The Economics of Cyber-Insurance

By: Nir Kshetri

Kshetri, Nir (2018)." The Economics of Cyber-Insurance" *IEEE IT Professional*, 20(6), 9-14.

Made available courtesy of IEEE: https://doi.org/10.1109/MITP.2018.2874210

Abstract:

The cyber-insurance market currently is at a nascent stage. According to the German reinsurance company Munich Re, worldwide spending on cyber-insurance was US3.4−US4 billion in 2017, which is estimated to increase to US8−US9 billion by 2020 (https://tinyurl.com/ycrwhvlf). Cyber-insurance premiums currently account for only a tiny fraction of total insurance premiums. For instance, only in OECD economies do total insurance premium exceed US$5 trillion in 2016 (https://data.oecd.org/insurance/gross-insurance-premiums.htm).

Keywords: Insurance | Economics | Computer crime | Market research | Computer security | Financial management

Article:

The economic costs of cyberattacks exceed those associated with natural disasters (https://tinyurl.com/y8w9gpwy). According to Juniper Research, the cost of data breaches would amount US$2.1 trillion globally by 2019 (https://tinyurl.com/y7yukpcx). Most estimates of cyberattack costs overlook the harms associated with damage and destruction of data, lost productivity, theft of intellectual property, personal and financial data, post-breach disruption of companies' businesses, forensic investigation, restoration of hacked data and systems, and reputational harm. Some of these are more difficult to measure. Including those costs, Cybersecurity Ventures estimated that cybercrimes cost the world US$3 trillion in 2015, which will increase to US$6 trillion annually by 2021 (https://tinyurl.com/y7jxx3zw). Organizations are thus finding it more imperative to have cyber-insurance.

Cyber-insurance enhances firms' cybersecurity performances. For instance, a company is required to strengthen cybersecurity in order to buy coverage at a lower rate. A system that requires cyber-insurance thus raises cybersecurity standards.

Unsurprisingly, regulators are pushing for increased investment in cyber-insurance. For instance, New York's Department of Financial Services (DFS) has urged financial companies to invest in cyber-insurance.

CYBER-NSURANCE: EXPLANATION AND THE CURRENT STATE

Cyber-insurance has been available since the 1990s.[1] Despite this long history, cyber-insurance has not yet taken off.

The U.S. cyber-insurance market is more advanced than the rest of the world (see Table 1). According to Marsh & McLennan, global cyber-insurance premiums was about US$3.5 billion in 2016 of which the U.S. and Europe accounted for US$3 billion and US$300 million, respectively (https://tinyurl.com/ycb7hrzv).

Table 1. Cyber-insurance markets in some key economies.

Economy	Cyber-insurance premiums	Total insurance premiums (US$, billion)	Cyber-insurance premiums as a proportion of total insurance premiums
Brazil	US$645,800 (2016) (https://tinyurl.com/yc6u4ap4)	58.9 (2016)[a]	0.001%
Germany	US$105-117 million (https://tinyurl.com/y8ypu8jw)	327.3 (2016)[a]	0.03%
India	US$ 27.9 million (2017) (https://tinyurl.com/y84jgxm2).	69.8 (2016)[a]	0.04%
Japan	Japan Network Security Association's estimate: US$134.2 million (2017) (https://tinyurl.com/y8l4jxlz)	407.4 (2016)[a]	0.03%
South Korea	US$26.4 million (2016) (https://tinyurl.com/yafs4p27).	185.6 (2016)[a]	0.01%
The U.S.	Verisk: commercial cyber-insurance market: US$ 6.2 billion by 2020 US$ 2.5 billion in 2016 (https://tinyurl.com/ydf7z28s).	2703.8 (2016)[a]	0.09%

a. *OECD. Gross insurance premiums, https://data.oecd.org/insurance/gross-insurance-premiums.htm.*

The cyber-insurance penetration rate is especially lower among small and medium sized enterprises (SMEs). In most OECD countries, the penetration level for stand-alone cyber-insurance among large companies was reported to be above 50% in 2017. The proportions of SMEs with cyber-insurance were in the single digits (https://tinyurl.com/ycyugnjm). Among big companies, data intensive companies exhibit a higher propensity to buy cyber-insurance. In India, only banks and ecommerce companies were reported to have cyber-insurance with large coverages (https://tinyurl.com/y84jgxm2).

