مجلة جامعة الشارقة للعلوم القانونية

جامعة الشارقة
UNIVERSITY OF SHARJAH

University of Sharjah Journal of Law Sciences

A Refereed Scientific journal

Vol. 22, No. 1
Ramadan 1446 A.H. / March 2025 A.D.

ISSN : 2616-6526

University of Sharjah Journal for Law Sciences, Volume 22, No. 1 March 2025

https//:doi.org/10.36394/jls.v22.i1.20

Opportunities for Cyber Insurance to Address the Challenges of Cyber Attacks: Repercussions for SMEs

Khalaf Albalawi(1)

Received on: 07-06-2024 **Accepted on: 04-12-2024**

Abstract:

The cyber insurance market has doubled in just two years reflecting how highly ranked cyber risks are within risk reports for all organisations, corporations, businesses and enterprises. Cyber risk is predicted to remain the main critical risk for organisations and enterprises up until 2026. The insurance industry has been recognised as playing a crucial role in promoting advancements in cyber security, which is advantageous to policymakers and insurers alike. Tremendous opportunities are possible for the insurance industry due to an increasingly expanding digital economy. Nevertheless, there are still significant risks with the primary challenge in this market being the identification and quantification of such risks. This paper explores the history of cyber insurance, the issues that may face insurers and policyholders alike, and how insurance can help to strengthen cybersecurity via enhancing resilience and lessening the impacts of cyber-attacks. It will give some examples of good practice at present in the market and culminate with some recommendations.

Keywords: Cyber Insurance, Cyber Security, Risk Challenges, Small-to-Medium Enterprises (SMEs), Moral Hazard.

(1) Law School - Tabuk University (Tabuk – K.S.A.)
Km.albalawi@ut.edu.sa

1. Introduction

Many insurance companies only began to understand cyber insurance in recent years, as their focus was on other lines of insurance. The application of cyber insurance is a measure to potentially allay the effects of cyber risk. Interest in cyber risk is longstanding, but in recent times, its importance has notably expanded, resulting in a rise in commercial and governmental interest. This is a consequence of the fact that financial responsibility connected to a cyber event or attack, can be transferred by organisations because of cyber insurance. Furthermore, cyber insurers may, in effect, strengthen cyber-security practices by incentivising improved risk management, for instance, by offering discounts for the application of security measures, or higher standards, or improved assistance in cyber-security that may be unobtainable to some organisations. According to the European Network and Information Security Agency (ENISA):

Cyber insurance refers to the insurance contracts having the purpose of covering a broad range of issues relating to risks in cyberspace. Researchers have identified contracts as covering things like: liability issues, property loss and theft, data damage, loss of income from network outage and computer failures or website defacement.

Large-scale cyber risk is easier for cyber insurers to manage, due to the inherent financial incentive to reduce claims and losses.(1)

Media coverage on cyber insurance has been generally negative, particularly regarding its asserted failure to compensate claims received

(1) Sullivan, N. and Nurse, J.R.C. (2020). Cyber Security Incentives and the Role of Cyber Insurance. Royal United Services Institute for Defence and Security Studies. Emerging Insights Paper. Accessed Online: https://rusi.org/publication/emerging-insights/cyber-security-incentivesand-role-cyber-insurance

and its contribution to the serious issue of ransomware. Furthermore, the rise in insurance premiums, and the triggering of some insurance companies leaving the market can be seen as results of the financial harm produced by ransomware incidents.(1)

1. This paper is structured as follows:
2. An overview of cyber risks and the advent of cyber insurance
3. Compatibility of cyber risks for insurance with global and legal goals
4. Cyber security regulation in the EU
5. Challenges in cyber insurance
6. The impact of cyber insurance on security practices
7. The challenges of cyber insurance in light of other insurance lines
8. Policy gaps in cyber insurance
9. The implications of cyber insurance for small-to-medium enterprises (SMEs)
10. Cyber risk insurance approaches in the risk management of SMEs
11. The potential of insuring against cyber risk
12. Coordinated governance for cyber insurance
13. Insurance tools for cyber risk and strategies for inclusion into legislation
14. Findings and conclusions
15. recommendations

(1) Kuru, D. and Bayraktar, S. (2017). "The effect of cyber-risk insurance to social welfare." Journal of Financial Crime, 24(2), pp. 329-346.

This paper explores whether cyber insurance can act as a trigger for encouraging stronger cyber-security methods and practices, and hence the paper focuses on two questions:

- Can cyber insurance be a motivating agent for enhanced cyber-security methods and behaviours?
- If so, what approaches could be engaged to encourage these positive effects more successfully?
- In addition to answering these questions, the paper considers the prospective negative effect of cyber insurance on cyber security. The methodology consists of undertaking an in-depth assessment of available literature, in addition to data-gathering and the evaluation of key insurance policy and legislation sources.

2. An Overview of Cyber Risks and the Advent of Cyber Insurance

Cyber insurance allows companies to transfer a proportion of financial responsibility connected to cyber incidents to an insurance provider. It is created to offer businesses a safeguard against possible financial damage and legal responsibilities that may be encountered, including costs sustained by the company. Global economic volatility, geopolitical conflicts, climate crises, energy vulnerabilities, cyber-attacks are but a few of the challenges that face the global economy at present.(1)

Insurers have a role in maintaining economic resilience via various means Europe has also borne the brunt of these challenges, yet its financial

(1) Jean Bolot and Marc LeLarge, 'Cyber Insurance as an Incentive for Internet Security', in M Eric Johnson (3rd ed.), Managing Information Risk and the Economics of Security (New York, NY: Springer, 2009). pp. 269–90.

services sector has generally stood the test of time. Insurance is about residual risk and putting things in place to handle potential problems when the unexpected happens, insurance will come into play. In cyber insurance, a business or enterprise purchases a policy, akin to how one would buy a car or home insurance policy and then in the event of a business having its data or systems breached or lost via a cyber-attack, the insurance company would assist. This may be in the form of facilitating the enterprise to get in touch with data forensics, incident report companies, public relations side and also regulations based on where the enterprise and its customers are located. All of this depends on the insurer.(1)

Furthermore, it is viewed as a key strategy for a business to limit cyber risk. Cyber risk is a concept that covers many factors posing threats to an individual's, company's or government's technology and information assets. Among the range of risks are business disruption, critical information leaks, identity theft and cyber-attacks. Rawlings, writing in 2015, brought attention to how insurance policies in the London market at the time often excluded liability for cyber risk. Rawlings also noted that the US insurance industry was ahead of the curve in comparison to the UK context when it came to insuring cyber risk.

It is also important to differentiate between *non-criminal* disruptions, like blackouts, loss of power and natural disasters, and *criminal* causes of cyber disruption such as doxing, phishing attacks, extortion, hackers and scammers. Cyber risk can also include a range of specific risks that relate to the use of computers, IT and virtual reality.(2)

(1) Ibid p.270.

(2) Middleton, K. and Kazamia, M. (2016). "Cyber Insurance: Underwriting, Scope of Cover, Benefits and Concern." Pierpaolo Marano, Ioannis Rokas and Peter Kochenburger (eds.),

Insurance companies can offer further services to boost cyber-security assistance. These services are equally advantageous to the insurance company since their intention is to improve the insurer's own risk profile. A wide range of assistance is available, from evaluating cyber-security risks and accessing, to offering consultant advice on enhancing the company's overall cyber-security situation. Moreover, further services are available to businesses in case of a security incident.(1)

It is possible to purchase cyber insurance either as an individual policy, which covers cyber risks alone, or included in a comprehensive insurance package encompassing a variety of risks. Specific specialised cyber insurance policies are frequently more expensive but offer the possibility of higher financial compensation in the face of damage. Additionally, they frequently apply the use of cyber-risk tools, which are designed to enhance cyber security. On the other hand, cyber insurance policies included in a comprehensive policy can be attractive as they are both simple and lower in cost.

3. Compatibility of Cyber Risks for Insurance with Global and Legal Goals

In the context of the US, which was ahead of the UK and the EU when it came cyber insurance, several precautions were taken to stop cyber-attacks and safeguard personal data. Initially, to develop and carry out a national policy to safeguard key facilities against cyber threats, former President

The "Dematerialized" Insurance: Distance Selling and Cyber Risks from an International Perspective. Cham, Switzerland: Springer. 185-201.

(1) Bolot, J., and Lelarge, M. (2009). "Cyber Insurance as an Incentive for Internet Security." M Eric Johnson (ed.), Managing Information Risk and the Economics of Security. New York, NY: Springer, Third Edition. 269–90.

Bill Clinton formed the Commission of Critical Infrastructure Protection in 1996. Then the Federal Gramm-Leach-Bliley Act of 1999, also known as the Financial Services Modernization Act obliged financial institutions (such as car dealers and retailers who offer credit, insurance companies, credit unions and banks) to make known information-sharing systems with consumers and safeguard sensitive information.(1)

Due to cyber risks facing these financial institutions in the US, in 2015 the Financial Industry Regulatory Authority (FINRA) and SEC produced some guidance advising these companies on their cyber security postures and resilience. These regulations and laws in the US were designed to prevent cyberattacks and lessen their impact when they do happen. However, none called for the disclosure of uniform information across organisations in a manner that can generate insightful data for competitors, clients, the general public and legislators.(2) The New York State DFS enforces what is arguably the most extensive set of regulations. It recently mandated, since 2017, that companies have a cyber security program in place.

