Society of Underwriting Professionals

Standards. Professionalism. Trust.

Is cyber liability insurance an answer against growing cyber threats?

by Preeti Agarwal

socup.org.uk

The Chartered Insurance Institute (CII)

The CII is the largest professional body for the Insurance and Financial Planning professions, with more than 127,000 members in over 150 countries.

Our purpose is to build public trust in insurance.

We do this through the provision of insightful leadership, relevant learning and an engaged membership.

This report forms part of our programme of insight – delivered with and on behalf of the profession – to drive positive action in support of society's experience of insurance.

www.cii.co.uk

The Society of Underwriting Professionals

The Society of Underwriting Professionals is the professional body dedicated to over 11,000 individuals working in the underwriting sector. As part of the Chartered Insurance Institute, we share a Royal Charter commitment to secure public confidence and trust by raising standards and technical excellence across the profession.

We make underwriters better by sharing insights and good practice guidance which focuses on the latest trends and evolution of the sector.

Our enhanced member experience supports you at every stage of your career and transforms how you engage with both your professional body and each other.

Contacting the CII

If you have any queries regarding the content of this report please contact Matthew Connell, Director of Policy and Public Affairs, CII email: **matthew.connell@cii.co.uk**

Disclaimer

All authors named contributed to this report in their own personal capacity. The views expressed are their own and do not necessarily represent the views of their respective employers or the Chartered Insurance Institute.

Contents

Acknowledgement

This thesis forms the final part of my Fellowship Program. I would like to take this opportunity to thank the people who have helped me in several ways with this project. First, I want to thank Mr. Abhijit Das (AII; Chief Risk Officer, Risk Department Trust Re for his professional guidance during this project).

Secondly I am grateful to Mr. Kodagali, Senior Underwriter in Property and Engineering for his moral support, encouragement and trust which helped me complete my dissertation.

Lastly, I would like to thank Hassan Tfayli FCII for his help on the technical part behind my thesis. Without these people, this thesis would not be as successful as it is now. Working with so many people on such an exciting subject has been a lifetime experience for me.

Abstract

Companies are exposed to a large number of dangers external to them and that they are often not even aware of. Evolution and technological advancements have brought evils that did not exist before and that increase every year in the forms of cyber risks.

It also adds irreversible damage to the corporate reputation of the company if it fails to mitigate and manage a data breach. At present, cyber risk is a real risk and suffering an attack of this type can have dire consequences, like loss of data and company reputation. In such cases, the need for cyber insurance was realised that enabled the companies to insure their data and protect it from theft. The significance of the cyber liability insurance cannot be undermined but it was necessary to determine the effectiveness of cyber insurance. The findings revealed that cybersecurity liability insurance is designed to protect companies against any legal repercussions, recovery costs and other expenses associated with cyber-attacks.

Conclusively, the findings revealed that there is a significant role for cyber insurance companies to raise financial support and claims against cyber-attacks. But it is a viable option for large organisations with big IT infrastructures, not for small enterprises. Meaningfully, cyber liability insurance is an answer against growing cybercrimes but there is currently more development in the concept. The suggestions for smaller companies needing protection from cyber-attacks have been proposed. Future research in this context is suggested by the primary findings to ascertain the research context comprehensively.

Introduction

1.1 Research background

The hackers are becoming more innovative and persistent, exploiting the vulnerabilities inherent in new technologies to steal information. Companies are exposed to a large number of dangers external to them and of which they are often not even aware. Evolution and technological advancements have brought evils that did not exist before and that increase every year in the forms of cyber risks (Gupta, Agrawal and Yamaguchi, 2016). Among the main damages derived from a cyber-attack to which a company is exposed include the loss of information of great importance or the destruction of operating and productive systems. It also adds irreversible damage to the corporate reputation of the company if it fails to mitigate and manage a data breach or the theft of private information of its customers (Liu et al. 2016). These problems, along with others, such as information leakage, electronic fraud or cybercrime, are some of the ones that concern many companies regardless of industry.