Cyber-insurance provides coverage for the theft or loss of first-party and third-party data, as well as support services.[2] For the loss or theft of first-party data, an insurer may cover expenses related to notifying clients regarding the data breach, purchasing credit monitoring services for affected customers, extortion, and launching a public relations campaign to restore the company's reputation following a cyberattack-led negative publicity.

Third-party cyber-insurance protects a firm from being accused in case of a breach. Third-party coverage includes claims related to unlawful disclosure of a third-party's information and infringement of intellectual property rights (https://tinyurl.com/yb2vter9). It may also protect if

an insurance holder's weak cybersecurity practices result in passing malware or virus to another user.[3]

Support services can help limit losses after a cyberattack. They cover expenses such as those related to public relations, IT forensics, and hiring experts in crisis management.

Some Challenges

The cyber-insurance industry and market have some major challenges to overcome. First, there is a lack of standardization across the cyber-insurance products offered by insurers. This means that those buying insurance products are required to have a clear understanding of their cyber risk exposures in order to determine the appropriate type as well as the amount of coverage required based on their specific situation.[4] According to a survey conducted by Marsh, 49% of respondents said that they had "insufficient knowledge" about their cyber risk exposures to assess the type and coverage of insurances they need.[4] Likewise, another survey found that 38% of U.K. companies had insurance that covered all types of cyber-threats. However, most policies were based on inaccurate risk assessments (https://tinyurl.com/yc8xnzux).

Second, the value chain of the cyber-insurance industry is not well developed. There is the lack of clear understanding and knowledge among intermediaries such as insurance brokers and insurance agents. For instance, according to survey conducted by U.K. legal expenses insurer DAS UK Group, and HSB Engineering Insurance, most insurance brokers in the U.K. were reported to view cyber-insurance as a key and growing market. Nevertheless, one third of them admitted that they had a "poor" or "very poor" understanding of cyber risks and cyber-insurance (https://tinyurl.com/y7675y3u).

Third, due primarily to newness and the scarcity of data on cyberattacks and related losses insurers face a high uncertainty in pricing cyber risk coverage. They thus tend to be conservative and overcharge for cyber risk coverage.[3] Moreover, various cyber-insurance coverages are separately priced.

Fourth, the existence of externality effects may discourage some firms to buy cyber-insurance. If a minimum level of cybersecurity is required from policyholders, it is likely to improve the security of all Internet users. This will create a free riding problem, which reduces incentives for individuals or firms to get cyber-insurance.

DEMAND- AND SUPPLY-SIDE MODELS AND MEASUREMENT ISSUES

Supply-Side Condition

In order to derive a risk-adjusted return on capital, insurance companies need to determine the economic values of the capital invested and earnings. Put simply, the economic value of earnings is equal to cash flow plus the change in the economic value of the assets minus the change in the economic value of liabilities.[5] Expressing in a simple equation, it is commercially viable for the insurance company if

Insurance premium > expected loss + risk margin + administrative costs. (1)

The risk margin in (1) represents an additional amount that investors in an insurance company require so that a return is expected for placing their economic capital at risk.[5] The risk associated with a policy is a function of many factors such as the company's industry, data risks and exposures, current practices, and financial health.[5] Among the biggest challenges facing the cyber-insurance industry and market is the lack of well-developed mechanisms to actuarially assess and price cyber risks.

