Cyber-Insurance: Past, Present and Future

Sakshyam Panda[1], Aristeidis Farao[2], Emmanouil Panaousis[3], and Christos Xenakis[2]
[1]Department of Computer Science, University of Surrey, Guildford, UK
[2]Department of Digital Systems, University of Piraeus, Piraeus, Greece
[3]School of Computing and Mathematical Sciences, University of Greenwich, London, UK

Definitions

Cyber-insurance is an insurance product designed to protect businesses and individuals from information technology-related risks.

Outline

Insurance, in general, is a financial contract between the one buying the insurance (also known as the *policyholder* or *insured*) and the one providing insurance (known as *insurance carrier* or *insurer*). The contract, known as the insurance policy, typically states that the policyholder will pay a regular insurance premium in exchange for a financial compensation, also known as *indemnification*, in the event of a loss defined in the *insurance policy*. Insurance is used to manage risks by transferring them to the insurer, and cyber-insurance in particular deals with cyber risks covering direct and indirect damages caused by cyberattacks. The cyber-insurance market is still growing and has been receiving broader interest from research communities and government bodies over the years. This paper provides an overview of cyber-insurance, novel models proposed throughout the years and future challenges to be addressed for cyber-insurance to become a key component of an organisation's and household's cyber risk management approach.

Background

Today, computer networks play a critical role in defining the economic success of most organisations and are essential for providing critical services and managing sensitive data. Due to the importance of these network systems, they have become preferable targets for adversaries, and keeping these connected networks protected from adversaries is a priority. Many organisations have started considering cybersecurity as a critical business risk and, as a result, are seeking methods to ensure the continuity of their business. Despite the wide application of security measures, a challenging task for cybersecurity decision-makers is to assign limited resources across a range of possible security countermeasures to prevent or mitigate the effects of a breach. Although security countermeasures and practices are important, decision-makers should also consider other options to deal with residual risks as no amount of investment in cybersecurity can assure complete

S. Jajodia et al. (eds.), *Encyclopedia of Cryptography, Security and Privacy*,
https://doi.org/10.1007/978-3-642-27739-9_1624-1

protection. One of the alternatives to deal with residual risks is risk transfer where organisations besides implementing countermeasures transfer a portion of their cyber risk (residual risk) by purchasing cyber-insurance.

Insurance is a financial contract between the insured (the policyholder or the one buying insurance) and the insurer (one who insures). The contract, known as the insurance policy, typically states that the insured party will pay a regular insurance premium in exchange for financial compensation, also known as indemnification, in the event of a loss defined in the insurance policy. One of the first works in cyber-insurance was published in the late 1970s discussing specialised insurance coverage against computer crime. Early works in 1990s focused on the general merits of cyber-insurance (Anderson 1994). As firms became increasingly dependent on network systems and technology, traditional insurance policies fell short in providing the required coverage. To address this, insurance companies started offering stand-alone cyber-insurance policies. These policies offered coverage for a specific set of cyber risks. Table 1 presents the most common coverage and risks that the policy provides liability for, adopted from Woods et al. (2017).

The most prominent researcher who brought cyber-insurance into academic research was Schneier (2001), and from there on it has drawn heightened interest in the research community. Böhme and Schwartz (2010) have presented a framework supporting cyber-insurance modelling decisions. While modelling cyber-insurance, the attitude of the agents towards risks plays a critical role. Insurance, in general, requires agents to be risk-averse and seek to reduce cyber risks posed to their assets. Böhme and Schwartz (2010) examine modelling decisions based on five key components: (i) network environment, (ii) demand side, (iii) supply side, (iv) information structure and (iv) organisational environment. The proposed framework offers models and methods to deal with interdependent security risks (or correlated risk) which, along with information asymmetry, are considered as the main obstacles to the development of the cyber-insurance market. The interdependent security risks express the effect (known as externality) of an organisation's security investment decisions on other organisations. Based on the nature of the effect, the externality can either be positive or negative. In the case of positive externalities, the decisions of an organisation have positive effects on itself and others, e.g., increased endpoint security may decrease aggregated losses due to network attacks. On the other hand, negative externalities have negative impact on the organisation and others, e.g., lack of anti-malware system may negatively impact neighboured PCs, which is under a malware attack, since a number of neighboured PCs may be unintentionally infected. On the other hand, information asymmetry refers to the situation where there is insufficient information about the market and participants. Lack of adequate information leads to two challenging problems: (i) *adverse selection* where the insurer cannot distinguish organisations based on their risk profiles before the insurance contract is in place and (ii) *moral hazard* where insured organisations could undertake risky actions that affect the probability of loss during the contract period. A recent survey on the existing cyber-insurance market and scientific advancements is presented in Marotta et al. (2017).

