ISSN 2959-3018 (print), ISSN 2959-3026 (online)
thecommonwealth.org/cyber-journal

The Commonwealth

Ensuring a Secure Future by Insuring Against Cybercrime

Eric Cho[1] and Serene Chan[2]

Abstract

The core concept of insurance is for individuals or entities to manage their risks by transferring such risks to a risk carrier like an insurance company in exchange for an insurance premium. With the escalating occurrence of cyber incidents coinciding with the digitisation of society, the imperative for adequate risk management has become critical in board meetings. With the established role of insurance in mitigating traditional risks, there exists a compelling case for the utility of insurance in addressing the consequences for entities facing emerging cyber vulnerabilities. This article investigates the burgeoning demand for cyber insurance policies, which serve to mitigate financial losses sustained by businesses as a consequence of cyber incidents.

This paper explores the role of cyber insurance. The main themes we investigate are:

1. Introduction to cyber risks and cyber insurance.
2. The benefits and challenges of cyber insurance.
3. Government involvement and the future.

Cyber insurance policies first became available in the 1990s, focusing mainly on third-party liability for cases in which companies may have leaked customer data as a result of a cyber incident. Since its inception, the product has seen rapid evolution and growth, driven by the need for more comprehensive coverage for clients and a general increase in awareness of cybersecurity.

The increase in adopting cyber insurance is a testament to its benefits. Cyber insurance is a core risk-management solution for companies to transfer their underlying cyber risks. Despite companies investing more in their cybersecurity, there are numerous cases of cybercriminals gaining unauthorised access to data, leaving companies and their customers exposed to financial loss. As long as the incident is insurable, companies can claim against their policies to reduce the financial losses and, in most cases, receive crisis-management support. Obtaining

1 Senior Cyber Underwriter, Munich Re. Email: echo@munichre.com.
2 Regional Head of Cyber, Asia Pacific, Munich Re. Email: szchan@munichre.com.

cyber insurance also involves underwriting, for which companies' cybersecurity policies and controls are assessed by insurance companies. This underwriting is rigorous, and necessitates that companies adhere to insurers' cybersecurity expectations in order to qualify for cover.

Cyber-attacks are an almost inevitable fate for many companies. Therefore, cyber resilience is fundamental for successful and sustainable digitisation of the economy and society. Cyber insurance can play a vital role in ensuring a tangible solution for companies. The public sector, including governments and regulators, must also play an active role to catalyse awareness of cyber risk and the corresponding risk transfer solution, as cyber insurance is a relatively new product. Increased dialogue and transfer of knowledge that occurs from cyber insurance can help to foster a more resilient digital economy, safeguarding the interests of individuals, businesses and society.

Introduction

Before examining the intricacies of cyber insurance, it is important to understand the context for such a risk transfer solution. With the rapid advancement of digital technology in recent years, cyber risk has synchronously emerged for individuals, companies and nations. Cyber risk can be defined as 'any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems' (Institute of Risk Management, 2023). In today's competitive, globalised markets, companies have targeted operational efficiencies by adopting modern technologies that enhance their ability to deliver value to customers.

The increase in centralisation and interconnectivity between new and old technologies has led to what the industry refers to as the expansion of attack surface (One Identity, 2024). The attack surface is, effectively, the sum of all possible points where an unauthorised user or system could try to enter, or extract data from, an environment. In other words, the more interconnected a system is, the wider the attack surface and the more systems may be affected at any one time, resulting in a more severe business impact following a cyber-attack.

An example of the risks relating to the expansion of the attack surface is the 2017 NotPetya ransomware strain, one of the most destructive malwares in history, which caused $10 billion in damages to companies globally. The origin of the attack could be traced to commonly used tax software in the Ukraine (HYPR, 2023). The dependency of companies and their subsidiaries on interconnected technology (in the case of NotPetya, the connection to a third-party software), creates a prime opportunity for criminals who want to extort money by crippling companies' computer systems and making ransom demands for stopping the attacks.