Although, a considerable amount of literature has been explored to explore the phenomenon of damages to the organisation with respect to cybercrime and the studies have also been conducted to focus on techniques to protect from cybercrime. Nevertheless, the area of cyber insurance as a means to

protect cybercrime has been left unexplored to determine its effectiveness. In recent years companies have seen a considerable increase in cyber-attacks, which are increasingly difficult to forecast and more sophisticated. In fact, only during the year 2013 could 740 million data files around the world been stolen (Rid and Buchanan, 2015). Despite these figures, companies continue to underestimate cyber risks such as theft, fraud and cyber sabotage. The concept of cyber liability insurance comes to rescue those companies, but its effectiveness needs to be evaluated.

1.2 Research rationale

Companies are increasingly dependent on new technologies and are increasingly exposed to risks that were never raised before, such as cybernetics. Thus, the best way to protect against cyber-attacks is to take out insurance that covers companies against these risks (Khalili, Naghisadeh and Liu, 2018). However, the effectiveness of cyber liability insurance is yet to be determined to claim that it is an answer against growing cyber-attacks. Therefore, it is necessary to conduct the study to evaluate whether the cyber liability insurance is an answer to growing cyber threats. Additionally, this research also highlights different types of cyber insurance, what they cover and to what extent they have been found reliable where the evidence from the literature will be explored. The rationale for the current research is to address whether cyber insurance is an answer to the growing cyber-attacks encountered by organisations. The recommendations based on these findings would also be presented to the companies in order to protect cyber-attacks.

Problem statement

Many companies in the contemporary business environment at risk of cyber-attacks face the problem that this present research aims to explore. Cyber risk is a real risk and suffering an attack of this type can have dire consequences. Among these consequences is the loss of data of the company and third parties, claims of third parties, complaints from the Data Protection Agency, loss of confidence or even cessation of activity (Keyser, 2017). In such cases, the need for cyber insurance was realised that enabled the companies to insure their data and protect it from theft.

Nevertheless, the effectiveness of cyber liability insurance to protect from cyber-attacks have yet to be determined and the companies that have relied on it have still suffered a data loss. Few of the world's renowned IT companies including Yahoo, eBay and LinkedIn have suffered data breaches in the last few years regardless of increased protection and huge investments to protect consumer data (Lee, 2015). Notably, present research aims to discuss the problem that whether cyber insurance, which has been marketed for a few years, helps mitigate the effects of cyber-attacks and whether it is an answer to the cyber-threats faced by the companies.

1.3 Motivation and need for research

With the advent and subsequent increasing popularity of smartphones and tablets, cybercriminals have ventured into the arena of attacking these mobile hand-held devices rather than computers. According to a report by McAfee (2010), there was an increase of about 46% in the number of malicious software programs (applications and games) specifically targeted to these hand-held devices. Also, the risk that arises as a result of human error and dishonesty of employees lead to events like the hacking of utmost confidential information as in the case of hacking of Google and WikiLeaks disclosures recently (KPMG, 2009). In view of these issues, the risk to information systems must be acknowledged and addressed, such that the risk can be mitigated at some level to avoid further damage or for damage control. Additionally, there is almost a certainty that each company and each organisation will have to face a data security breach (Lafuente, 2015).

In such a scenario, the preventive methods of risk mitigation do not seem to be foolproof. Corrective ways like cyber liability insurance are sought by companies to reduce their personal liability in case of any such occurrences. Cyber liability insurance is a necessary coverage that can support a company financially in the scenario of a cyber-attack posing huge financial losses (Lagazio, Sherif, and Cushman, 2014). In the case of cyber liability insurance, the calculation of premium and claims is done based on the estimated cost of loss resulting from a cybercrime. However, it is not possible to estimate losses resulting from the loss of intangible assets like goodwill and reputation, meaning they are not covered by insurance.

1.4 Research aim and objectives

The aim of this research is to evaluate the effectiveness of cyber liability insurance to determine whether it is an answer to growing cyber-attacks. In order to address these aims, the following research problems have been proposed:

- To explain and discuss cyber liability insurance and its types in light of literature.
- To determine the coverage of cyber liability insurance in protecting cyber-attacks.
- To investigate whether cyber liability is a viable option for small companies.
- To explore whether cyber liability insurance is an answer to growing cyber-attacks.