In the EU, in order to safeguard people and increase consumer confidence through regulation of personal data, the EU began concentrating on the information security issue in 1995 with the European Data Protection Directive. In 2014, GDPR was brought in by the European Council and shortly afterwards, it founded the European Data Protection Board (EDPB) in2015.(3)

(1) Erkan-Barlow, A. and Wells-Dietel, B.P. (2023). "The Current State of Cyber Insurance and Regulation in the Context of Investment Efficiency and Moral Hazard: A Literature Review." Journal of Insurance Regulation, 42.

(2) Ibid p.44.

(3) Cyber risk. The emerging cyber threat to industrial control systems, Report by Lloyd's & Guy Carpenter, https://assets.lloyds.com/media/542bea95-0d28-4ce1-

In 2019, the EU passed the EU Cybersecurity Act, effective since 2021, and created the EU Cybersecurity Agency (ENISA). A cybersecurity certification system for goods, services, and procedures was introduced by the EU Cybersecurity Act. This certification aids businesses in responding to and recovering from cyber disasters as well as in preventing and detecting them. More on this will be discussed in the following section.(1)

Erkan-Barlow and Wells-Dietel bring attention to the Hiscox (2022) *Cyber Readiness Report* presents a contrasting picture, despite the EU's seeming stricter stance on cybersecurity and data protection. A few key figures from this report are broken down by nation in Table 1. The Netherlands, Ireland, and the United States saw the biggest rises in the percentage of businesses that suffered a cyberattack, while France, Belgium, and Germany saw the fewest increases. Spain is experiencing a minor downturn. A similar pattern can be seen when examining the median cost of cyberattacks. Once more, France and Germany are seeing a fall, while the Netherlands, Ireland, and the United States are seeing the biggest increases. All things considered, ransomware assaults increased most in the Netherlands, Spain, and France, decreased in France, and increased least in Germany and Ireland. In the United States, the proportion of companies that suffered a ransomware assault was constant. Regarding the adoption of cyber insurance, the figures vary from 58 to 69 percent; nevertheless, the United States, Germany, Spain, and Ireland seem to be depending more on risktransfer.(2)

a603-63db54aa24f9/The%20Emerging%20Cyber%20Threat%20to%20Industrial%20Control%20Systems_ Final%2016.02.2021.pdf [access: 4.12.2023]. p.46.

(1) Ibid p.48.

(2) Erkan-Barlow, A. and Wells-Dietel, B.P. (2023). "The Current State of Cyber Insurance and Regulation in the Context of Investment Efficiency and Moral Hazard: A Literature

Cyberattacks in the US, along with car hacking and identity fraud, are the main threats. While the most worrisome threats in the EU are ransomware, supply chain assaults, and phishing.(1) According to these figures, cyber incidents happen even in European nations with stricter laws, demonstrating that cybersecurity is a global issue. Despite having conflicting views on data security and privacy, the US and the EU began working together to stop ransomware attacks and released a joint declaration in 2021. However, cyberattacks continue to pose a problem for companies worldwide. The most notable finding from Table 1 is that, among other things, just 25% of IT budget is devoted to cybersecurity, and there is a significant reliance on risk transfer through the purchase of cyber insurance.(2)

4. Cyber Security Regulation in the European Union

The European Union (EU) began to focus on data security with the enactment of the European Data Protection Directive in 1995. This directive was designed to protect individuals and improve customer confidence by managing the administration and free use of personal data. In 2011, a proactive approach to the data privacy issue was taken, with the release of opinion statement about the launch of a broad strategy aiming to protect personal data. In 2014 the General Data Protection Regulation (GDPR) was enacted, and in 2015 the European Data Protection Board (EDPB) was founded, with the aim of guaranteeing standardized application of the GDPR across the EU.(3) Later, in 2016, the GDPR went into effect, bringing

Review." Journal of Insurance Regulation, 42.

(1) Nuvias. (2023). Cybersecurity Perspectives: Europe vs. USA. https://www.nuvias.com/en-us/cybersecurity-perspectives-europe-vs-usa/. p.28.

(2) Ibid p.29.

(3) Ibid p.20.

with it a host of new and existing data protection rights, such as the ability for people to ask for the deletion of their personal information from the systems used by collecting organisations.(1)

GDPR introduced a variety of data-protection rights. One right permits an individual to request their personal data to be erased from the systems of any business that has gathered it. In 2017, two new regulations were introduced, obliging companies to apply security measures to protect personal data and allowing only essential personal data to be processed, and even then, only for a designated reason. Member countries were obliged to enact the Data Protection Directive into their national legislation by 2018. Companies were required to create data and communication systems, ensure technology obeyed privacy standards and include data-protection measures. After a two-year grace period, the GDPR was formally established as the authorised EU framework, replacing the 1995 Data Protection Directive.(2)

Since May 2018, the GDPR has ruled that companies engaging in wide-ranging handling of sensitive personal data must specify a data protection officer. As stated in the directive, the operator of essential services (OES) must implement the required technical and organisational security procedures and inform state authorities about any substantial incidents. In addition, member countries must create a national contact point in order to cooperate with other member states and create 'computer security incident response teams. Furthermore, states must offer clear instructions to the OES to address weaknesses, assess the compliance of other member states, and

(1) Nuvias. (2023). Cybersecurity Perspectives: Europe vs. USA. https://www.nuvias.com/en-us/cybersecurity-perspectives-europe-vs-usa/. p.28.

(2) Adamski, D. (2021). "Lost on the Digital Platform: Europe's Legal Travails with the Digital Single Market." Common Market Law Review, 55. 27.

require them to provide data, including evidence of execution. Providers of digital services are also required to fulfil the same security and reporting requirements as the OESs.(1)

The establishment of EU Cybersecurity Agency (ENISA) and the EU Cybersecurity Act, adopted in 2019, was put into practice in 2021.(2) The Act applied an accreditation system for products, services and processes in the cyber security field. This accreditation helps companies to practically recognise and prevent cyber incidents, in addition to enabling them to quickly respond to and recover from incidents. Any company undertaking business in the EU zone must obtain a product or service accreditation. This requirement also includes companies located in the United States. The certificate, recognised across the EU, enables cross-border business. The GDPR framework imposes large penalties for breaches of data protection. Intended to deter, the penalties imposed are proportionate to the offence, with a range of €10 million to €20 million being imposed. A company, however, might find a penalty of 2–4% of its global revenue imposed, dependent on the scale of the offence. Financial penalties are an additional method or an alternative to disciplinary measures, aiming to bring data processing into accordance with the GDPR. Penalties may also include limitations on a company, such as a ban on data processing.(3)

5. Challenges for Cyber Insurance

Additionally, the fluctuating characteristics of cyber threats create challenges in forecasting the required insurance coverage; problems may

(1) Ibid p. 29.

(2) ENISA (2019). "Consultation Paper – EU ICT industrial policy: breaking the cycle of failure." European Agency on Cybersecurity, p 12.

(3) Ibid p. 14.

arise in accurately pricing premiums as a consequence of insufficient data. Thus, finding a balance between clients' risk tolerance and their financial capabilities becomes problematic. Issues may also arise in communicating the measurable benefits of insurance to potential clients in an intelligible manner.(1) Yet despite that, Wolff has noted that cyber insurance policies have been more profitable for US insurers than other lines of insurance. Besides ransomware attacks, cyber insurance provides coverage for scams, identity theft and data breaches.(2)

The challenge of quantifying the benefits of cyber insurance is potentially deepened by a prevailing lack of knowledge concerning the specific events that cyber insurance policies can cover. It is becoming apparent that organisations often do not understand the specific coverage of their insurance policies. Reasons for insurance claims vary, from individual errors to being accidentally subjected to hostile actions from antagonistic states. Some parties falsely believe that other insurance categories will cover costs occurring from a cyber-attack. The relative infancy of the industry makes it difficult to locate previous case studies explaining incidents and the subsequent financial damages.(3)

As an illustration, UK data point towards cyber insurers largely fulfilling their contracts. The Association of British Insurers gauges that 99% of claims were settled in 2022. This results from a total of 207 cyber

(1) Ibid p. 26.

(2) Wolff, J. (2022). Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches and Cyber Attacks. Cambridge, Massachusetts: The MIT Press. p. 21.

(3) Woods, D.W. and Moore, T. (2019). "Does Insurance have a Future in Governing Cybersecurity?" Security and Privacy 18(1), p.18. Accessed October 2024: https://www.danielwoods.info/assets/pdf/DW2020_governance_IEEESP.pdf

claims stated and resolved in 2022 and displays a notable claim acceptance percentage within the industry.(1) In comparison, the Association of Insurance Commissioners in the USA found that a mere 28.4% of 9,107 claims in 2021 led to a payment. The lack of clear evidence in either result emphasizes the perception of cyber insurance that insurers encounter regarding prompt claim payouts. Widespread media coverage of insurance firms failing to offer compensation maintains the common belief that cyber insurance companies are unwilling to resolve claims. Moreover, many companies are unaware of their vulnerability to cyber threats, seeing a cyber insurance policy as a poor use of funds. The intangible attributes of a cyber event create issues for potential customers in evaluating the value of cyber insurance compared with the benefits of fire or flood insurance. Research suggests that companies frequently purchase cyber insurance proactively after a serious incident that has negatively impacted either the company or their counterparts.(2)

The challenges in regulating insurance premiums, the paucity of detailed information on coverage, anxiety about insurers' reluctance to offer compensation after a cyber event and the incomplete sense of risk seen with companies are all factors in the poorer-than-expected uptake in cyber insurance within the cyber community, in spite of insurance companies highlighting the significance of cyber risks. These are a few of the many factors leading to the reduced uptake of cyber insurance to date. There is still work to be done on enhancing confidence in cyber insurance products and highlighting the benefits, particularly security-related benefits.(3)

(1) Lemnitzer, J. (2021). "Why Cybersecurity Insurance Should Be Regulated and Compulsory." Journal of Cyber Policy, 6(2), 118-136.