Ransomware is

> *'a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files until a ransom is paid. More modern ransomware families, collectively categorized as cryptoransomware, encrypt certain file types on infected systems and force users to pay the ransom through certain online payment methods to get a decryption key'.*
> (Trend Micro, 2024)

The first ransomware known was the AIDS Trojan in 1989: Joseph Popp handed out 20,000 floppy disks with the malware to attendees at a World Health Organization conference. Those whose files were encrypted by the ransomware needed to send $189 to a PO box in Panama (Kostka, 2022). Today, ransomware demands can be in the hundreds of millions of dollars, usually in the form of cryptocurrency, with the average ransom payment in 2023 being $1,542,333 compared to $812,380 in 2022 (Sophos, 2023). What used to be a technical term has become a household word because of the numerous headlines about companies and individuals falling victim to ransomware attack.

Recognition of cyber risk

As cyber risk and its consequences have become more significant, managing cyber exposure has become a top priority for many companies and countries. A severe cyber-attack not only poses a tangible threat to a company's operations but also inflicts substantial harm on its reputation, eroding customer trust. A report by the International Data Corporation showed that '80% of consumers in developed nations will defect from a business because their personally identifiable information is impacted in a security breach' (Lieberman, 2017).

Furthermore, cyber risks extend beyond technological disruption and business impact: they have far-reaching implications for national security as well. A breach in cybersecurity can compromise sensitive government data, disrupt critical services and undermine the economic stability of a nation. With the rise of sophisticated cyber threats, including state-sponsored attacks and ransomware incidents, the potential for disruption, economic espionage and the compromise of critical infrastructure becomes more pronounced. Effective cybersecurity and mitigating measures are essential for protecting national interests, preserving economic vitality and safeguarding citizens from the far-reaching consequences of cyber-attack. This makes them fundamental to national security.

Regulators around the world have responded to the escalating threat of cyber attacks by implementing various measures and regulations aimed at enhancing cybersecurity and protecting sensitive data. These include mandatory breach notifications such as the General Data Protection Regulation (GDPR) in the EU and the UK, industry-specific regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in

the US, cybersecurity audits and assessment, and increased scrutiny resulting in hefty fines and penalties being imposed. These are all to keep companies accountable for their cyber risk management.

Cyber risk has, therefore, been recognised as a top priority for management across all levels and industries. One major reason why it has become such an important topic among executives is the potentially significant financial consequences of a cyber incident. The global average cost of a data breach in 2023 was $4.45 million, which was a 15 per cent increase over three years (IBM, 2023). Due to the significant financial and regulatory ramifications of a cyber breach, an increasing number of annual reports include cyber-attacks as one of their top risks.

Cybersecurity market

As the world continues to invest in modern technologies and the interdependency of systems, the need to manage the resulting risks is apparent, with the first step being prevention.

Several companies have emerged in the cybersecurity industry in providing technical solutions. According to McKinsey, 'organisations around the world spent $150 billion in 2021 on cybersecurity, growing by 12.4 percent annually'. This sum is based on a 10 per cent penetration of the market, meaning that the total addressable market size of cybersecurity is expected to be around $1.5 to $2 trillion (Mckinsey, 2022). Given that cybercriminals create progressively more sophisticated attack methods and identify new vulnerabilities to exploit, companies need to rely on dedicated experts both in-house and third parties. Companies are spending considerable efforts on optimising cybersecurity and are constantly looking for ways to protect themselves against threat.

Cyber insurance market

Many insurance companies have formed cyber insurance departments that focus on underwriting cyber risks and providing cyber insurance solutions. Insurance has, historically, played a vital role, allowing individuals and corporations to shift their risks to an insurance company in exchange for insurance premiums. In our increasingly digitised world, the development of solutions that allow companies to mitigate cyber risks is both relevant and crucial. Given the constantly evolving nature of cyber threats that can exploit undiscovered vulnerabilities, companies face perpetual risk. Consequently, having cyber insurance as a second line of defence becomes a prudent and important risk-management option.

History and purpose of cyber insurance

Cyber insurance first emerged in the late 90s, sold through security software companies that partnered with insurance companies (Holot and Lelarge, 2008). Projecting into the future, it is estimated that the global cyber insurance market is worth $12.1 billion in

2023, and is expected to increase to $90.6 billion by the end of 2033 (Market.us, 2024) As one of the newest products in the insurance market, many insurance companies target cyber as one of the strategic growth segments. Also, insuring a critical and emerging risk such as cyber risk allows insurance companies to stay relevant.