Firms face heterogeneous cyber risk environments. In order to understand the essential components and the context of cyber risks, a process-based mode of such risks could be helpful. In such a model, risk equals "threat plus vulnerability plus consequences" (https://tinyurl.com/yc7ycokf). A threat is a danger related to cyber-attack that has the potential to cause harms to an organization. For instance, factors such as a firm's jurisdiction, physical location, nature of business, political orientation, and symbolic significance affect the degree of cyber-threats.

Cyber-vulnerability refers to the degree to which an organization is susceptible to harm from cyber-attacks. For instance, a firm with a poor cybersecurity practice is more likely to be harmed by cyber-criminals.

Finally, consequences of possible cyberattacks need to be evaluated in terms of factors such as reputational damage, financial loss, and possible physical harm. More severe consequences can arise if the jurisdiction of the firm's operations has strict laws against companies' failure to protect personally identifiable information.

Proper assessment of cyber-threat, cyber-vulnerability, and consequences of cyber-attacks are needed to gain a better understanding of cyber risks facing the firm. Insurance companies have realized that there is a fundamental need for better risk assessment tools.

On the plus side, there have been efforts to develop better analytical approaches, improving data collection efforts, and sharing relevant data with other players. When insurers model and test more information, insurance products are likely to be sold at more reasonable prices. Insurance companies are also taking measures to address legal uncertainties.[1]

Demand-Side Condition

A customer will invest in cyber-insurance if expected utility without cyber-insurance < expected utility with cyber-insurance (2)

Alternatively, the demand-side condition can also be written as[6,7]

U(Benefits of insurance) > U(Costs of buying an insurance plan). (3)

U(*) is a utility function, which evaluates a cyber-insurance plan's benefits and costs in a common metric.

Firms and individuals invest in cyber-insurance only if its value proposition is clear. A current challenge is that the coverage terms are often complex, which makes it difficult to articulate the value proposition. There is still the lack of data on the odds of companies being victimized, which makes it difficult to estimate the costs of cyberattacks. It is also difficult for companies to measure the nature and extent of cyber-related exposure and to make decisions as to what coverages for how much to purchase (https://tinyurl.com/y7g3fjuy).

A related point is that some cyber-insurance policy holders find that their insurance does not cover all the losses in case of a cyberattack. To take an example, in December 2013, Target faced a high-profile security breach, which compromised 40 million credit and debit-card accounts and 70 million customers' personal data (https://tinyurl.com/y9vgktf3). Target had cyber-insurance when it was hacked. However, it only covered the first US$100 million. Actual costs exceeded US$450 million.[3]

Transaction Costs in Cyber-Insurance Markets

In the context of business transactions involving two or more parties Nobel Laureate Douglas North argues that ".. transaction costs are . . . two things: (1) the costs of measuring the dimensions of whatever it is that is being produced or exchanged and (2) the costs of enforcement."[8] He goes on to say that "a lot of what we need to do is to try to measure the dimensions of what we are talking about in such a way that we can define them precisely."[3] Emphasizing the importance of measurements in enforcement, North argues: "Without being able to measure accurately whatever it is you are trying to enforce, there cannot be effective enforcement, even as a possibility."[8]

A transaction cost problem has two main components: (a) There is the presence of uncertainty and (b) the ability of the policy holder to change her/his behavior without detection.[9] Regarding (a), it is worth noting that due to the newness and limited availability of data, there is a challenge in estimating the probability of cyberattacks.

As to (b), a key challenge that insurers face in other types of insurance products is that the behavior of policy holders is often unobservable. Unlike many other insurance products, by working closely with the policy holder, cyber insurers can avoid some of the above-mentioned problems. They can support overall risk management for their clients and tailor cyber-insurance to only residual risks in a cost-effective manner. For instance, using specialized software, insurers can remotely check whether policyholders have up-to-date software and defense mechanisms in place.[1] There has already been some progress on this front. Companies with strong cybersecurity practices pay lower insurance premiums.[1]

The above-mentioned feature also leads to a lower enforcement costs. A second-party enforcement, in which one party retaliates against the other (e.g., a cyber insurer penalizing a cyber-insurance policy holder for having a poor defence measure), can especially be more easily carried out in the context of cyber-insurance. It reduces the risks of policyholders failing to protect themselves against cyberattacks, thinking that they are covered against losses associated with such attacks.[1]

CONCLUSION

Cyber-insurance market currently accounts for a vanishingly small proportion of the total insurance market. Nonetheless, it is growing fast. There are challenges associated with actuarially estimating the likelihood of cyberattacks and the total anticipated costs of such attacks. The lack of relevant data has led to an inaccurate assessment of cyber risks and higher premiums.