(2) Bolot, J., Lelarge, M.: Cyber insurance as an incentive for internet security. In: Managing information risk and the economics of security, (2009). pp. 269–290

(3) Ibid p. 273.

6. The Impact of Cyber Insurance on Security Practices

It could be said that the desire to minimise the frequency of cyber incidents is the spur to cyber insurers as this would reduce the number of claims received and minimise the compensation paid to clients. While many businesses see cyber incidents as improbable but major events, studies suggest that such events occur frequently and are a key part of a cyber insurer's approach to business. Clients with a larger budget can employ full-time cyber-security experts, to reduce their cyber risk, but SMEs frequently find these services too expensive to employ an expert internally.(1)

Cyber insurers can aid clients by creating expert teams to reduce risk and provide customers with specialised knowledge to assist them before, during and after an incident. These teams may include specialists in forensics and breach counsel, in addition to PR and other areas of cyber risk. Cyber insurance coverage allows organisations to access this information and critical services. It is important to understand that organisations maintain this degree of security even if the recommendations made by insurers are notfollowed.(2)

Cyber insurance is thought to motivate organisations to assess their level of cyber risk. Cyber insurers can contribute to this, by creating clear standards of cyber security, and thus advocate for greater recognition of risk management. Insurance firms can both improve organisations'

(1) Abrams, (2020, September). "Cyber Insurer's Security Scans Reduced Ransomware Claims by 65%." Bleeping Computer, 22 September 2020. Accessed Online: https://www.bleepingcomputer.com/news/security/cyber-insurers-security-scans-reduced-ransomware-claims-by-65-percent/

(2) Ibid p.16.

understanding of their weakness and offer continuing reviews of the potential risk to support them. Cyber insurers can offer expert knowledge and information to improve customers' understanding of risk management. Using relevant information and data, cyber insurers can accumulate a mass of information on the various types of cyber risk that companies can face.(1) Consequently, they are able to create detailed simulations that can clarify and evaluate many cyber risk factors. These simulations help identify the most efficient management processes, despite the fluctuating nature of the industry and the ever-evolving risks, which both hinder the collection of data. Thus, steps have already been taken by insurers to create products and services that positively allay cyber risk.(2)

Measures are available to gauge and assess insufficient cyber security and potential risks. Insurance conditions guarantee that preliminary steps are frequently reviewed and renewed to meet contractual obligations. Businesses can be encouraged to apply cyber-security measures to prevent possible losses stemming from a lack of necessary safety practices required by insurance. Cyber insurance must not neglect to discuss the question of ransomware and payments to cyber criminals. There is currently a debate as to whether cyber insurers are *indirectly* encouraging ransomware payments,(3) leading to a rise in the frequency of ransomware attacks.(4)

(1) Principles for Board Governance of Cyber Risk, Insight Report, World Economic Forum, March 2021, p.21 http://www3.weforum.org/docs/WEF_Cyber_Risk_Corporate_ Governance_2021.pdf [access: 27.11.2023]

(2) Ibid p. 23.

(3) Halikias, H. (2024). Digital Shakedown: The Complete Guide to Understanding and Combating Ransomware. Cham, Switzerland: Springer.

(4) MacColl, N., Sullivan, J. Nurse, J.R.C., Turner, S., Mott, G., Cartwright, E. and Cartwright, A. (2023). Cyber Insurance and the Cyber Security Challenge. London: RUSI. Accessed

Case studies illustrating the positive results of cyber insurance are lacking. The existing evidence is predominantly hypothetical and assumes that buying a policy will result in improved cyber-security behaviours. Detractors can highlight the incomplete uptake of cyber insurance, the absence of clarity in defining what constitutes 'excellent' security procedures, the drivers for a reduction in insurance rates and conditions, and the prospect that cyber insurance could inspire reckless security practices. As stated, the uptake of cyber insurance has been considerably smaller than expected, creating particular issues for SMEs. Fluctuating policy cost is a disincentive for SMEs. Insurers offer lower prices to businesses that demonstrate strong cyber-security systems, but these discounts are generally eclipsed by other concerns, including the overall policy cost. Businesses may see the policy premium and decide (often wrongly) that their cyber risk is not serious enough to be worth the price. In addition, ambiguity remains concerning the definition of 'good' cyber-security practices.(1)

Furthermore, cyber-security standards and the application of limits or controls by organisations can affect policy underwriting. However, security control requirements differ between cyber insurers when approving coverage. For instance, several recognized structures exist around the world, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and Cyber Essentials in the UK. While parallels exist between the structures, so do variations, especially regarding the assessment achievement criteria. Cyber Essentials is a UK government-backed programme. However, it has been argued that it is

Online: https://static.rusi.org/OP-cyber-insurance-ransomware-challenge-web-final.pdf

(1) S. Romanosky , "Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?" Journal of Cybersecurity (2021). p. 18.

merely a superficial method of cyber security box ticking, which could have poor cyber security consequences.(1)

A further issue concerns market incentives and to what degree cyber insurers systematically gauge the purchaser's cyber-security situation before coverage is offered. With the growth of the cyber insurance market, insurers are facing increased competition for customers, theoretically resulting in lower costs. These lower costs may lead to a fall in the quality of required criteria (specifically evidence of existing security procedures), and also an inferior level of difficulty in purchasing insurance. In such an event, insurers will lack the motivation to encourage higher levels of cyber-security, and insurers who maintain higher prices may doubt their cost-effectiveness. This trend has been described by some commentators as a 'race to the bottom',(2) yet on the other hand falling cyber insurance rates represent how organisations and businesses are improving security and the competitive cyber insurance market at present.(3)

Woods and likewise Shetty ,(4) have discussed how the purchase of cyber insurance coverage may lead to organisations and companies being less likely to maintain secure behaviour. This is a trend known as 'moral hazard'. Research has demonstrated that companies are more likely to

(1) Talesh, S.A. (2018). Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as Compliance Managers for Businesses. Law And Social Inquiry, 43(2).

(2) Dambra, S., Bilge, L., Balzarotti, D. (2020). "SoK: Cyber insurance? technical challenges and a system security roadmap." 2020 IEEE Symposium On Security And Privacy (SP), pp. 1367-1383.

(3) Ibid p.1381.

(4) Shetty, N. Schwartz, G., Felegyhazi, M. and Walrand, J. (2010). "Competitive cyber-insurance and internet security." Proceedings of Workshop of Economic Information Security (WEIS) 2010, p. 229–47.

avoid assigning resources to risk prevention if they consider that any potential incidents that occur, will be addressed and covered by their cyber insurance coverage. The phenomenon of the 'moral hazard', which suggests riskier behaviour among covered groups, also applies to the wider insurance industry. Consequently, there is a likelihood of a rise in insurance costs, thereby increasing the monetary load on organisations that invest in both security processes and insurance. A further issue lies in uncertainty regarding security controls, and the paucity of information regarding the most effective current security procedures. Hence, there may be a lack of intelligible information regarding essential measures needed to alleviate the risks of moral hazard.(1)

Discussion continues concerning to what extent government involvement is necessary in the cyber insurance business, to increase a nation's ability to resist and recover from potential cyber risks. The enactment of strong measures could mean cyber insurance becoming a legal requirement, comparable to vehicle and employee liability insurance. Further measures could involve enforcing certain security procedures or employing standardized terminology in cyber insurance policies to improve understanding.(2) Similar non-invasive measures, such as the NCSC publishing a handbook on obtaining cyber insurance, have already been investigated by The UK government. In the United States, the subject of cyber insurance has undergone governmental scrutiny, with the Federal Trade Commission (FTC) issuing direction on purchasing, with discussions continuing with the Cybersecurity and Infrastructure Security Agency

(1) Bohme, R., and Kataria, G. (2006). "On the Limits of Cyber Insurance." Trust and Privacy in Digital Business, 31-40.

(2) Alani, M. (2021). "Big data in cybersecurity: a survey of applications and future trends." Journal of Reliable Intelligent Environments, 7(6).

(CISA). The EU has also explored the effectiveness of cyber insurance, publishing on best practice and recommendations regarding overcoming industry-related problems.(1)

Ongoing doubts remain regarding the correct approach for the insurance industry to adopt, in order to improve stronger security behaviour. Frequent suggestions include lowering premiums or deductibles for companies maintaining a minimum level of security, for instance achieving accreditation from Cyber Essentials, NIST CSF or an equivalent programme. By creating a link between a programme and an objective analysis, cyber insurance companies can adjust premiums based on the appropriate decisions. Consequently, consumer organisations lacking cyber-hygiene or security systems would experience higher insurance premiums. Should a cyber incident occur, deductibles would be applied to the original fixed cost. Some have argued that comprehensive exclusion clauses, which release insurance companies from making payouts, are essentially used to mitigate risks. To address these concerns, governments must therefore offer succinct recommendations that define steps that businesses should take to be eligible for cyber insurance.(2)

7. The Challenges of Cyber Insurance in Light of Other Insurance Lines

Several strategic issues faced in cyber insurance have been previously encountered in other sectors, such as property, vehicle, terrorism, health and maritime. By leveraging the situations experienced by other insurance

(1) City of London (2020). "The Future of Cyber Insurance: Next Steps for the London Market," p.16.