1.5 Research questions

Based on the problem statement and the knowledge gap, the following research objectives have been proposed to ensure that the research addresses the gap in the knowledge:

- What is cyber liability insurance and what types of cyber-attacks are covered?
- How much is cyber liability insurance effective in protecting cyber-attacks?
- Is cyber liability insurance a viable option for small businesses?
- Is cyber liability insurance an answer against growing cyber threats?

Literature review

2.1 Cyber liability insurance and its significance

Cyber liability insurance is a service offered to businesses or a policy that protects businesses and individuals from the risks associated with information technology activities and infrastructures. According to Chaisiri, Ko and Niyato (2015), cyber insurance can be an excellent tool to help transfer the risk in the event of a cybersecurity filtering, but only if it is applied with adequate foresight. The significance of cyber liability insurance cannot be undermined because cyber insurance is the correct assessment of damage resulting from an accident or an IT attack. This assessment is feasible and objective in a few cases. In this context, Meland et al. (2017) argued that the aim of cyber insurance is to protect the information that is associated with the company clients and sensitive information that can adversely influence the company and its reputation.

It has also been evidenced by Hoang et al. (2017) that in a typical data leak scenario cyber insurance would help with the costs of notifying about the attack, its analysis, repairs or restoration of data, and identity verification

The significance of cyber liability insurance cannot be undermined

services for victims. Consider a cyber-attack or incident that causes the unavailability of an e-commerce site for a limited and measurable period. In this case, the deriving damage can be calculated by analysing the turnover that this e-commerce site generated in similar periods. However, in most cases, this assessment is not at all simple. In such cases where the losses cannot be estimated in monetary terms, the companies cannot recover from the risks like customers' trust and their goodwill (Biener, Eling and Wirfs, 2018). However, in the cases where the economic damages can be estimated, cyber liability insurance is supportive where it not only covers restoration of data but also covers the costs including lawsuits and legal fees for the company, which makes it significant.

2.2 Types of cyber liability insurance and coverage extent

Two basic coverage types are insured with cyber insurance. The first covers the direct risks associated with the company, including the loss of or damage to company data. The second type of coverage is protection from third-party risks that include the responsibility to the clients, regulatory entities and associated stakeholders (Khalili, Naghisadeh and Liu, 2018). Most companies will prefer to have the benefits of both types of coverage. The most rigorously regulated, such as those pertaining to the education and health sectors, will have to ensure that they have good third-party coverage. According to Eling and Schnell (2016), if it is beyond the size of the company or the type of industry where the company belongs, it is best to start the search with a thorough risk analysis to determine how much coverage a company really needs. It is suggested to take into account all the groups that make up the organisation to include as many risks as possible.

On the other hand, a company may have two options to mitigate the huge financial losses resulting from a cybercrime. The company may either transfer the risk to an external insurance company by purchasing cybercrime insurance or it may assume the risk internally and financial provisions for the same by arranging funds for any potential future loss resulting from the attack, which is called self-insurance. However, self-insurance is not a very lucrative option since it is riskier in the sense that the company may not be able to make correct estimates about the possible losses (Jain and Kalyanam 2012). Cyber liability insurance, on the other hand, involves the transfer of the financial loss risk to the insurer to an extent that is measurable or calculable. In this context (Woods et al. 2017) argued that the companies offering the insurance plan for protecting cyber threats vary pertaining to the services offered. For some companies, it is often assumed that direct coverage includes notification to customers affected by data leakage, in some cases this service is not provided.

Collectively, the literature revealed that cyber liability insurance is very significant for the businesses to recover their losses by claiming for funds. Since the losses of the cyber-attacks are irreversible, the insurance policy is a significant answer because it raises funds to recover the organisational system and damages that otherwise would not have been possible (Laszka and Grossklags, 2015). However, two types were found in the liability insurance policy where the first covers the internal issues of the organisation, like data theft and data loss. Whereas the second covers third party cyber-attacks. Some of the policy covers both whereas some policies only cover the first type claims.

