan metode Hidden Markov Models. In: Seminar Nasional Aplikasi Teknologi Informasi (SNATI), 2014 Jun.
42. Rathbone Group. Cyber liability, 2024 Apr. Available from: https://www.rathbonegroup.com/practice-areas/cyber-liability/. Accessed 2024 Apr 8 at 01:44 AM WIB.
43. Sudarmadi DA, Runturambi AJS. Strategi Badan Siber dan Sandi Negara (BSSN) dalam menghadapi ancaman siber di Indonesia. J Kajian Stratejik Ketahanan Nasional, 2019, 2(2).