So, what is cyber insurance and what does it cover? The purpose of cyber insurance policies is to cover certain financial losses that an organisation has to bear as a result of a cyber incident. The cover of a cyber policy typically falls into two categories: first-party cover and third-party cover.

Originally, cyber insurance policies were primarily created to address third-party liability risks. For example, if an organisation's network is breached and their customer data leaked, customers could launch a class action against the organisation on the basis of a breach of privacy. In such cases, cyber insurance could cover liabilities and legal costs. Over time, as cyber incidents have increased, so has the prevalence of first-party financial losses, resulting in an increase in demand for first-party cover. First-party cover includes necessary expenses relating to recovering systems that have been compromised by cyber-attack. For example, IT forensics investigation expenses or the costs of restoring data could be covered by a cyber insurance policy. Cyber insurance is, fundamentally, a risk-management solution that companies adopt to safeguard against potential financial losses in the event that their cybersecurity measures fail to prevent a breach.

Availability of cyber Insurance

A survey of global C-level executives showed that 33 per cent of participants were never offered cyber insurance. Also, when asked why their company did not have cyber insurance, 25 per cent stated that they did not know cyber insurance existed; 38 per cent of those who did not know were from smaller companies with revenues below $1 million [Munich Re, 2022]. Cyber insurance is generally an underpenetrated insurance policy and appears to be more of a 'reactive' purchase. For example, 32 per cent of companies purchased cyber insurance after a cyber-attack, and 37 per cent of companies purchased it as a reaction to a cyber-attack in a peer company (Deloitte, 2019). During the initial phases of cyber insurance availability, there was scepticism about its necessity, with companies prioritising cybersecurity tools and considering them sufficient to thwart all cyber threats. The dilemma was compounded by the reluctance of IT managers, responsible for overall cybersecurity, who were often known in the industry as adopting a defensive stance. This posed a challenge for risk managers tasked with deciding whether or not to invest in cyber insurance when confronted with the reservations of their counterparts in IT management.

Despite these reservations, the continued increase in severe incidents affecting even the most highly resourced companies resulted in more understanding that cyber risk is essentially inevitable. The innately dynamic and evolving nature of cyber threats meant that it is challenging to eliminate the risk entirely, and the substantial market size of $11.9 billion in 2022 noted above suggests a tangible demand for such a product.

The cyber insurance industry has also proven its ability to compensate and to pay claims. These increased with the accelerated expansion of attack surface owing to increased remote working during the pandemic. From 2018 to 2021, reported claims in the United States cyber insurance market grew 100 per cent annually. In the same period, of those reported claims, there was a 200 per cent annual increase in the number of claims with payment, reaching a total of 8,100 claims paid in 2021 (Fitch Ratings, 2022).

How cyber insurance supports the improvement of cybersecurity

A key benefit of cyber insurance is that it can encourage companies to improve their cybersecurity. When organisations apply for cyber insurance, they must fill out an application form or questionnaire. Traditionally, these application forms contained questions relating to the applicant's cybersecurity position such as, 'Do you have a business continuity plan in place?' By collecting responses to these questions, in addition to general information about the organisation (such as revenue, amount of personal data held), a cyber insurance underwriter can assess the exposure and risk of the organisation. Once a cyber insurance underwriter evaluates the cybersecurity controls and governance of a company, they can structure and price an insurance policy suitable for that organisation.

As cyber threats have become increasingly sophisticated, organisations have developed sophisticated IT infrastructure. It is becoming commonplace for insurance companies to have risk-assessment conference calls or on-site inspections to evaluate the cyber risks. In the case of larger companies, this has become a minimum requirement by insurance companies as part of the underwriting process. Thus, companies that apply for cyber insurance can become more aware of their exposure and any weakness in their cybersecurity controls. The insurance industry has valuable insights about cyber threats and loss information that other sectors may not have and can serve as a hub for knowledge exchange. Cybersecurity companies also leverage their services to assist policyholders in improving their risks in order to be more insurable.