(2) Jan Lemnitzer, 'Ransomware Gangs Are Running Riot – Paying Them Off Doesn't Help', The Conversation, 17 February 2021, accessed 23 August 2023; Dudley, 'The Extortion Economy'.p.22.

industries through existing research, the cyber insurance market could benefitsignificantly.(1)

Comparisons are regularly made between property, vehicle and cyber insurance because of the comparable security requirements. For instance, without evidence of an adequate lock on the front door, it would be challenging to obtain home insurance. Similarly, an individual without a driver's licence, will face issues in purchasing car insurance, and it is exceptionally difficult if the car lacks seatbelts. Moreover, lower insurance premiums are available to homeowners who apply security measures, such as the installation of an alarm or the erection of obstructions like a high fence.(2)

Incentives are also significant. Motorists are encouraged to drive carefully, partly by the threat of increased insurance premiums if they are involved in a crash. Telematics, also defined as digital vehicle monitoring, permits insurers to analyse driver behaviour by exchanging data and information between a vehicle and a centralised supervision system. By making use of personal driver analytics, insurance companies can proactively adjust premiums.(3) Similarities also exist between cyber and terrorism insurance. Both man-made risks contain a level of unpredictability that is missing from natural disasters or fire. It is therefore challenging for both parties to gather reliable data, which results in uncertainty over the scale of the risk being insured. Initially, the terrorism insurance sector encountered a

(1) Aziz, B. Suhardi, S. and Kurnia (2020). "A systematic literature review of cyber insurance challenges." International Conference on Information Technology Systems and Innovation (ICITSI), pp. 357-363.

(2) Ibid p.364.

(3) Bailey, L. (2014). "Mitigating Moral Hazard in Cyber-Risk Insurance." Journal of Law and Cyber Warfare, 3(1).

paucity of industry knowledge and data, with which to evaluate insurance premiums, owing to the highly specific features of the coverage.(1)

Momentous events often spur the purchase of terrorist insurance, similarly, a serious breach can stimulate the purchase of cyber insurance. Additionally, companies that purchase terrorism insurance encounter a significant risk similar to the issues faced in cyber insurance. This means that organisations that acknowledge the value of terrorism insurance are more prone to terrorist attacks in contrast to other organisations. The continuation of the terrorist attacks of the 1990s which had a significant effect, combined with the events of 9/11, made the terrorism insurance market aware of its inadequate understanding of the scale of risk that it was undertaking. This risk was accepted by governments, which promised guarantees or financial backing for this type of insurance. For instance, the UK government, gave a guarantee to Pool Re, a terrorism insurer, starting in the 1990s. This guarantee safeguarded any terrorist attack-linked expenditures over a specific limit would be covered. The United States government has enacted the Terrorism Risk Insurance Act to award federal reinsurance to insurers of both property and personal injury that offer terrorism insurance. In enacting this Act, it has demonstrated its commitment to compensating insurance companies for part of any damages, up to a maximum of $100 billion, on commercial policies. The collaboration of 95 governments in focusing on cyber insurance may have a similar effect as regards the consequences of a large-scale future cyber event.(2)

The health insurance industry also encounters issues when managing moral hazards. Some insured individuals may neglect pre-emptive care

(1) Ibid p.12.

(2) Miller, L. (2019). Cyber Insurance: An Incentive Alignment Solution to Corporate Cyber-Insecurity. Journal of Law and Cyber Warfare, 7(2), 147-182.

measures after purchasing insurance, believing that any costs arising from treatment will be met by the policy. Consequently, insurers face financial issues, as preventative treatment tends to be less expensive than treating a serious future illness.(1) Likewise, the customer is more likely to find themselves in hospital for longer or suffering more serious effects. A similar situation is found when companies avoid allocating money for cyber security, assuming that they will receive compensation in the event of a cyber incident. The notion of 'moral hazards' has been widely investigated by the health insurance industry. By investigating methods, cyber insurers can gain an understanding of how to successfully encourage the uptake of cyber-related pre-emptive action among cyber insurance customers.(2)

Encouraging healthy individuals to purchase health insurance is a constant issue. The enactment of the 2010 Affordable Care Act in the US brought to light the reality that little health insurance is acquired by younger and fitter individuals. It seems to be a common misconception among this demographic that they are immune to the risks that health insurance aims to alleviate, and therefore believe it to be irrelevant to them. Considering the expense of premiums, this group generally concludes that savings outweigh the slight risks they face. Consequently, this lack of uptake leads to higher premiums in different areas. Only individuals with a substantially higher risk of expensive medical costs decide to purchase health insurance in this event.(3)

(1) S. Romanosky , "Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?" Journal of Cybersecurity (2021). p. 18.

(2) Ibid p.19.

(3) L. Miller, "Cyber Insurance: An Incentive Alignment Solution to Corporate Cyber-Insecurity" Journal of Law and Cyber Warfare (2019). p. 31.

Thus, without premiums from low-risk customers, insurance companies are unable to meet the costs of paying compensation in high-risk situations. Likewise, many companies do not see the risk related to cyber insurance to be substantial enough to justify purchasing, leading to low uptake.(1) Furthermore, it can be contended that companies with an increased outlay on risk-mitigation measures, will be disincentivised to economically support the insufficient risk-management procedures of other companies. Intending to improve the rate of uptake, the health insurance industry focuses on information and awareness schemes, whilst also amending premiums and deductibles to reflect the requirements of lower-risk customers more closely. These initiatives may also prove applicable to the cyber insurance industry.(2)

Maritime insurance is an insurance category with a long history. Traditionally, potential hazards have been minimised and moderated by insurers in alliance with the maritime sector. The iterative procedure is reliant on an understanding of the existing circumstances; for instance, ship structure and tendencies in pirate attacks may be analysed. During the early 1900s, the focus moved to an exploration of boiler explosion-related incidents. More recently, the maritime insurance industry has had to face the increasing frequency of piracy-related risks. Given the widespread and well-known history of the maritime insurance industry, it is likely that cyber insurance could benefit from its proven measures or insights.(3)

(1) Insurance Journal, 'Boston Bombing Lesson: Risk Managers Urge Better "Terror Act" Certification', 18 March 2015, accessed 5 August 2023. p.13.

(2) Ibid p.13.

(3) Jan Lemnitzer, 'Ransomware Gangs Are Running Riot – Paying Them Off Doesn't Help', The Conversation, 17 February 2021 , accessed 23 August 2023; Dudley, 'The Extortion Economy'.p.22.

Cyber insurance also demonstrates certain parallels to kidnap and ransom (K&R) insurance due to the nature of ransomware attacks. These attacks have particularly targeted a variety of organisations such as hospitals, corporations and even insurance companies. K&R policies include coverage for ransoms, incident response consultancy services, negotiators' costs and further correlated costs. These actions are key during ransomware attacks. Thus, lessons can be learned from this insurance sector.(1) Wider exploration is necessary to investigate the links between the motivations engaged by other insurance sectors to promote wider uptake and the cyber insurance sector.

8. Policy Gaps in Cyber Insurance

Firstly, while disruption to business is increasingly becoming a core component of commercial property coverage, most property insurance policies and plans suffice to cover physical asset loss. Meanwhile, cyber risks are excluded, unlike liability coverage. Hence, the insurer arrives at a different assumption than the policyholder who may believe that cyber incidents are fully covered. Such vagueness can expose defects in basic principles like the lack of insurability by leading to legal challenges and flaws in protection.(2)

Secondly, companies take a long time, sometimes up to six months, before they can secure coverage. Thirdly, there are also increasing lists of exclusions that could void cyber insurance coverage such as: a lack of security protocols, human error, acts of war and non-compliance. Fourthly,

(1) Ibid p.23.

(2) Daniel Schwarcz & Peter Siegelman, eds., Research Handbook on the Economics of Insurance Law, Cheltenham, UK & Northampton, MA: Edward Elgar Publishing (2022). p. 52.

the aggregation potential of cyber losses if a cloud operation came to a standstill. It is also difficult to know the losses across over time.(1)

Finally, Ransomware is an issue as governments encourage organisations to be aware of it considering hostile state and non-state actors who may utilise such ransomware to cause disruption leading to being offline for lengthy periods. Ransomware attackers have also been known to target organisations that possessed cyber insurance policies, and in case there was open admission of this as they were aware that the organisations could therefore make the payouts. Hence, if an organisation has a cyber insurance policy this could be accessed to pay out a ransom. Some attackers therefore tried to leverage that to force organisations to pay. To the extent that the threat environment at present is significant, with BitCoin wallets being utilised in this regard, with attacks on businesses, manufacturing, construction and healthcare systems.(2)

Herein, therefore cyber insurance does not work as smoothly as it could. Likewise, encouraging to organisations to have better security practices also does not work as efficiently as it could. As if a business approaches five insurers for example, they may request five different security measures. This makes it very difficult therefore, for an organisation to be able to adequately know exactly what good security measures are for cyberspace. Insurers are struggling with this, as each insurer will not be sure what good security practice looks like or may have a different opinion. Hence, in some instances insurers may utilise security controls that may offer the best value

(1) Ibid p.56.