Evaluating effectiveness of cyber insurance

3.1 Effectiveness of cyber liability insurance

Cyber-attacks are one of the biggest risks that companies face today. Using robust computer systems with effective security, companies must cover the costs of a data breach and loss of digital assets. In such cases, it requires insurance coverage to cover the costs and damages due to breach and hacking whereas extensive insurance coverage can also cover reputation harm inflicted on the company (Hoang et al. 2017). Unfortunately, the more valuable digitally managed data is, the more incentives cybercriminals have and the more exposed companies are to the risks of a failure in the network compromising that data. The growing and increasingly stringent legislation around the responsibilities of a company in case of a cyber-attack only adds to the burden for them (Page, Kaur, and Waters, 2017). In this essence, the response of the cyber insurance coverage is to offer with the policies that other

Evaluating effectiveness of cyber insurance

insurance companies cannot cover that include the policies of material damage, liability and employee infidelity (Eling and Schnell, 2016).

Pertaining the effectiveness of the cyber insurance, it has been highlighted by Young et al. (2016) that the insurer identify the type of fraud within a day and take action to estimate and identify losses incurred to the company. Notably, cyber risk policies do not work just at the time of the problem, there is a team poised to be the head of the whole operation. However, if within 24 hours of the fraud the company does not take action, it loses value in the market. Additionally, with law firms triggered, public relations teams release communications including one from IT to verify the effect of the attack (Woods et al. 2017). This finding indicates that it is complex for the cyber insurance company to identify the type of cyber breach or cyber-attack and estimating the market value of the loss inflicted to be covered. Nevertheless, the insurance companies consult a professional IT company in this essence to sort out the type of coverage and the extent that should be covered.

3.2 Issues and limitations of cyber liability insurance

Although incidents and cyber-attacks are very numerous, insurance companies do not yet have sufficiently accurate actuarial statistics to be used as a basis for risk assessment. Moreover, considering the rapid evolution of information technologies and business models connected to them, many doubts emerge on the real usefulness of historical databases. According to Gottlieb (2017), it should also be considered that one of the main motivations for companies to consider the underwriting of cyber policies is the growing number and impact of deliberate cyber-attacks.

Even though there are companies and organisations that already have similar activities in their risk management plan, it is hard to believe that insurers make them mandatory for all customers wishing to take out an IT risk. Low (2017) said that there is a need to improve cyber insurance policies in order to address a number of concerns associated with risk assessment. It is clear that IT risk insurance will be the protagonists of a substantial growth.

Findings and discussion

4.1 Role of cyber insurance in preventing companies from cyber-attacks

A number of studies in this context have been presented in the literature where different researchers have argued and counter-argued using cyber insurance policies. It was found that cyber insurance policies are effective for the large companies and support them with the infrastructural development to protect from cyber-attacks. In order to avail the cyber insurance policies, the subscriber company or individuals work closely with the cyber insurance company to design a coverage that suits the specific needs of the subscriber. Another benefit highlighted by Chaisiri, Ko and Niyato (2015) to highlight its effectiveness is that it offers surveillance of the users that visit the website, identify malware, help determine how the attack occurred, and solve the problem so that company can resume their digital activity quickly and efficiently.

Cyber insurance policies are effective for large companies and support them with the infrastructural development to protect from cyber-attacks

To manage their reputation, cyber insurance is also effective as argued by Eling and Schnell (2016) that it helps to manage the response of the public relations manager to minimise the effects that may have on the company's reputation.

In addition, cyber insurance also offers other important services such as legal advice, especially with regard to compliance with regulatory requirements, as well as control of identity theft after a data privacy gap. Within the context of cyber insurance coverage, Lu et al. (2018) argued that the insurance mechanism is based on the insurer's ability to reliably estimate and predict the financial risk associated with the covered loss by studying past claims. It indicates that the cyber insurance cannot statistically predict financial risks and since the IT threats evolve rapidly and constantly, it requires continuous improvement, otherwise the policy would be susceptible for companies. On the other hand, the operating methods of hackers, typologies of attacks and security breaches are not the same from one year to another, so continuous improvement is necessary. Consequently, insurers find only limited predictive value in the study of past incidents, making it difficult to establish balanced insurance premiums.