As cyber insurance gains prominence, insurance companies have started to offer complementary services for insured companies to improve their cybersecurity. This creates a win-win situation. Organisations can benefit from additional risk-assessment perspectives and consulting, and insurance companies have a better understanding of organisations' cybersecurity policies and controls. Certain insurance companies incentivise cybersecurity improvements by offering more competitive terms and conditions to organisations with robust controls.

Some insurance companies go further in mandating certain cybersecurity controls as a prerequisite for cyber insurance cover. With an insurance quote offer, there can be 'subjectivities'. These are conditions that an applicant needs to fulfil such as a security control being implemented (Woods and Simpson, 2017). For example, if the applicant

responds in the insurance questionnaire that they do not have multifactor authentication, the insurance company could stipulate that, in order for the company to receive cyber insurance cover, they must implement such a system within six months after the inception of the policy. Incorporating subjectivities ensures that applicants' cybersecurity policies and controls achieve a level that insurance companies are comfortable to insure, meaning that applicants can obtain cyber insurance cover.

Cyber insurance will play a critical role in encouraging organisations to improve their cybersecurity standards. When – not if – an organisation is faced with a cybersecurity incident, cyber insurance provides the necessary resources for it to mitigate losses and to obtain indemnification for covered losses. Cyber insurance is not a replacement for improvements in cybersecurity. Organisations sometimes face budgetary decisions between investing in cybersecurity or obtaining insurance. However, they must continually demonstrate to insurers that they manage cyber risks effectively through robust governance.

Cyber insurance response to incidents

A significant benefit of having cyber insurance is that companies can access a claims service when there is an incident. Generally, insurance companies establish partnerships with various cybersecurity companies, incident response providers, and law firms with experienced legal practitioners capable of guiding victims of a cyber-attack through the cyber crisis. Often, there are also experts in cyber extortion incidents, who have intelligence about the various ransom tactics of different ransomware gangs, ensuring that companies take the best actions. In a ransomware scenario in which a company is at the mercy of hackers, having an expert who knows how to handle such situations benefits the company greatly. The expert can also advise, for example, that paying the ransom may not benefit the policyholder in certain situations.

Mandating cyber insurance?

On June 12 2018, the South Korean government passed an amendment to its Act on Promotion of Information and Communications Network Utilization and Data Protection (Network Act) (adopted on May 12, 1986). which required companies handling large amounts of personal information to have liability insurance that would compensate them in the case of a cyber incident (Yulchon LLC, 2019). Despite having a law that requires companies to have such cyber insurance, the take-up of liability insurance was lower than expected. Confusion about the amendment, minimal enforcement by the authorities, and a lack of growth in business discouraging insurance companies, have contributed to the lack of adoption (Kim, 2023).

If, and when, countries realise the need for risk management and transfer for such cyber risks to warrant mandatory insurance, the subsequent steps become crucial. Given the previous shortcomings in implementing data-protection and associated laws, achieving success in

mandating risk transfer would require awareness campaigns, meaningful regulatory actions for non-compliance, and clarity for companies about intent and consequences.

Challenges of cyber insurance

Cyber insurance, being a relatively new product, is open to more challenges than life, property and accident insurance. Data is relatively scarce given the newness of the product (Awiszus et al., 2023). Insurance companies employ actuaries who use historic data to try to model and price the expected loss associated with certain risks. The limited data about cyber insurance makes it challenging to use historical pricing methodologies and it often requires expert judgement. However, there is also a question about whether historical data can truly reflect future risks, especially for cyber risk. Technology's rapid evolution means new vulnerabilities and attack threats which may not be accounted for in historical data. The dynamic nature of cyber risk makes it a 'highly non-stationary' risk (Awiszus et al., 2023). One of the main reasons for this is that cyber risk is a manufactured risk. Unlike natural catastrophe risks like hurricanes, for which weather patterns can be analysed to estimate severity or location, for cyber risks, an individual cybercriminal's actions can create an entirely new threat. Therefore, even if historical data is available, its value in predicting the future behaviour of cybercriminals is questionable.