(2) Lawrence A Gordon, Martin P Loeb and Tashfeen Sohail, 'A Framework for Using Insurance for Cyber-Risk Management', Communications of the ACM (Vol. 46, No. 3, March 2003). pp 85.

to reduce the number of claims of the size of the attack, but these may conflict with a government's advice on cyber security measures. An insurer may suggest that a company ignores such governmental advice and instead adheres to their own cybersecurity controls to reduce risk.(1)

Data is a key gap, as insurers focus on it and reliable insights. Cyber insurance, compared to the natural disaster insurance industry or crime industry, they can ascertain the likelihood of a crime or natural disaster – such insights determine an insurance premium. This is not yet the case for cyber insurance, as the nature of cyberspace is dynamic and fast-moving in comparison to other insurance lines. This forces insurance companies out of their comfort zone; urges them to think about what data they need; and what insights can be developed to determine appropriate premiums. In the case of ransomware – there is no benchmark by which to measure that an attack will not occur tomorrow. Generative AI for instance is a case in point, and the questions around its future as a threat to organisations and attackers utilising it to create malware for instance. The rapid pace of cyberspace makes it increasingly difficult for insurers to adequately decipher the risk from which to develop insurance policies with a substantial level of certainty.(2)

9. The Implications of the Cyber Insurance Market for SMEs

As previously stated, the cyber insurance market has not yet adopted equivalent methods to the maritime, energy, aviation and transport insurance sectors. A set of consistent insurance coverage terms exists for

(1) Ibid p.89.

(2) Sachin Shetty et al., 'Reducing Informational Disadvantages to Improve Cyber Risk Management', The Geneva Papers (Vol. 43, 2021). p 38.

these industries, and they have been created by insurers in partnership with market players. As a result, insurance companies generally make use of their own predefined circumstances to offer cyber-risk insurance to SMEs.(1) Cyber-risk insurance has a rather low uptake rate. This is attributed to the fact that an average SME does not fulfil the fundamental conditions to qualify for insurance coverage. For instance, to attain cyber risk insurance coverage, cyber insurers may require the prospective policyholder to have employed security procedures such as multi-factor authentication (MFA), undertaken awareness training for employees and applied strict rules for remote working. Furthermore, SMEs frequently underestimate the prospective risks created by cyber threats, particularly when data processing is a key part of company operations. This failure illustrates a general lack of awareness of expenditure following a cyber-attack, in addition to the legal obligations if a data breach happens.(2)

Traditionally, insurers have implemented different approaches when covering SMEs and large corporations. The underwriting investigations performed for larger companies are more demanding, requiring extended (and at times numerous) proposals. Moreover, larger companies generally face higher deductibles and coinsurance conditions, particularly in cases of extortion. Their proposals may also contain a larger number of prohibitions compared to SME proposals. Brokers also suggest a low level of interest in SME firms on the London insurance market. Therefore, opportunities exist for smaller-scale (and specialised) insurance companies to contribute to the

(1) Schwarcz, D. and Siegelman, P. (2015). "Insurance agents in the twenty-first century: The problem of biased advice." Daniel Schwarcz and Pete Siegelman (eds.), Research Handbook on the Economics of Insurance Law. Cheltenham, Glos: Edward Elgar Publishing. 36-71.

(2) Ibid p.74.

SME cyber insurance market. As a result, the SME market often requires a single insurer to provide coverage, compared with several insurers dividing the risk, which is seen more frequently in the transport, energy, marine and aviationsectors.(1)

10. Cyber Risk Insurance Approach to Risk Management of SMEs

Caution is being exercised as a result of the scarcity of previous supply-side data for claims for this modern type of business. The products proposed to SMEs often contain exclusion terms and features to control risk, such as retrospective dates and discovery clauses, which may be overly dependent on. This outcome is not unexpected considering the composition of potential developing risks. Yet, it is evident that, in aiming to widen the uptake of products, some adjustments will have to be applied; these will be considered later in this paper.(2)

Considering the demand side of the industry, an examination of numerous SMEs visibly reveals that few companies view cyber-risk insurance as a necessary tool for reducing risks. Regrettably, this cannot be ascribed to their application of vigorous cyber security measures. Furthermore, the larger part of companies, including those strongly reliant on operational data that is stored on in-house systems (for instance SMEs involved with in technology and science) and those in hospitality, dependent on Internet sales and bookings, do not see cyber risks as a business-related issue. The survey

(1) Richard Knight and Jason R C Nurse, 'A Framework for Effective Corporate Communication After Cyber Security Incidents', Computers and Security (Vol. 99, December 2022). p.23.

(2) Gordon, L.A., Loeb, M.P., Sohail, T., (2003). "A Framework for Using Insurance for Cyber-Risk Management." Communications of the ACM, 46(3), 81-85.

also illustrates the lack of awareness of possible results of certain risk-control contracts, such as maintenance guarantees and limits, in addition to claim regulator procedures such as discovery clauses and retroactive dates, which are regularly applied in cyber insurance contracts. This is to be expected, since numerous phrases employed in cyber-risk policies are rather technical. Yet, it is worrying to note that most of the examined SMEs displayed this tendency.(1)

Moreover, respondents seem unaware of the need to maintain and frequently upgrade both security software and hardware. It is also evident that a considerable majority of respondents were not aware that a variety of types of cyber-risk insurance products existed on the market. It is noteworthy that a cyber product that includes restoration costs in place of compensation, may prove more suitable for small companies, since they may not have adequate understanding or information technology (IT) experts to help them to rapidly and safely restore their systems after a cyber-attack.(2)

Most SMEs do not have the essential technological assistance and expertise needed to enhance their cyber-security procedures or the security of their commercial operations systems. A cyber-security constituent to an insurance product is vital, as it will reliably evaluate the failings of SMEs' digital networks, improve their security based on the most recent cyber hazards and create a cyber-resilient atmosphere with a practical risk-management approach. Hence, the security of the cyber environment is

(1) Ibid p.83.

(2) Woods Daniel. 'Mapping the Coverage of Security Controls in Cyber Insurance Proposal Forms'; ENISA, Commonality of Risk Assessment Language in Cyber Insurance. (2017). p 27.

of higher importance to SMEs than large businesses. Considering their reduced size and incomes, SMEs are particularly susceptible to the harmful outcomes of successful cyber-attacks. These outcomes may involve a lasting loss of clients as a result of bad publicity, a danger that insurance cannot completely mitigate. It may, however, be more successfully managed by the application of preventive measures. Research posits the advantage of incorporating a cyber-security business into an SME's cyber-dependence approach, since this will allow vital training of SME personnel in cyber hygiene. Insurers should specify the companies that will offer training on effective responses to a cyber breach. It is important that the training include both operational procedures that reduce the harmful effects of the attack and legal measures, incorporating regulatory announcements and data gathering. This will permit the assigned staff of the SME to employ a clear procedure during the crucial initial hours after the attack. Conversely, this product also provides numerous benefits for risk carriers.(1)

Significantly, assigning cyber-security assessments to a reliable cyber-security company, will not only permit insurers to precisely calculate the level of risk from the start, but will also ensure that the risk does not rise to an unacceptable level at any point in the insurance term. That is to say, the burden of maintaining cyber-security will not simply fall on the customer, but will be undertaken by cyber-security experts. Any additional instructions from the cyber-security company to the covered SMEs will be documented. This documentation will also be helpful for insurers should they wish to query a potential breach of insurance conditions by the policyholder at a later date.(2)

(1) Ibid p.29.

(2) Dariusz Adamski, "Lost on the Digital Platform: Europe's Legal Travails with the Digital

Yet it is necessary to consider whether a solution offering both cyber-security services and protection will lead to higher premiums, potentially outpricing a large part of SMEs. The scale of this paper (and the expertise of its authors) is inadequate to undertake an actuarial analysis to test this assumption. However, this will be unlikely since any compensation paid out should be substantially decreased by the measures put in place by cyber-security firms (both at the start of and throughout the policy). Hence, if robust cyber-security methods are applied, cyber insurance claims will decline. As a consequence, there will be no financial loss to the insurers by allocating a part of the premium to their partner cyber-security firm. Thus, any need to increase the premium is eliminated.(1)

Presently, cyber-risk insurance is normally marketed with a fixed period, yet for SMEs there may have to be changes in how these are pitched to them. At the beginning, insurers must assess the risk and determine the premium for the period of insurance. This premium is established based on a preliminary evaluation of risk. This evaluation considers data given by the insured and data obtained from other existing sources by the insurer. It is inevitable that historical data is used to evaluate risk, meaning that previous performance of cyber-security systems is considered, in addition to any earlier claims made. However, if regular and up-to-date information is received from a cyber-security partner regarding the performance of the cyber-security systems of the appropriate SME, in addition to the SME's method of cyber security, there is potential for cyber-risk insurers to apply an innovative product called 'usage-based insurance'. Using real-time data,

Single Market", Common Market Law Review 55, (2021).p 27.