4.2 Coverage of cyber liability insurance

Regarding the extent of cyber liability insurance coverage, a number of researchers have evidenced different aspects that are covered by cyber insurance companies. Nevertheless, one of the aspects that have been covered by most of the insurance companies is the damage to the digital assets where the costs of recreating and rebuilding digital assets that are damaged or lost, altered, corrupted or stolen, and any other cost to prevent, minimise or mitigate additional damages (Laszka and Grossklags, 2015). Another aspect that is covered by cyber insurance is damage to third parties and legal expenses as a result of unauthorised use or access to data networks, the transmission of a virus, denial of service attacks and other cybercrime (Lagazio, Sherif and Cushman, 2014). Additionally, it covers the costs of notifying victims of privacy violations and providing them with the necessary assistance after identity theft. Lu et al. (2018) emphasises that cyber insurance covers the damages and legal expenses for an illicit act with the publication of contents in electronic or printed media, including social networking platforms.

Although factors like customer loyalty and goodwill cannot be measured and cannot actually be covered, insurance companies support claims by providing funds to cover the loss of income to recover (Niyato et al. 2017). Over the passage of time, the coverage extent is being improved and broadened to ensure that the companies facing cyber threats overcome them using cyber insurance. In a context where innovation is going faster and faster, it is difficult, to take the time to identify and quantify the risks associated with the emergence of a new technology. However, this is a real opportunity for players in cyber insurance to rethink their offers and move a course, adapting to changing uses and associated cyber risk.

Findings and discussion
- continued

4.3 Cyber liability insurance for small businesses

This section highlights the evidence from the literature regarding small and medium enterprises to determine the effectiveness of cyber insurance policies and whether they are a viable option for small businesses. Pooser, Browne, and Arkhangelska (2018) argued that there are a number of reasons why small businesses are targeted for data breaches and hacked than large businesses, where the smaller companies are much more likely to have a limited IT staff department or none at all. Another reason identified in this context was that smaller companies are less likely to follow good internet security practices and often intermingle personal life and work, and they do everything with a reduced budget (Franke, 2017). Additionally, smaller companies have much simpler networks than a larger company does. They have a handful of computers and devices with a much less sophisticated configuration that is easier to penetrate.

Few other reasons that small businesses are more prone to risk is that they rely more on the cloud than a larger business with the IT infrastructure to support their own needs. Each time they access through the cloud, store or share something, they put the data, the network and the company at risk (Henson and Garfield, 2016).

Moreover, using a third-party solution to service a digital need through the internet also puts their company at risk in many ways. In comparison to large companies who have the power to analyse big data in their hands; the smaller companies cannot evaluate the malicious content in ads that they encounter. Large companies which can detect and deal with potential cyber threats in real time, as they occur, instead of trying to figure out what happened after the fact (Lafuente, 2015). For the smaller companies, the costs of cyber liability insurance can be higher so the researchers have suggested improving good internet practices to protect from cyber-attacks.

As also suggested by Low (2017) and Page, Kaur and Waters (2017), smaller companies should always use firewalls and internal servers for their data and websites to ensure data protection. Keeping their own servers safe does not eliminate all the risks, but it does reduce them to a more manageable level. Besides, firewalls are meant to protect the software and the connection requires entry into the network, which will prevent known or questionable threats from entering. Eling and Schnell (2016) suggest using anti-virus and anti-malware as these software packages protect company devices, networks, and data from infections that have happened despite the firewalls.

Moreover, Franke (2017) emphasises to back up the data as anyone who has ever used a computer or other digital device must know how to back up the data. The sad thing is that too few follow the advice and when their personal devices are infected, the data cannot be restored (Marotta et al. 2017). In summary, smaller companies are not more vulnerable to risks because of limited IT infrastructure but due to financial constraints. They also find it difficult to purchase a policy for cyber liability so were suggested to improve their work practices to protect from cyber threats.