Related to data, cyber underwriters typically depend on 'yes' or 'no' answers in assessing cybersecurity risk. This is challenging. For example, a questionnaire may simply ask whether or not a company has a privacy policy. A positive response may not provide sufficient insight into the quality and appropriateness of the privacy policy, nor the company's procedures for reviewing, implementing and updating it. The need for efficiency in the insurance application process to enable distribution and reach, often leads to using binary questions instead of open-ended inquiries that could result in better insights. Understandably, SMEs prefer a streamlined process and may be discouraged if they need to have a lengthy risk-assessment call with an IT professional as part of the insurance application. Furthermore, the insurance company would need to weigh the resources and time invested against the value of a small insurance policy. There is a trade-off between efficiency and ensuring that enough risk information is captured. As a result, SME companies generally fill out shorter questionnaires related to their cybersecurity controls and governance, whereas large corporations may be subject to a full risk-assessment conference call.

Due to the limited number of questions which can be asked, every insurance company has its own cyber insurance application as priorities in risk assessment may be different. This results in a lack of standardisation and consensus on what information is critical for underwriting. The European Union Agency for Cybersecurity (ENISA) conducted a study of the cyber insurance questionnaire of the top ten cyber insurers, to assess how many unique questions were asked (unique meaning the question is asked by only one insurer out of the ten). The analysis found that there were 129 unique questions. Although there were some core questions and areas that all the questionnaires asked, there was still

a lack of standardisation in data required for underwriting (European Union Agency for Network and Information Security, 2017). This can cause confusion for policyholders if they are requesting insurance from different insurance companies, and facing different questions which may be relevant for only some insurers.

Controversies behind cyber Insurance

Despite its growing prominence, cyber insurance has also faced scrutiny and criticism. The nascent nature of the cyber insurance market, coupled with the rapid evolution of cyber threats, has resulted in a lack of standardisation in cover and wording. This adds to confusion for policyholders (Deloitte Center for Financial Services, 2017). As more cyber incidents occur, and thus both policyholders and insurance companies gain experience, there is an expectation that the cyber insurance market will eventually achieve greater clarity and standardisation.

There are also challenging views in the insurance industry about the product, with arguments about the insurability of the risk in itself due to, among other concerns, lack of data and accumulation scenarios resulting from the interconnectivity of the risk (Greco, 2022). Unlike property risks that can be physically bifurcated and quantified through zoning and addresses, computer systems, software and applications are connected remotely, and the risk is inherently intangible. The resulting cascading impact of an outage to a large interconnected system may have significant consequences that are challenging to quantify objectively.

In confronting a risk that persists for us and future generations, finding a solution becomes imperative. To do so, the cyber insurance industry needs to continue finding solutions which can be sustained in the long run.

Cyber war

A fundamental aspect of sustainability in insurance is ensuring that unquantifiable risks are eliminated, and that there is sufficient capital backing to support accurately assessed and quantified risks.

One of the largest unknown cyber scenarios to consider is cyber war. Cyber war is a complex topic, the definition of which even scholars and experts struggle to reach consensus (Ashraf, 2021). The most catastrophic scenario envisioned by many regarding cyber-attacks comes in the form of cyber warfare between nations. Imagine national telecommunication systems facing outages due to disruptive cyber-attacks; hospitals not being able to operate due to their systems being encrypted; and individuals not being able to access their finances because of an outage of national banking systems. In such a scenario, individuals, companies and nations themselves would face tremendous losses.

The crucial question arises: can the exposures of a cyber war also be shifted to insurance companies? In general, armed conflicts between nation states are by

their very nature a matter for governments, and it is for the state to intervene to mitigate the consequences of a war, for the population but also for the economy, as its consequences are so large and wide-reaching that private industry simply lacks the capital to support such a ruinous risk. Therefore, looking at conventional lines of insurance such as property and accident, insurance policies have long incorporated exclusion clauses for war risks, as the industry is generally incapable of accurately predicting the likelihood or severity of damage arising from war. It is, therefore, unable to charge the appropriate premiums (Kathy, 2022). This has resulted in specialist insurance markets for war for which limits of liability and corresponding conditions are carefully and conservatively managed.