On the plus side, insurers can remotely monitor policyholders' cyber-defense mechanisms. It provides a low-cost mechanism for a second-party enforcement.

It is important to have a thorough understanding of the multifaceted nature of loss in case of cyberattacks. For non-IT businesses, first-party cybersecurity insurance could be enough, but third-party cybersecurity insurance may be needed for firms dealing with sensitive data of customers.
Since most current policies are bespoke in nature, firms need to look for policies that are based on the need rather than the cost.

Due to the lack of prior experience, potential clients do not immediately understand the value proposition of cyber insurance. It has resulted in low demand. Cyber-insurance education and awareness can make a big difference. A higher public awareness of cyber security risk and a higher degree of understanding of the sophistication of cyberattacks can also stimulate the demand of cyber insurance. Firms should be convinced that the value proposition of insurance is interesting for them. Insurers need to make sure that potential clients get a simple and clear explanation of benefits from their cyber insurance. It is important to take measures to increase perceived economic benefits of cyber insurance.

Insurers must consider new market segments that are not currently investing in cyber insurance. They need to pursue firms in industries low digitization, households, and SMEs.

Data protection regulations that require financial protection against cyber-related losses could also lead to the growth of the cyber-insurance market. Finally, proper regulations may address the free-riding problem. Measures such as those taken by New York's DFS indicate that there have been some initiatives on this front.

REFERENCES

1. iif.com, "Cyber risk insurance: A growth market adapting to a changing risk," Insti. Int. Finance, Washington, D.C., USA, Dec. 7, 2017.

2. C. P. Baban, Y. Gruchmann, C. Paun, A. C. Peters, and T. H. Stuchtey, "Cyber insurance as a contribution to IT risk management: An analysis of the market for cyber insurance in germany," 2017, Brandenburg Inst. Soc. Security gGmbH

3. L. DeFranco, “What you need to know about cybersecurity insurance,” 2017. Available at https://blog.abacus.com/basics-of-cybersecurity-insurance/

4. Marsh & McLennan Co., “Cyber risk in Asia-Pacific the case for greater transparency risk in focus series,” 2017.

5. L. Rubin, M. Lockerman, R. Tills, and X. Shi, “Economic measurement of insurance liabilities: The risk and capital perspective,” 2009. Actuarial Practices Forum.

6. H. P. Binswanger-Mkhize, “Is there too much hype about index-based agricultural insurance?” J. Dev. Studies, vol. 48, no. 2, pp. 187–200, 2012.

7. D. S. Nagin and G. Pogarsky, “Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence: Theory and evidence.” 2001. Available at http://onlinelibrary.wiley.com/doi/10.1111/j.1745-9125.2001.tb00943.x/abstract

8. D. C. North, “Dealing with a nonergodic world: Institutional economics,” Property Rights, Global Environment: Duke Environment, Law, Policy Forum, vol. 10, no. 1, pp. 1–12, 1999.

9. D. W. Allen, “Transaction costs,” in B. Bouckaert and D. G. Gerrit, Eds., The Encyclopedia of Law and Economics. Chelthenham, UK: Edward Elgar, 2000, vol. 1, pp. 893–926.

ABOUT THE AUTHOR

Nir Kshetri is a Professor of Management with the Bryan School of Business and Economics, University of North Carolina at Greensboro, Greensboro, NC, USA. Contact him at nbkshetr@uncg.edu.