Besides modelling, another stream of research develops analytical models to determine the cyber-insurance premiums based on the risk profile of the organisations. Mukhopadhyay et al. (2013) introduce models assisting organisations to decide on the utility of cyber-insurance products and to what extent they can integrate them into their procedures. The authors introduced an assessment algorithm based on copula-aided Bayesian belief network for cyber vulnerability assessment to price insurance products incorporating the risk profile and the wealth of the insured organisation. The model took a directed acyclic graph containing the nodes that could lead to a security breach as input and provided a vulnerability assessment report detailing the expected cyber risk value at each node of the graph. They derived the cyber-insurance premium based on the computed

Cyber-Insurance: Past, Present and Future, Table 1 The range of available cyber-insurance coverage

Coverage	Risks covered
First-party coverage	Coverage for the cost of replacing or restoring lost data. Excludes intellectual property
Data privacy and network security liability	Coverage for liability claims of a third party (e.g. a data breach or unintentional transmission of a computer virus)
Business interruption	Covers revenues lost as a result of network down time
Cyber-extortion	Cover for investigation costs, sometime the extortion demand
Public relations	Fees for public relations firm to manage reputation in the event of a breach
Multimedia liability	Costs relating to the content of a firm's website like copyright infringement
Professional services	Liability relating to a service offer such as web hosting or Internet service

expected cyber risk of the nodes. Finally, they introduce a model for assisting organisation to decide whether to transfer the cyber risk or to manage it in-house. Biener et al. (2015) took an alternative way by investigating cyber loss cases from an operational risk database to gain statistical insights between loss and cyber-insurance. A key finding was that organisations integrating cyber-insurance achieve to become more aware of risk-appropriate behaviours and protect themselves from cyber risks. The authors have also identified randomness of loss occurrence, information asymmetries, and cover limits as vital obstacles that hinder the development of the insurance market.

Growing cyber-insurance market has encouraged researchers to study various regulatory mechanisms including fines and rebates, liability coverage and competitive markets ensuring better investments in self-protection and acceptable cyber-insurance contracts. Despite the willingness in considering the cyber-insurance due to increase in number of cyber incidents, a gap exists between the current cyber-insurance assessment process and established security practices (Woods et al. 2017). These gaps can be bridged by coordination among the stakeholders belonging to both government and private sectors. To develop cyber-insurance market further, insurers should not only ask organisations to individually invest in cybersecurity in exchange for lower premium but also should take a proactive role in improving the overall security of their clients. However, such incentivising schemes might bring additional challenges for cyber-insurers as organisations might be inclined to misreport their actual security standards to gain lower premium. To counter such adverse scenarios, Panda et al. (2019) introduced a game theoretic model to study optimal auditing strategies against fraudulent claims in post-incident scenarios to prevent collapse of the cyber-insurance market when policyholders can fraudulently report their security levels.

Advantages

Apart from the primary advantage of transferring cyber risks, insurance in general and cyber-insurance, in particular, have additional benefits. First, cyber-insurance can be used to provoke organisations in increasing their investments in protection to reduce their insurance premium. Secondly, cyber-insurance is believed to improve the social optimum by increasing the level of cyber protection for each participant. Third, cyber-insurance can serve as an indicator of the level of protection of an organisation. Last but not least, cyber-insurance may lead to new and improved standards in cybersecurity. The growing market of cyber-insurance has encouraged researchers to study various regulatory mechanisms including fines and rebates, liability coverage and competitive markets ensuring better investments in self-protection and acceptable cyber-insurance contracts.

Key Challenges

The existing insurance industry and market have many challenges hampering the growth of cyber-insurance. First, there is a lack of experience and standardisation across cyber-insurance products offered by insurers. This indicates that those buying cyber-insurance products need to have a comprehensive understanding of their cyber risk exposure to determine appropriate cyber-insurance type as well as coverage required to address their risks. However, the fast-evolving computer systems and rapidly emerging technologies contribute to the changing cyber risk landscape making risk identification, likelihood determination and impact determination an extremely challenging task. Second, due to the novelty of the field and scarcity of data on cyberattacks and related losses, insurers face high uncertainty in pricing cyber-insurance products. Further, the complexity in accurately estimating risks leads to insurability of cyber risks, unclear coverage and higher premiums. Finally, the existence of externalities and information asymmetry may encourage some firms to not buy cyber-insurance or perform risky activities increasing the chances of loss during the contract period.

Acknowledgments This research has been funded by the European Union’s Horizon 2020 research and innovation programme under the Marie SkÅ, odowska-Curie SECONDO grant agreement No 823997.

References

Anderson RJ (1994) Liability and computer security: nine principles. In: European Symposium on Research in Computer Security, Springer, pp 231–245

Biener C, Eling M, Wirfs JH (2015) Insurability of cyber risk: an empirical analysis. Geneva Papers Risk Insur Issues Pract 40(1):131–158

Böhme R, Schwartz G (2010) Modeling cyber-insurance: towards a unifying framework. In: WEIS

Marotta A, Martinelli F, Nanni S, Orlando A, Yautsiukhin A (2017) Cyber-insurance survey. Comput Sci Rev 24:35–61

Mukhopadhyay A, Chatterjee S, Saha D, Mahanti A, Sadhukhan SK (2013) Cyber-risk decision models: to insure it or not? Decis Support Syst 56:11–26

Panda S, Woods DW, Laszka A, Fielder A, Panaousis E (2019) Post-incident audits on cyber insurance discounts. Comput Secur 87:101593

Schneier B (2001) Insurance and the computer industry. Commun ACM 44(3):114–114

Woods D, Agrafiotis I, Nurse JR, Creese S (2017) Mapping the coverage of security controls in cyber insurance proposal forms. J Internet Serv Appl 8(1):8