Generally, insurance policies will contain a war exclusion that 'specifically excludes coverage for acts of war, such as invasions, insurrections, revolutions, military coups, and terrorism'. This also holds true for cyber insurance policies (Kagan, 2023). The magnitude of damage that would arise from cyber warfare would be so immense that the insurance industry would not be able to pay every policyholder sufficiently.

Merck, a large pharmaceuticals company, was affected by the NotPetya attack in 2017, involving 40,000 of its computers globally (Tilley and Poulsen, 2023). As a result of the attack, Merck claimed damages under its property 'all risk' policy which included affirmative cyber coverage. However, as NotPetya was allegedly connected to the Russian government, the insurance company tried to deny the claim by applying the war exclusion. As it was a property insurance policy, it had a general war exclusion, which read:

> 'A. 1) Loss or damage caused by hostile or warlike action in time of peace or war, including action in hindering, combating, or defending against an actual, impending, or expected attack:
>
> a) by any government or sovereign power (de jure or de facto) or by any authority maintaining or using military, naval or air forces;
>
> b) or by military, naval, or air forces;
>
> c) or by an agent of such government, power, authority or forces;
>
> This policy does not insure against loss or damage caused by or resulting from Exclusions A,B, or C, regardless of any other cause or event contributing concurrently or in any other sequence to the loss.' (Tilley *et al.*, 2022)

Essentially, the courts found that conventional war exclusion could not be relied upon by the insurers. The insurers submitted that the NotPetya attack was state-backed with 'ill will or a desire to harm' which would be applicable to the 'hostile/warlike' part of the war exclusion (Liu, 2023). However, the courts opined that the insurers were 'stretching the meaning of "hostile" to its outer limit', and that the attack 'is not sufficiently linked to a military action or objective as it was a non-military cyberattack against an accounting software provider' (Liu, 2023).

The case of Merck was pivotal in demonstrating how a traditional war exclusion may not be clear enough in the context of cyber-attacks. Cyber insurance policies, in general, have adopted the same war exclusions as those of traditional property policies. However, given the decisions of the judge in the Merck case, it clearly shows that, for war exclusions to function as intended for the purposes of eliminating cyber warfare scenarios, further clarification of the exclusionary language would be needed. This has sparked many discussions within the cyber insurance industry on how to appropriately exclude cyber war exposures in order to achieve a sustainable risk transfer solution for the market.

In 2022, Lloyd's, which is one of the world's largest insurance marketplaces, published a bulletin outlining minimum requirements for what it considered a robust cyber war exclusion:

1. 'Exclude losses arising from a war (whether declared or not), where the policy does not have a separate war exclusion
2. (Subject to 3) exclude losses arising from state backed cyber-attacks that (a) significantly impair the ability of a state to function or (b) that significantly impair the security capabilities of a state
3. Be clear as to whether cover excludes computer systems that are located outside any state which is affected in the manner outlined in 2(a) & (b) above, by the state backed cyber-attack and
4. Set out a robust basis by which the parties agree on how any state backed cyber-attack will be attributed to one or more states
5. Ensure all key terms are clearly defined' (Lloyd's, 2022).

Today, many insurance companies have started to update their war exclusions in accordance with the above, knowing that traditional war exclusions that are found on other insurance policies do not work for cyber insurance policies. Munich Re, one of the largest reinsurers in the world, has stated that clear and transparent cyber war exclusions are one of the cornerstones of a sustainable cyber marketplace (Shi and McNestrie, 2023). Critical components are clarity in policy language and ensuring uninsurable risks such as war are excluded.

Government and cyber insurance

Governments play a key role in increasing awareness of cyber insurance and fostering a nation in which individuals and organisations are well-protected. As shown in the case of South Korea, one method is to make cyber insurance compulsory for organisations. However, this is not the only method, and it requires strong enforcement to ensure it is effective. General regulations related to data protection, not specific to cyber insurance, can still be effective in stimulating the growth of cyber insurance. For example, demand for cyber insurance across Europe increased after the introduction of the GDPR in 2018

(IFSEC Insider, 2020). With strict data regulations that govern data privacy and create meaningful regulatory consequences for companies that do not comply, this increases awareness in companies that they need to manage their cyber risks appropriately.