(1) Lawrence A Gordon, Martin P Loeb and Tashfeen Sohail, 'A Framework for Using Insurance for Cyber-Risk Management', Communications of the ACM (Vol. 46, No. 3, March 2003). p 90.

insurers would be able to estimate the premium rate throughout the duration of the policy. This means that insurers could leverage a considerable amount of data to offer a new type of insurance that would adapt the premium rate to correspond to the SME's most recent cyber-security conduct.(1)

Hence, such a comprehensive approach would enhance not only cyber security but also guarantee its long-term sustainability. Several analysts have contended that requiring cyber insurance, especially for SMEs, is an effective method of improving cyber security.(2) Nevertheless, there remain several hesitations concerning this approach. Firstly, it is clear that cyber-risk insurance acts as a key risk-management instrument against cyber hazards. However, requiring its application as the primary line of defence would lead to higher operational costs for SMEs. In the current economic climate, it is debatable whether SMEs would be able to finance these additional expenditures without government subsidies. In addition, creating a compulsory insurance system would require the construction of a legal framework, which at present is not a government priority for the government. Therefore, our initial proposal in this document is to develop an innovative product that leverages insurance as a promoter to advance cyber security for SMEs.(3)

Finally, reflecting on the fact that most of the SMEs interviewed demonstrated a low level of awareness concerning the vulnerability of their companies to cyber threats, it is clear that additional instruction must be offered to SMEs. This must be the insurance industry's highest priority.

(1) Ibid p.92.

(2) Association of British Insurers (ABI), 'Cyber Risk Insurance,' accessed 9 September (2023). p 24.

(3) Ibid p.26.

Providing cyber-security training has strong economic advantages since such attacks are associated with significant costs. Yet with the application of a comprehensive insurance product, as illustrated in this paper, there can be significant reductions in the incidence of successful cyber-attacks on SMEs.(1)

11. The Potential of Insuring Against Cyber Risk

It is apparent that the digital economy functions as a spur to economic expansion. For instance, the employment of IT added 21% to the gross domestic product (GDP) growth of developed countries between 2019 and 2023.(2) The use and reliance on IT is growing, leading to a new menace: cyber risk. Cyber risk is categorised as the chance of physical damage to individuals or property, in addition to any monetary damages stemming from the failure of digital systems or the corruption of data. The consequences for society are substantial, owing to the interdependency of information systems. This can result in a domino effect, whereby a negative event can rapidly spread between all the users of an information system.

Therefore, cyber risk is a hazard to a complete system. For instance, a failure in a cloud-computing service could quickly spread among all its users, creating the potential for devastating consequences. Cyber risk can be divided into three sections: threat, vulnerability and impact. Threat refers to the probability of a potentially harmful or damaging event; the cited article explores three categories of threat: cybercrime, human error and system

(1) Sachin Shetty et al., 'Reducing Informational Disadvantages to Improve Cyber Risk Management', The Geneva Papers (Vol. 43, 2021). p 40.

(2) Johansmeyer, T. (2021). Cybersecurity Insurance Has a Big Problem. In Harvard Business Review, 11th January 2021. Accessed Online: https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem

failures[1] Vulnerability signifies the likelihood of experiencing losses once a threat becomes a certainty. In systems that are generally described as resilient, threats can occur without causing any loss. By applying automatic data back-ups and robust firewalls, for example, losses caused by issues such as accidental file deletion or viruses can be effectively stopped. Impact means the negative outcomes stemming from the incident.[2]

Two substantial differences can be noted with regard to impact. Firstly, first-party damage denotes the injury or destruction that takes place within the company that owns the IT system, while third-party damage denotes the injury experienced by other parties as a consequence of the cyber risk. When a number of third parties have mutually dependent information systems, it is probable that the value of their assets (those belonging to the third parties) is higher than the value of the first party's assets. The harm caused by a third party is higher than the harm caused by the first party. This is especially important for SMEs, whose resources are relatively limited but have the capacity to cause considerable damage to third parties.[3]

Additionally, first-order damage describes any instant financial losses encountered by organisations as a consequence of a cyber event, for instance, the hypothetical loss of personal or corporate data as a result of hacking, failures of hardware or software, and human error, all of which can throw business operations into disarray. Second-order damage describes the negative consequences that follow an incident becoming public, such

(1) Lawrence A Gordon, Martin P Loeb and Tashfeen Sohail (2003). "A Framework for Using Insurance for Cyber-Risk Management." Communications of the ACM, 46(3), March 2003, p 90.

(2) Ibid p.91.

(3) Sachin Shetty et al., 'Reducing Informational Disadvantages to Improve Cyber Risk Management', The Geneva Papers (Vol. 43, 2021). p 41.

as damage to an individual's reputation. A further example might concern receiving a fine for failing to communicate details of a breach to a data-breach-notification organisation. Determining second-order damage is more difficult than determining first-order damage, resulting in more challenges informing a third party, such as an insurer. This may result in inadequate or unsuitable claim behaviour within the context of cyber insurance.(1)

12. Coordinated Governance for Cyber Insurance

An internationally recognised standard, ISO/IEC 27001 offers to organisations guidance on privacy protections, cybersecurity and information security. This was updated in October 2022. These guidelines include creating organisation-specific information security management guidelines and putting information security controls in place in tandem with globally recognised best practices. Any company or organisations that wish to utilise well-recognised information security rules can use this generic standard. As a result, this enabled Adriko and Nurse to review insurance proposal forms.(2) Their work highlighted the real-world limitations that insurers experience. Each of the 14 Security Clauses in the framework has many Security Control categories, each having associate controls.

Adriko and Nurse discovered that Information Security Governance forms the core of cyber resilience strategies and drives the security program. Yet this control was found to be neglected. This can put insurers and their insureds at risk as despite the controls that may be present these will be less effective if there are no governance procedures and strategies to

(1) Ibid p.43.

(2) Adriko, R. and Nurse, J.R.C. (2024). "Does Cyber Insurance Promote Cyber Security Best Practice? An Analysis Based on Insurance Application Forms." Digital Threats: Research and Practice, 5(3), 1-39. Accessed Online: https://dl.acm.org/doi/full/10.1145/3676283

determine how these controls should be applied and how security programs can be continuously improved. They found therefore that there is neglect of governance aspects including policies and procedures which form the foundation of a cyber security program.(1)

13. Insurance Tools for Cyber Risk and Strategies for Inclusion into Legislation

In light of the cyber security challenges outlined earlier in this paper, it is important to consider strategies for how insurance tools could be incorporated into legislation.

Firstly, there are several insurance tools that can be utilised for cyber risk management. Woods found that organisations approach insurers and after informing the insurance company of their current cyber security position, which may be poor, many insurance companies simply wash their hands from the corporate customer as they are deemed as high-risk customers. Based on this, Woods suggests that insurers should consider underwriting businesses if they undertake several cybersecurity measures. So cybersecurity can be extremely useful when it offers pathways to motivate businesses to enhance their cybersecurity protocols. Likewise, the insurance industry can advise companies on various measures and security practice frameworks and in return obtain insurance premium discounts, this serves to incentivise companies to improve their internal security protocols.

Secondly, some insurance companies will not pay out via citing "act of war" exceptions. Carter and Enoizi,(2) in a paper for the Geneva

(1) Ibid p.41.

(2) Carter, R.A. and Enoizi, J. (2020). Cyber War and Terrorism: Towards a common language to promote sustainability. Zurich: The Geneva Association. Accessed Online: https://www.genevaassociation.org/sites/default/files/research-topics-document-type/

Association, suggest that any hostile acts from hostile state actors, short of 'declared war,' should be demarcated as 'hostile cyber attacks' [HCA]. The designations of "terrorism" or "acts of war" are particularly problematic for victims of ransomware attacks, as insurance will not cover the claim or risk potential sanction violations by paying out if sanctioned entities are involved. Nevertheless, Halikias highlights some light at the end of the cyber insurance tunnel. The purchase of cyber-specific policies that do away with "act of war" and "terrorism" exclusions – organisations can then be fully covered. This in practice may mean, stipulating an addendum to an insurance policy to explicitly cover, for example, "the malicious introduction of a machine code or instruction. It is for this reason that some companies are leading the way when it comes to merging cybersecurity with insurance. With companies such as CFC in the UK; Stoïk in France and Germany and the big hitters of AIG, AXIS, Chubb and AXA XL in the US and beyond.(1)

14. Findings and Conclusion

14.1 Conclusionary Remarks

Cyber risk poses a complicated and increasing issue for governments, businesses and customers. The economies of Europe, the Gulf and the Far East may be particularly susceptible to cyber risks due to their reliance on centralised cloud systems and other digital supply chains. For some, this may call into question to what extent are risks in the cyberspace insurable.

Cyber insurance offers SMEs security support which they may not be able to obtain. Larger companies would buy a cyber insurance policy as they

pdf_public/cyber_war_terrorism_commonlanguage_final.pdf

(1) Ibid p.17.

understood the relevance yet even if they had a cyber incident would not claim it unless there was a major breach. For SMEs without IT or security departments, if they have a breach the cyber insurance company will connect them to a PR firm, incident response team, digital forensics team, data recovery company etc. essentially a whole suite of expertise which they could not afford by itself. This can be the value in cyber insurance.(1) Furthermore, cyber insurers will request an upfront risk assessment and a cyber resiliency score to ascertain how equipped an organisation is for a cyber-attack. Yet in saying that, the average SME cannot realistically obtain cyber insurance due to threats such as ransomware which stretch the market.