4.4 Evaluating cyber insurance as an answer to growing cyber threats

The literature had highlighted a number of aspects covered by a cyber insurance policy to support threats where Abramovsky and Kochenburger (2016) and Henson and Garfield (2016) believe the development in this sector to support future cyber threats. In contrast, Woods et al. (2017) and Khalili, Naghisadeh, and Liu (2018) have a viewpoint that over the passage of time, the cyber-attacks would be more aggressive and destructive. This would challenge the companies offering cyber insurance policies. Nonetheless, the policies are decided and predefined to illustrate what would be covered and to which extent the cyber insurance company would support the victim of cyber-attacks. Therefore, based on the mutual understanding of the cyber insurance company and client, the limitations associated with the coverage can be addressed. In case of a cyber-threat, the victims may consult the insurer any time. Another concern that was raised by Young et al. (2016) emphasised the transparency of the cyber-attack that how the insurance company would evaluate the cyber-attack.

In response, it was revealed that the cyber insurance company would consult a professional IT company that would investigate and estimate the market value of the loss. Based on the evaluation of the cyber insurance company in line with the agreed policies would cover the victim with funds and financial support (Niyato et al. 2017). To sum up, it can be said that cyber insurance is not an ultimate answer to growing cyber threats because over the passage of time, cyber-attacks would be more destructive and the cyber insurance

policy is at the progressing stage. It needs more time to standardise and generalise the policy that covers all types of cyber-attacks including the growing cyber threats that arise in the future. For the large enterprises with a significant infrastructure, they need to utilise the policy because they have a growing threat of cyber-attacks that should be protected with policy in case of loss and destruction.

Besides, Pooser, Browne, and Arkhangelska (2018) argued that cyber insurance is effective in covering damage to property if the operative event is a computer attack that has permanently or temporarily rendered unusable an infrastructure of the enterprise. In addition, it is also the effective liability of a controller in the event of personal data breach, contractual non-performance following a computer attack crippling the company. For Laszka and Grossklags (2015) to insure against IT risks, it will be necessary to take stock of the vulnerabilities of the company, for example through risk mapping, vulnerability analysis and evaluation of the issues for the company. In addition, insurance covers the hazard, whether due to external attacks or human errors. The consideration and prevention of the hazard will help the company survive the unforeseen that is the security incident (Meland et al. 2017).

In this context, subscribing to cyber insurance will allow the company to be part of a process of prevention and compliance with regulations. In sum, the effectiveness of cyber insurance in some aspects is a viable option but the concept tends to innovate and improve over time to become more effective. Clearly, the assessment of the probability of an IT attack cannot be exclusively linked to statistical factors and is influenced by the quality and quantity of technological, training and organisational countermeasures that a company has implemented to protect its information assets. This assessment proves to be extremely complex (Hoang et al. 2017). Therefore, it is considered that more research is necessary in the context of a cyber insurance policy to determine whether it is an answer to growing cyber-attacks in the future.

Conclusion

These findings reveal that cyber liability insurance is designed to protect companies against any legal repercussions, recovery costs and other expenses associated with cyber-attacks.

In addition, cyber responsibility can help companies recover from business interruptions, reimburse for data breach expenses and provide assistance in any legal matter (Page, Kaur, and Waters, 2017). The research was conducted to determine the effectiveness of cyber insurance that covers responsibility for security and privacy, legal defence and bonds, third-party notification and crisis management expenses, administrative sanctions, multimedia liability, loss of income, data restoration and extortion of data (Lu et al. 2018). According to Marotta et al. (2017), a cyber-risk is the probability that a threat will materialise on a vulnerability of a computer system, causing situations that may include the loss of equipment, the theft of data, the action of hackers to manipulate data and actions. The consequences of a cyber-attack can be very serious.