Governments can also engage with the insurance industry to identify how a sustainable cyber insurance market can be created. Singapore launched its Cyber Risk Management Project in 2016, in which part of the ambition was to support cyber risk underwriting and pricing in order to create a sustainable domestic cyber insurance market (Wolff, 2022). The government worked jointly with the insurance industry, which led to the announcement in 2018 of the world's first commercial cyber risk pool in Singapore (ibid). The idea was to create more transparency and consistency in order to price cyber risks accurately, incentivising more purchasing by companies.

Another role for governments in fostering a more sustainable cyber insurance market is in data collection. The existing lack of standardisation in data collection poses challenges for insurers striving to gather meaningful and accurate data. Governments could establish data standards or minimum requirements to enhance transparency in risk information, thereby optimising efficiency (Woods and Simpson, 2017).

Governments could address these shortfalls by working with the industry to ensure adequate cybersecurity data is available and transparent for accurate pricing and modelling for cyber risks. This data-driven approach allows for more in-depth analysis. For example, it could determine which cybersecurity controls are most effective for preventing ransomware trends by comparing differences in controls between those companies that have filed a ransomware claim and those that remain incident-free.

Conclusion

Cyber-attacks are inevitable. Therefore, cyber resilience and risk mitigation are fundamental for the successful digitisation of the economy. As more sophisticated cyber-attacks emerge, the demand for cyber insurance will continue to increase. As a result, cyber insurance will play an increasingly critical role in delivering a meaningful risk transfer solution, to enable organisations to continue operating and innovating. Cyber insurance should not be the first line of defence against cyber criminals, just as fire insurance does not prevent fires. However, for fire insurance, policyholders usually implement safety measures to mitigate risk and to be eligible for cover, giving policyholders peace of mind and the assurance that they will be covered if there is a fire.

The public sector needs to play an active role in this ecosystem to ensure that the various stakeholders adequately manage their cyber risks, as this relates to national security. It is incumbent on the insurance industry, governments and the private sector to collectively understand and face the challenges of cyber risks in order to proactively address these and to ensure security against cybercrime for this generation and for future generations.

References

Ashraf, C. 2021. Defining cyberwar: towards a definitional framework. *Defense & Security Analysis,* 37(3), pp. 274–294.

Awiszus, K., T. Knispel, I. Penner, G. Svindland, A. Voss and S. Weber 2023. Modeling and pricing cyber insurance. *European Actuarial Journal*, 13, pp. 1–53.

Deloitte Center for Financial Services, 2017. *Demystifying cyber insurance coverage: clearing obstacles in a problematic but promising growth market.* s.l.: Deloitte University Press.

Deloitte, 2019. *Overcoming challenges to cyber insurance growth.* New York: Deloitte.

European Union Agency for Network and Information Security, 2017. *Commonality of risk assessment language in cyber insurance.* Heraklion: ENISA.

Fitch Ratings, 2022. *US Cyber Insurance Payouts Increase Amid Rising Claims, Premium Hikes.* [Online] Available at: https://www.fitchratings.com/research/insurance/us-cyber-insurance-payouts-increase-amid-rising-claims-premium-hikes-06-05-2022 [Accessed 20 November 2023].

Greco, M. 2022. *Cyber attacks set to become 'uninsurable'.* [Interview] (22 December 2022).

Holot, J. and M. Lelarge 2008. *Cyber Insurance as an Incentive for Internet Security*. Seventh Workshop on the Economics of Information Security.

HYPR, 2023. *Notpetya. Five Facts to Know About History's Most Destructive Cyberattack.* [Online] Available at: https://www.hypr.com/security-encyclopedia/notpetya [Accessed 13 November 2023].

IBM, 2023. *Cost of a Data Breach Report 2023.* Armonk: IBM.

IFSEC Insider, 2020. *Two years on from GDPR: Has it driven growth in cyber security insurance?* [Online] Available at: https://www.ifsecglobal.com/cyber-security/two-years-on-from-gdpr-has-it-driven-growth-in-cyber-security-insurance/ [Accessed 19 November 2023].

