UK FINANCE

CYBERSECURITY INSURANCE FOR A RESILIENT ECONOMY?

May 2022

EXECUTIVE SUMMARY

Insurance policies for cybersecurity incidents have been on the market for a number of years now. During that time the market has evolved and with it the sophistication of the coverage and underwriting, as well as the threat faced by firms.

With the growing prevalence of cybersecurity threats and the number of victim firms increasing, policy makers are considering whether cybersecurity insurance should be a mandatory requirement. Potential benefits include not only loss coverage, but the chance that cybersecurity insurance could direct or guide secure behaviours in firms.

UK Finance has worked with the Association of British Insurers and the International Underwriters Association to gain an understanding of the experience across the market for cybersecurity insurance and the effect holding such coverage has on firms we represent within the banking and finance sector.

We considered several aspects of cybersecurity insurance coverage and the market below. Our conclusion is that based on the current state of the market and the external threat facing firms, while there are some benefits of cybersecurity insurance from a loss coverage perspective, it is not clear that policy coverage will change behaviour, uplift resilience environment, or improve the overall exposure of the economy to cybersecurity threats. Financial sector regulators expect organisations to be resilient irrespective of the maturity of their coverage, underwriting practices or policy wording.

Is it best practice for firms to hold cybersecurity insurance?

Financial institutions (FIs) often hold cybersecurity insurance with significant coverage. These policies are typically constructed to focus on catastrophic events with significant economic consequences, rather than the lower tier of cybersecurity incidents. This is in line with other corporate insurance policies which are also focused on the lower-probability, high-impact events (for example, in the area of property insurance).

FIs are also increasingly requiring their third parties who hold or have access to sensitive information to hold a cybersecurity insurance policy. The purpose of such policies is to provide the FI with assurance in the event of a catastrophic cybersecurity incident that the third party will remain financially viable and able to continue providing the service in the short term.

To what extent could cyber insurance direct and guide secure behaviours?

While some insurance firms are actively attempting to improve their information collection, there are practical limits to the level of detail and sophistication of analysis that underwriters can perform in the course of underwriting an insurance policy.

Current practices such as the completion of a simple online form cannot provide the level of insight or understanding that would be necessary for underwriters to begin to

pressure firms into improving their behaviours and overall cybersecurity stance through policy pricing. Where insurers require and seek more detailed information regarding a firm's technical practices, such information could itself be a risk to the reporting firm; more sophisticated firms with cybersecurity insurance policies often provide only verbal information to underwriters rather than risk exposure of detailed information regarding their security practices.

Where cybersecurity insurance is to be mandated, as some policy makers such as the European Insurance and Occupational Pension Authority (EIOPA) have theorised, current assessment practices would continue to limit the ability of insurance to drive firms' behaviour.[1] It is likely that to fill the void, an industry would develop cybersecurity assessments. Participants would compete to gain market share by marketing their assessment methodologies. This would be likely to lead to a cottage industry of assessors that would leave the market no better off in terms of impact on firms' behaviour, as there would be no common understanding of best practice.

The situation could be improved with greater use of the Cybersecurity Profile, a financial services industry-led cybersecurity assessment tool.[2] Use of the Profile would more easily allow firms to benchmark their cybersecurity practices compared to the bespoke questionnaires currently used by insurance firms. Benchmarking would allow not only for better pricing of risk, but by operating within the framework provided by the Profile, firms would have a roadmap to improving their cybersecurity risk management.

Will the insurance market continue to be viable as the prevalence of attacks increases?

Ransomware attacks have proliferated through the economy and in supply chains, adding pressure to the cybersecurity insurance market along the way. In the context of a tightening insurance market more generally, the continued success of ransomware may lead insurance providers to exclude ransomware from their coverage in order to maintain the viability of their wider policies. We are already seeing indications of significant rises in policy costs as insurers adjust to the prevalence of ransomware attacks. Should that trend continue, it may become untenable for larger firms to require suppliers to maintain cyber insurance coverage.

This risk is compounded by the behaviour of some firms in the supply chain or smaller start-ups who have demonstrated a willingness to accept significant liability in the case of a cybersecurity incident. Such behaviour and the inevitable consequences could constrain underwriters in the future.

1 EIOPA, Cyber security and cyber risk, a universal challenge, 2019. https://www.eiopa.europa.eu/content/cyber-security-and-cyber-risk-universal-challenge

2 Originally known as the Financial Services Sector Coordinating Council (FSSCC) Cybersecurity Profile, the Financial Services Profile (FSP) in Europe, and the Profile in the United States, the non-profit Cyber Risk Institute's (CRI) Cybersecurity Profile was a collaborative effort of 150 financial firms and more than 300 bank representatives over several years. The result is a unified harmonized approach to cyber security assessments that can be used by the smallest and the largest financial services firms: banks, securities, and insurance. The CRI Cybersecurity Profile is recognized as a global cyber tool and convergence instrument bringing together a catalogue of global security standards, regulations, and legal framework requirements. www.cyberriskinstitute.org

As the scale of the cybersecurity threat to the economy increases, we may see cybersecurity insurance become an area that is simply too problematic for the market to cover. In such an event the market may respond by firms of similar size and risk profile forming a risk retention group to pool resources to cover risk. This may have the added benefit of encouraging improved standards as firms will seek to hold each other accountable. Additionally, the government may choose to intervene to provide a backstop for insurers. The precedent for such an intervention comes from the role the US government played in terrorism insurance following the events of September 11, 2001.