This paper has considered the potential role of cyber insurance in tackling this question. Presently, cyber insurance is limited in its ability to resolve the issues required by regulators and businesses. Only a minority of cyber insurance industry players have used financial incentives or security requirements to improve the cyber-security practices of policy owners. The increase in resulting losses has highlighted the fact that insurance companies too are dissatisfied with the current situation. Numerous issues face the cyber insurance sector, reducing the efficiency and growth of its products. One key issue is the shortage of knowledge concerning factors that cause loss and specific cyber-security processes and recommendations that might successfully resolve them.

14.2 Findings

A key finding is that the United States and the United Kingdom are leading the field in embracing cyber insurance particularly among large-

(1) Edwards, J. and Weaver, G. (2024). The Cybersecurity Guide to Governance, Risk and Compliance. Hoboken, NJ and Chichester, West Sussex: John Wiley & Sons.

scale businesses. However, small- and medium-sized enterprises (SMEs) show a far lower uptake. As the 2022 UK Cyber Security Breaches Survey reports, the UK government estimates that only around 4% of all businesses have a specific cyber insurance policy, and just 28% are covered for cyber risk within a wider insurance policy. A mere 2% of 'micro' businesses own a specific cyber insurance policy.(1)

A feasible explanation for this is the alleged excessive cost of these plans and companies' readiness to assign money for them. This has hampered the market considerably in accurately pricing cyber insurance products, since measuring cyber risk is a vital move in assessing insurance costs. Owing to their comparatively recent development, evidence is lacking concerning the incidence and consequences of cyber-attacks, counter to more familiar occurrences such as hurricanes or earthquakes. In particular, the lack of data concerns the tangible financial impact of a cyber incident, considering that the speed, nature and seriousness of incidents can vary dramatically.

The cost of a data breach for a small organisation, defined as one with less than 500 employees, went up from $2.35 million in 2020 to $2.98 million in 2021. Regretfully, after a cyber-attack, 60% of small businesses shut down within six months.(2) By generating jobs, paying taxes, and delivering goods and services to nearby areas, small companies contribute significantly to the economy. Consumers and the economy at large suffer greatly from any threat to their survival, which emphasises the necessity for the best cybersecurity laws to lessen the probability and financial impact

(1) Avraham, R. (2012). The Law and Economics of Insurance Law – A Primer. Connecticut Insurance Law Journal, 19 (3).

(2) See:https://www.salford.ac.uk/business/greater-manchester-cyber-foundry/cybersecurity-isnt-a-priority-for-smes-right-change-your-strategy#:~:text=Cyber%20security%20statistics%20show%20that,than%20%242.2%20million%20a%20year.

of cyberattacks. At present, there are increases in email compromises and fewer claims for ransomware.

Some insurers suffered losses when ransomware was first unleashed in cyberspace as a result of the payouts for such attacks. Nevertheless, these insurers continued to operate in the cyberspace market to gather more insights and regarding ransomware and its nature. How can insurers therefore work together to formulate a comprehensive dataset for cyber insurance that can be used by all to better understand cyber risks, the impact of security controls and the pros and cons of different controls? There was little appetite for this however as every insurance company used their own insights as a competitive advantage over other insurance companies. This however may be starting to change. Another challenge is in insurers ascertaining that a company is indeed implementing security controls. This is often based on trust. However, there may be cases where an organisation experiences a breach due to not disclosing the real condition of their cybersecurity. In these cases, such withholding of the real specifics renders the insurance policy null and void.

Secondly, some insurers have attempted to apply what is utilised in car insurance when car insurers deem an individual as risky the company may still underwrite the individual yet stipulate the installation of a black box device. This device will determine how fast you drive, your location and how safe you drive. This monitors the driver and as a result of this the premium may fluctuate in tandem with the driver's driving risk, if the driver is less risky the premium will reduce and if the driver is riskier the premium will increase.

More recently, there has been better joint-working between security companies and insurance companies. In this way cybersecurity companies

benefit from the data that insurers have and likewise, insurers gain more expertise about the cyberspace and latest trends as insurance companies are now starting to better comprehend cyberattacks, threats and mitigations.

15. Recommendations

When it comes to developing guidance for insurers providing risk cover, there are a range of recommendations that can be forwarded to those who are at the helm in the field:

1. A common framework wherein indirect losses from cyber-crime, such as reputational damage which can often exceed the direct losses, are covered by insurance products.

2. Increased dialogue between policymakers and regulators on the one hand, and academics, risk management experts and providers of cyber insurance and risk cover on the other. In this way, the market for cyber risk insurance, cyber threats and developments in insurer's risk management and governance.

3. Increased joint working between cyber insurers and public sector authorities to develop approaches with insureds that support the accurate and timely sharing of incident data.

4. This emphasises the need for better collaboration between government and the insurance industry to formulate and facilitate the solutions that bolster the above and improve threat intelligence.

5. Where the insurer has expertise in both cybersecurity and cyber insurance, it can offer a suite of support to bolster the organisational resilience and prevention against a range of cyber threats, while also providing insurance.

6. With this model, both the insurer and the insured win, as it were. The cyber insurance company as it has less claims and the business as from the initial day of the insurance contract, they have a tangible benefit. Whereas in conventional lines of insurance there is only a 'benefit' for the insured when they sustain a loss. There are some insurance companies in Europe that are making strides in this regard.

7. In cyber insurance, some insurers may effectively stipulate the installation of a 'virtual black box' in cases where there is lax security within an organisation. In this way, such a virtual black box will allow the easy monitoring of an organisation's security, flag cyber threats and have some mitigations.

8. Pre-breach services can also be offered by insurers, which support an organisation from start to finish by making services available to bolster security. Such as security awareness initiatives which are particularly useful for companies which do not have dedicated security personnel.

9. Where cyber insurance is in its infancy, there should be educational initiatives regarding cyber threat awareness and preparedness, promoted by policymakers and regulators.

References:

Abramovsky, A. and Kochenburger, P. (2016). "Insurance Online: Regulation and Consumer Protection in a Cyber World." Pierpaolo Marano, Ioannis Rokas and Peter Kochenburger (eds.), *The "Dematerialized" Insurance: Distance Selling and Cyber Risks from an International Perspective*. Cham, Switzerland: Springer. 117-143.

Abrams, (2020, September). "Cyber Insurer's Security Scans Reduced Ransomware Claims by 65%." *Bleeping Computer*, 22 September 2020. Accessed Online: https://www.bleepingcomputer.com/news/security/cyber-insurers-security-scans-reduced-ransomware-claims-by-65-percent/

Adamski, D. (2021). "Lost on the Digital Platform: Europe's Legal Travails with the Digital Single Market." *Common Market Law Review*, 55. 27.

Adriko, R. and Nurse, J.R.C. (2024). "Does Cyber Insurance Promote Cyber Security Best Practice? An Analysis Based on Insurance Application Forms." *Digital Threats: Research and Practice*, 5(3), 1-39. Accessed Online: https://dl.acm.org/doi/full/10.1145/3676283

Alajmani, A., and Syed, M. (2024). "Using artificial intelligence techniques to achieve justice efficiency in the United Arab Emirates." *University of Sharjah (UoS) Journal of Law Sciences, 21*(2).

Alani, M. (2021). "Big data in cybersecurity: a survey of applications and future trends." *Journal of Reliable Intelligent Environments*, 7(6).

Al-Salman, N., and Sarhan, A. (2024). Civil liability for the act of robots. *University of Sharjah (UoS) Journal of Law Sciences*, *21*(1).

Avraham, R. (2012). The Law and Economics of Insurance Law – A Primer. *Connecticut Insurance Law Journal*, 19 (3).

Aziz, B. Suhardi, S. and Kurnia (2020). "A systematic literature review of cyber insurance challenges." *International Conference on Information Technology Systems and Innovation (ICITSI)*, pp. 357-363.

Bailey, L. (2014). "Mitigating Moral Hazard in Cyber-Risk Insurance." *Journal of Law and Cyber Warfare*, 3(1).

Bohme, R., and Kataria, G. (2006). "On the Limits of Cyber Insurance." *Trust and Privacy in Digital Business*, 31-40.

Bolot, J., and Lelarge, M. (2009). "Cyber Insurance as an Incentive for Internet Security." M Eric Johnson (ed.), *Managing Information Risk and the Economics of Security*. New York, NY: Springer, Third Edition. 269–90.

Boston Bombing Lesson: Risk Managers Urge Better and Terror Act Certification. (2023).

Carter, R.A. and Enoizi, J. (2020). *Cyber War and Terrorism: Towards a common language to promote sustainability.* Zurich: The Geneva Association. Accessed Online: https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cyber_war_terrorism_commonlanguage_final.pdf

Conde Pérez, E. (2019). Cybersecurity in the European Union: Resilience through Regulation? In *Routledge Handbook of EU Security Law and Policy*. Routledge.

Dambra, S., Bilge, L., Balzarotti, D. (2020). "SoK: Cyber insurance? technical challenges and a system security roadmap." *2020 IEEE Symposium On Security And Privacy (SP)*, pp. 1367-1383.

Daniel, W. (2022). "Mapping the Coverage of Security Controls in Cyber Insurance Proposal Forms." *Journal of Internet Services and Applications*, 8(1).