Conclusion - continued

Different aspects and costs that can be covered with cyber liability insurance include the costs to hire specialists and lawyers to investigate and respond to a system failure or violation of privacy (Niyato et al. 2017). It also includes the costs of hiring crisis management experts and paying ransoms, if deemed necessary. Expenses resulting from research and defence of the procedures for regulating privacy in terms of rewards and fines might also be covered. In this context, Marotta et al. (2017) argued that the costs of notifying victims of privacy violations and provide the necessary assistance after identity theft are also covered. An important point raised by Chaisiri, Ko, and Niyato (2015) was that the costs of the related services are included to mitigate the damage to the reputation whereas Hale and Hirn (2017) opposed that the damages that are incalculable are not covered by cyber insurance.

In this sense, there are already examples of partnerships between companies specialised in vulnerability assessment and insurance groups, with the aim of accurately assessing the IT risk of medium and large customers approaching an insurance policy for the first time. Besides, taking action now can help reduce the exposure to cyber-attacks that can intentionally access through vendors and other networks. With the best cyber insurance coverage programs, companies can improve their ability to meet the new challenges of cyber risk. It was discussed in the literature that there are a number of aspects that are covered in the cyber liability insurance whereas there were also a few aspects that were not covered extensively. Particularly the aspects that are covered in the policy include digital assets, stolen or corrupted data, breach into the data systems and the costs associated with damages (Niyato et al. 2017).

Cyber insurance was also found to cover virus attacks and associated cybercrimes by the third party apart from the internal damage done like loss of data. Franke (2017) opposes that it cannot cover the defamation and reputable loss of the company including goodwill. However, there is evidence that the policy is improved by offering financial support to help secure goodwill and reputation in the event of a claim (Abramovsky and Kochenburger, 2016). Notably, the limitations and concerns with the cyber insurance persist but it is one of the best possible solutions for the large enterprises to get support in case of cyber-attacks. In sum, there is a significant role of cyber insurance companies to raise financial support and claims against cyber-attacks but it is a viable option for large organisations with a big IT infrastructure. The suggestion for smaller companies to protect themselves from cyber-attacks has been proposed but cyber insurance is not always an affordable option.

For future research, it is recommended to study the case of a company who suffers a data loss and had an insurance policy. It would comprehensively address the effectiveness of the cyber insurance policy. Additionally, it is also recommended to conduct a survey to evaluate how much smaller companies have undersigned cyber liability insurance and whether it helped. Besides, the viewpoint of the industry specialists in this essence is also important; therefore, the data in the form of interviews is necessary to explore the phenomenon comprehensively.

References

Abramovsky, A. and Kochenburger, P., 2016.
Insurance Online: Regulation and Consumer Protection in a Cyber World. In the" Dematerialised" Insurance (pp. 117-142). Springer, Cham.

Biener, C., Eling, M. and Wirfs, J.H., 2018.
Insurability of cyber risk. Methodology, p.9.

Chaisiri, S., Ko, R.K. and Niyato, D., 2015.
August. A joint optimisation approach to security-as-a-service allocation and cyber insurance management. In Trustcom/ BigDataSE/ISPA, 2015 IEEE (Vol. 1, pp. 426-433). IEEE.

Eling, M. and Schnell, W., 2016.
What do we know about cyber risk and cyber risk insurance? The Journal of Risk Finance, 17(5), pp.474-491.

Eling, M. and Schnell, W., 2016.
What do we know about cyber risk and cyber risk insurance? The Journal of Risk Finance, 17(5), pp.474-491.

Franke, U., 2017.
The cyber insurance market in Sweden. Computers & Security, 68, pp.130-144.

Gottlieb, M., 2017.
Is your salon cyber safe? Professional Beauty, (SepOct 2017), p.140.

Gupta, B., Agrawal, D.P. and Yamaguchi, S. eds., 2016.
Handbook of research on modern cryptographic solutions for computer and cybersecurity. IGI Global.

Hale, M.S., and Hirn, M.L., 2017.
Packing Their Parachutes: Advising Clients about Business Insurance Coverages. Mich. BJ, 96, p.24.

Henson, R. and Garfield, J., 2016.
What Attitude Changes Are Needed to Cause SMEs to Take a Strategic Approach to Information Security? Athens Journal of Business and Economics, 2(3), pp.303-318.