Do exemptions make cyber insurance unreliable (e.g., war and terror)

There have been well-publicised concerns related to the limits of cybersecurity insurance. The focus on war and terror exemptions are connected to the well-known difficulties of attribution for cyber-attacks. Another consideration is whether a firm was specifically targeted for the cyber-attack or a victim of a broader campaign. Untargeted organisations may not be covered under some policy terms, leaving the victim without compensation. As the nature of the ransomware market evolves, we expect this exemption to become more significant.

Beyond these better-known areas, there are questions about the limits of policy coverage for physical damage caused through cyber means (e.g., a cyber-attack activates a building's sprinkler system). We have also observed a focus on data breaches in policies as compared to coverage for systemic events. These concerns raise questions as to whether the insurance market is segmenting too much, leading to unclear coverage limits.

Does insurance covering ransomware encourage payment and therefore further attacks?

According to the 2022 cyber security breaches survey published by the UK government, when asked about the insurance coverage within the financial and insurance sector, 60 per cent of respondents reported having some sort of coverage against cyber security breaches. Of those with some sort of coverage, a tiny proportion have made an insurance claim on a cyber-attack.[3] In the US, the Treasury Office of Foreign Assets Control (OFAC) and Financial Crimes Enforcement Network (FinCEN) have both issued recent advisories warning firms about the sanctions risk they incur by using the financial system to pay ransoms.[4]

Insurers often bring in third parties to engage with their client in the event of a cybersecurity incident, including ransomware, and some may even facilitate the payment of the ransom on behalf of their clients. They often recommend that their clients pay the

3 2021/2022 UK Government Cyber Security Breaches Survey. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

4 FinCen Advisory FIN-2020-A006, Advisory on Ransomware and the use of the Financial System to Facilitate Ransom Payments. https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf

ransom if the costs of doing so are less than cleaning and rebuilding the IT environment. Payment of ransoms should not be made illegal and must be a last resort where nothing else can be done to protect the confidentiality and integrity of the data.

While it is difficult to conclude that insurance covering ransomware encourages payment and further attacks and apart from the sanctions risk this raises for firms, if the economics of insurance leads insurers and firms to more frequently pay ransoms then there is the potential that insurance is facilitating the growth of ransomware attacks. If true, this could create a vicious circle that plays into the previous concern regarding the ability of cybersecurity insurance to sustain coverage for ransomware.

Would the prevalence of cybersecurity insurance in a particular market or market segment encourage the attention of threat actors?

A connected issue is whether the prevalence of cybersecurity insurance in a particular market may in fact encourage targeting of that market by threat actors. There are precedents for insurance coverage encouraging the commission of the very crime it is meant to cover (e.g., kidnap insurance).

While there is not yet enough statistical evidence, anecdotal evidence, such as the above statements from FinCEN, suggest that the increased prevalence of cybersecurity insurance in an economic sector or a specific national economy may increase the attractiveness of that economy to threat actors who may consider payment more likely under such conditions.

Should the government collect data on cyber breaches to facilitate the insurance market?

There has been an increase in recent years of information available on cybersecurity breaches, raising the question of whether further data would benefit underwriters. It is also the case that, depending on the type and level of coverage being sought, underwriters will consider market scenarios and firm-specific data to determine costs rather than wider statistics. The government is not expected to outrightly ask organisations to provide data on cyber breaches with the exception of peculiar cases where critical national infrastructure is involved or scenarios with possible significant impact to the economy. Insurance bodies may choose to work with organisations such as the Information Commissioner's Office (ICO) to receive secure access to data submitted directly to the ICO in scenarios where said data would be beneficial for underwriters.

Could cybersecurity insurance be required?

The potential for authorities to require firms to maintain cybersecurity insurance coverage raises a number of questions. The type and level of coverage would need to be determined by the firm according to their own risk profile and appetite. The variation in coverage that may result would have implications for the policy objectives that such a requirement was attempting to achieve.

An additional question arises from the increasingly outsourced nature of IT operations. With firms more often relying on IT infrastructure or services provided by a third party, such as a cloud provider, would

they have the necessary ability to flow down clauses in their insurance policies to their sub-contractors?

Finally, cybersecurity insurance policy costs would represent an opportunity cost. With the threat and risk to insurers increasing, costs are expected to rise. Under such circumstances firms may be better off allocating scarce resources to improving their cybersecurity and resilience rather than purchasing insurance.

Conclusion

The debate on the merits of cybersecurity insurance for resilience is live and evolving, much like the technology and threat environment to which it is intimately linked. We have provided views based on our member experiences to date. These experiences suggest that in the event of an incident the primary benefit of cybersecurity insurance is financial; cybersecurity insurance is currently acting as a risk transfer mechanism but not primarily to uplift security posture. Therefore, if the objective is to improve the cybersecurity posture and resilience of firms, there may be merit in those firms considering additional investments to improve their said posture.

As the market continues to evolve, cyber insurance may be able to play a more prominent role in improving the behaviours of policy holders. Key to this change will be underwriting practices, most notably the methods for assessing firms' security practices and controls framework. The Cybersecurity Profile would be a viable tool for this purpose and its use should be considered by insurance companies.

The potential for cyber insurance to be made mandatory is still being discussed and no definite conclusion is yet possible. For policy makers, it will be important to consider carefully the various concerns raised in this paper when determining whether certain sectors or firms should be subject to cyber insurance requirements. The current state of the market suggests that a blanket requirement is unlikely to be successful and, therefore, carefully constructed rules will be necessary requiring input from multiple sectors, not only insurance providers.

AUTHORS:

Ian Burgess
Director, Digital, Tech and Cyber, UK Finance

Oge Udensi
Principal, Cybersecurity, UK Finance