Daniel, W. (2022). *The Evolutionary Promise of Cyber Insurance*. The Fin Reg Blog, 1 February 2022. Accessed Online: https://sites.duke.edu/thefinregblog/2022/02/01/the-evolutionary-promise-of-cyber-insurance%EF%BF%BC/

Dariusz, A. (2021). "Lost on the Digital Platform: Europe's Legal Travails with the Digital Single Market." *Common Market Law Review*, 55(4).

Edwards, J. and Weaver, G. (2024). *The Cybersecurity Guide to Governance, Risk and Compliance.* Hoboken, NJ and Chichester, West Sussex: John Wiley & Sons.

Erkan-Barlow, A. and Wells-Dietel, B.P. (2023). "The Current State of Cyber Insurance and Regulation in the Context of Investment Efficiency and Moral Hazard: A Literature Review." *Journal of Insurance Regulation*, 42.

Gordon, L.A., Loeb, M.P., Sohail, T., (2003). "A Framework for Using Insurance for Cyber-Risk Management." *Communications of the ACM*, 46(3), 81-85.

Halikias, H. (2024). *Digital Shakedown: The Complete Guide to Understanding and Combating Ransomware*. Cham, Switzerland: Springer.

Huq, N. & Vosseler, R. and Swimmer, M. (2021). *Cyberattacks Against Intelligent Transportation Systems: Assessing Future Threats to ITS*. TrendMicro Principles for Board Governance of Cyber Risk. Accessed Online: https://documents.trendmicro.com/assets/white_papers/wp-cyberattacks-against-intelligent-transportation-systems.pdf

Ignatuschtschenko, E. (2021). "Assessing Harm from Cyber Crime." Paul Cornish (ed.), *The Oxford Handbook of Cyber Security*. Oxford: Oxford University Press. 127-142.

Jean, B., Marc, L., & Johnson, E. (2009). "Cyber Insurance as an Incentive for Internet Security." M Eric Johnson (ed.), *Managing Information Risk and the Economics of Security*. New York, NY: Springer, Third Edition.

Johansmeyer, T. (2021). Cybersecurity Insurance Has a Big Problem. In *Harvard Business*

Review, 11th January 2021. Accessed Online: https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem

Knight, R. and Nurse, J.R.C. (2022, December). "A Framework for Effective Corporate Communication After Cyber Security Incidents." *Computers and Security*, vol. 99, p.23.

Koezuka, T. (2016). "The Cyber Insurance in Japan." Pierpaolo Marano, Ioannis Rokas and Peter Kochenburger (eds.), *The "Dematerialized" Insurance: Distance Selling and Cyber Risks from an International Perspective*. Cham, Switzerland: Springer. 201-225.

Kuru, D. and Bayraktar, S. (2017). "The effect of cyber-risk insurance to social welfare." *Journal of Financial Crime*, 24(2), pp. 329-346.

Lawrence, A. (2017). Cyber Insurer's Security Scans Reduced Ransomware Claims By 65%. *Bleeping Computer*.

Lawrence, G., & Martin, L. (2003). A Framework for Using Insurance for Cyber-Risk Management. *Communications of the ACM*, 46(3).

Lemnitzer, J. (2021). "Why Cybersecurity Insurance Should Be Regulated and Compulsory." *Journal of Cyber Policy*, 6(2), 118-136.

Lyngaas, S. (2023). Saudi cyber authority uncover new data-wiping malware, and experts suspect Iran is behind it. *Cyber-Scoop*. https://www.cyberscoop.com/saudi-arabia-iran-cyberattack-soleimani

MacColl, N., Sullivan, J. Nurse, J.R.C., Turner, S., Mott, G., Cartwright, E. and Cartwright, A. (2023). *Cyber Insurance and the Cyber Security Challenge*. London: RUSI. Accessed Online: https://static.rusi.org/OP-cyber-insurance-ransomware-challenge-web-final.pdf

Miller, L. (2019). Cyber Insurance: An Incentive Alignment Solution to Corporate Cyber-Insecurity. *Journal of Law and Cyber Warfare*, 7(2), 147-182.

Middleton, K. and Kazamia, M. (2016). "Cyber Insurance: Underwriting, Scope of Cover, Benefits and Concern." Pierpaolo Marano, Ioannis Rokas and Peter Kochenburger (eds.), *The "Dematerialized" Insurance: Distance Selling and Cyber Risks from an International Perspective*. Cham, Switzerland: Springer. 185-201.

Murdoch, S. (2021). "Cybersecurity Information Sharing: Voluntary Beginnings and a Mandatory Future." Paul Cornish (ed.), *The Oxford Handbook of Cyber Security*. Oxford: Oxford University Press. 314-328.

Nuvias. (2023). Cybersecurity Perspectives: Europe vs. USA. https://www.nuvias.com/en-us/cybersecurity-perspectives-europe-vs-usa/

Principles for Board Governance of Cyber Risk. (2022). http://www3.weforum.org/docs/WEF_Cyber_Risk.

Quadri, A. and Khan, M.K. (2019). *Cybersecurity Challenges of the Kingdom of Saudi Arabia: Past, Present and Future.* Global Foundation for Cyber Studies and Research. January 2019.

Rawlings, P. (2015). "Cyber Risk: Insuring the Digital Age." *Legal Studies Research Paper No. 189/2015.* London: Queen Mary University of London, School of Law. Accessed Online October 2024: https://bila.org.uk/wp-content/uploads/old/550ab0bbb91c09.11321920.pdf

Romanosky, S., Ablon, L., Kuehn, A. and Jones, T. (2021). "Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk." *Journal of Cybersecurity*, 5(1).

Sachin, S. (2021). Reducing Informational Disadvantages to Improve Cyber Risk Management. *The Geneva Papers*, *43* (4).

Sachin Shetty et al. (2021). "Reducing Informational Disadvantages to Improve Cyber Risk Management." *The Geneva Papers*, vol. 43, p 38.

Schwarcz, D. and Siegelman, P. (2015). "Insurance agents in the twenty-first century: The problem of biased advice." Daniel Schwarcz and Pete Siegelman (eds.), *Research Handbook on the Economics of Insurance Law*. Cheltenham, Glos: Edward Elgar Publishing. 36-71.

Shetty, N. Schwartz, G., Felegyhazi, M. and Walrand, J. (2010). "Competitive cyber-insurance and internet security." *Proceedings of Workshop of Economic Information Security (WEIS) 2010*, p. 229–47.

Sullivan, N. and Nurse, J.R.C. (2020). *Cyber Security Incentives and the Role of Cyber Insurance*. Royal United Services Institute for Defence and Security Studies. Emerging Insights Paper. Accessed Online: https://rusi.org/publication/emerging-insights/cyber-security-incentivesand-role-cyber-insurance

Talesh, S.A. (2018). Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as Compliance Managers for Businesses. *Law And Social Inquiry*, *43*(2).

Wessel, R.A. (2019). "Cybersecurity in the European Union: Resilience through Regulation?" Elena Conde Pérez (ed.), *Routledge Handbook of EU Security Law and Policy*. London and New York: Routledge. p.17.

Woods, D. (2017). *Mapping the Coverage of Security Controls in Cyber Insurance Proposal Forms ENISA, Commonality of Risk Assessment Language in Cyber Insurance*.

Woods, D.W., Agrafiotis, I. Nurse, J. and Creese, S. (2017). "Mapping the Coverage of Security Controls in Cyber Insurance Proposal Forms." *Journal of Internet Services and Applications*, 8(8).

Woods, D.W. and Moore, T. (2019). "Does Insurance have a Future in Governing Cybersecurity?" *Security and Privacy* 18(1), p.18. Accessed October 2024: https://

www.danielwoods.info/assets/pdf/DW2020_governance_IEEESP.pdf

Wolff, J. (2022). *Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches and Cyber Attacks*. Cambridge, Massachusetts: The MIT Press.

فرص التأمين السيبراني لمواجهة تحديات الهجمات السيبرانية: التداعيات على الشركات الصغيرة والمتوسطة

خلف بن محمد البلوي[1]

ملخص البحث:

يناقش هذا البحث المزايا والتحديات المتعلقة باستخدام التأمين السيبراني كوسيلة فعّالة في تعزيز إجراءات الأمن السيبراني ومواجهة مخاطرها. من خلال الاستقراء نجد أن البحوث القائمة بشأن مدى فعالية التأمين السيبراني في مواجهة التحديات والتهديدات الإلكترونية تظل محدودة. على الرغم من أنّ أصحاب وثائق التأمين السيبراني لديهم الفرص مع شركات التأمين في تحسين فهمهم للمخاطر السيبرانية وحاجتهم إلى هذا النوع من التأمين في تعزيز حمايتهم من المخاطر الإلكترونية، إلا أن استيعاب أهمية التأمين السيبراني، ولا سيما بين الشركات الصغيرة والمتوسطة الحجم، لا يزال محدوداً. علاوة على ذلك، لا يزال هناك قدراً كبيراً من الغموض ينطوي على مدى إمكانية تغطية مجموعة من الأحداث السيبرانية المتنوعة، تستخلص هذه الدراسة نتائج جديدة مستمدة من دراسة لبعض من تقارير شركات التأمين، ودراسة لقوانين التأمين والتحقيقات العلمية المتعلقة بها

الكلمات الدالة: التأمين السيبراني، الأمن السيبراني، المخاطر، الشركات الصغيرة ومتوسطة الحجم.

(1) كلية الشريعة والقانون - جامعة تبوك (تبوك - المملكة العربية السعودية)
Km.albalawi@ut.edu.sa