Hoang, D.T., Wang, P., Niyato, D. and Hossain, E., 2017.
Charging and discharging of plug-in electric vehicles (PEVs) in vehicle-to-grid (V2G) systems: A cyber insurance-based model. IEEE Access, 5, pp.732-754.

Keyser, M., 2017.
The Council of Europe Convention on Cybercrime. In Computer Crime (pp. 131-170). Routledge.

Khalili, M.M., Naghisadeh, P. and Liu, M., 2018.
Designing cyber insurance policies: The role of pre-screening and security interdependence. IEEE Transactions on Information Forensics and Security, 13(9), pp.2226-2239.

KPMG, 2009.
E-Crime Survey, Available at: www.kpmg.com/ FR/fr/IssuesAndInsights/ArticlesPublications/ Documents/20090501-e-crime-survey-2009.pdf.

Lafuente, G., 2015.
The big data security challenge. Network security, 2015(1), pp.12-14.

Lagazio, M., Sherif, N. and Cushman, M., 2014.
A multi-level approach to understanding the impact of cybercrime on the financial sector. Computers & Security, 45, pp.58-74.

Laszka, A. and Grossklags, J., 2015.
September. Should cyber-insurance providers invest in software security? In European Symposium on Research in Computer Security (pp. 483-502). Springer, Cham.

Lee, N., 2015.
Cyber-attacks, prevention, and countermeasures. In Counterterrorism and Cybersecurity (pp. 249-286). Springer, Cham.

References - continued

Liu, S., Wei, G., Song, Y. and Liu, Y., 2016.
Extended Kalman filtering for stochastic nonlinear systems with randomly occurring cyber-attacks. Neurocomputing, 207, pp.708-716.

Low, P., 2017.
Insuring against cyber-attacks. Computer Fraud & Security, 2017(4), pp.18-20.

Lu, X., Niyato, D., Jiang, H., Wang, P. and Poor, H.V., 2018.
Cyber insurance for heterogeneous wireless networks. IEEE Communications Magazine, 56(6), pp.21-27.

Marotta, A., Martinelli, F., Nanni, S., Orlando, A. and Yautsiukhin, A., 2017.
Cyber-insurance survey. Computer Science Review, 24, pp.35-61.

McAfee, 2010.
A Good Decade for Cybercrime, Available at: www.shabakeh.net/information/articles/mcafee/EN/rp-good-decade-for-cybercrime.pdf.

Meland, P.H., Tøndel, I.A., Moe, M. and Seehusen, F., 2017.
September. Facing Uncertainty in Cyber Insurance Policies. In International Workshop on Security and Trust Management (pp. 89-100). Springer, Cham.

Niyato, D., Hoang, D.T., Wang, P. and Han, Z., 2017.
Cyber insurance for plug-in electric vehicle charging in vehicle-to-grid systems. IEEE Network, 31(2), pp.38-46.

Page, J., Kaur, M., and Waters, E., 2017.
Directors' liability survey: Cyber-attacks and data loss—a growing concern. Journal of Data Protection & Privacy, 1(2), pp.173-182.

Pooser, D.M., Browne, M.J. and Arkhangelska, O., 2018.
Growth in the Perception of Cyber Risk: Evidence from US P&C Insurers. The Geneva Papers on Risk and Insurance-Issues and Practice, 43(2), pp.208-223.

Rid, T. and Buchanan, B., 2015.
Attributing cyber-attacks. Journal of Strategic Studies, 38(1-2), pp.4-37.

Woods, D., Agrafiotis, I., Nurse, J.R. and Creese, S., 2017.
Mapping the coverage of security controls in cyber insurance proposal forms. Journal of Internet Services and Applications, 8(1), p.8.

Young, D., Lopez Jr, J., Rice, M., Ramsey, B. and McTasney, R., 2016.
A framework for incorporating insurance in critical infrastructure cyber risk strategies. International Journal of Critical Infrastructure Protection, 14, pp.43-57.

The Chartered Insurance Institute
tel: +44 (0)20 8530 0997
info@socup.org.uk
socup.org.uk

Chartered Insurance Institute

@UnderwritingSoc

COH_J012913 01/21