Institute of Risk Management, 2023. *Cyber risk.* [Online] Available at: https://www.theirm.org/what-we-say/thought-leadership/cyber-risk/ [Accessed 13 November 2023].

Kagan, J. 2023. *What Is a War Exclusion Clause in an Insurance Contract?* [Online] Available at: https://www.investopedia.com/terms/w/war-exclusion-clause.asp [Accessed 19 November 2023].

Kathy, D. 2022. *Does your insurance cover war?* s.l.:s.n.

Kim, Y.-m. 2023. *Why is the 'cybersecurity insurance product' market so weak in Korea?* Bo-an News, 3 April.

Kostka, C. 2022. *The First Ransomware Attack: Lessons Learned from History,* s.l.: Ransomware.org.

Lieberman, M. 2017. Mind The Trust Gap: How Companies Can Retain Customers After A Security Breach. *Forbes*, 8 December.

Liu, A. 2023. *Merck entitled to $1.4B in cyberattack case after court rejects insurers' 'warlike action' claim.* [Online] Available at: https://www.fiercepharma.com/pharma/merck-entitled-14b-payout-cyberattack-case-after-judge-refutes-insurers-warlike-action-claim [Accessed 19 November 2023].

Lloyd's, 2022. *State backed cyber-attack exclusions.* London: Lloyd's Market Bulletin.

Market.us. (2024, January). Global Cyber Insurance Market By Insurance Type. Available at: https://market.us/report/cyber-insurance-market/

Mckinsey, 2022. New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers. *Mckinsey*, 27 October.

Munich Re, 2022. *Munich Re Global Cyber Risk and Insurance Survey 2022,* Munich: Munich Re. Available at: https://www.munichre.com/landingpage/en/global-cyber-risk-and-insurance-survey-2022.html [Accessed 17 November 2023]

One Identity, 2024. *What is attack surface expansion?* [Online] Available at: https://www.oneidentity.com/learn/what-is-attack-surface-expansion.aspx#:~:text=An%20attack%20surface%20is%20the,complexity%20of%20these%20entry%20points [Accessed 20 February 2024].

Richardson, R. and M. North 2017. Ransomware: Evolution, Mitigation, and Prevention. Georgia: *International Management Review,* 13(1)

Shi, C. and A. McNestrie 2023. Munich Re takes hard line on narrower cyber war exclusions. *Insurance Insider,* 19 May.

Tilley, H. and L. Poulsen 2023. *Cyber Attack Not Within War Exclusion.* London: Carter Perry Bailey.

Tilley, H., S. Zaozirny and S. Carter 2022. *It's war but not as we know it?* London: Carter Perry Bailey.

Trend Micro. (2024, March 19). Ransomware. Retrieved from Trend Micro: https://www.trendmicro.com/vinfo/us/security/definition/ransomware

Wolff, J. (2022). *Cyber-Insurance policy: Rethinking international risk for the Internet age*. Cambridge: MIT Press.

Woods, D. and A. Simpson 2017. Policy measures and cyber insurance: a framework. *Journal of Cyber Policy,* 2(2).

Yulchon LLC, 2019. Amendments to the Network Act Coming into Effect in 2019. *Lexology*. [Online] Available at: https://www.lexology.com/library/detail.aspx?g=fa96ac52-003b-4ec9-92b0-22fd0e8c1192 [Accessed 18 November 2023].

About the authors

Serene Chan leads Munich Re's Cyber service offering in the Asia-Pacific region, being one of the founding members of the local set-up since 2018. Prior to joining Munich Re, Serene was working on the primary side at Lloyd's of London, underwriting large US corporate cyber and intellectual property business. Serene is a Barrister-at-law of England and Wales, and is a member of the Lincoln's Inn of London. She is originally from Malaysia and moved to the UK to complete her A-levels, after which she graduated from the King's College London School of Law.

Eric Cho is a Senior Cyber Underwriter at Munich Re, currently based in the Tokyo office. He joined Munich Re in 2020 in the Singapore office, and also spent a year in the South Korea office. Prior to Munich Re, he worked at AIG in Canada, underwriting financial lines for the Western Canada region. Eric graduated from the University of British Columbia with a Bachelor of Commerce (Honors), specialising in accounting and operations and logistics.