RESEARCH BRIEF:
Cyber Insurance as a Risk Mitigation Strategy

THE GENEVA ASSOCIATION

Contours of an emerging market for cyber risk transfer

Daniel M. Hofmann, Senior Advisor Financial Stability and Insurance Economics, The Geneva Association

Cyber insurance is the fastest growing line of business in the insurance industry. A combined assault of daily front-page news items about cyberattacks, increasing government regulation, and insurance industry awareness is raising the profile of cyber risk. According to surveys, 99 per cent of all boards of directors discuss cyber risk on a regular basis,[1] and 80 per cent of CEOs consider cyber risk as the number one threat to business growth.[2] As more regulations are adopted, the corporate sector is looking to insurance to offer solutions that can effectively deal with this emerging risk

THE CHALLENGE TO CREATE NEW SOLUTIONS

If not properly addressed, cyber risks have the potential to constrain and even reverse the forward momentum created by digitisation, which could adversely impact growth and prosperity around the world. This opens up an opportunity for the insurance industry to help mainly corporate and commercial customers to better manage and mitigate cyber risk. The new offerings, however, are not free of challenges. Cyber risk is unique and at this point still not well understood by either insurers or their customers.

THE UNIQUE NATURE OF CYBER RISK

Cyber incidents can not only occur with high severity, they can also occur with high frequency.

Insurance companies are used to dealing with risk. But cyber appears to be different. Based on many years of observations, we know that natural disasters occur with a certain frequency. For example, the likelihood of having several simultaneous earthquakes around the world is very small, but cyberattacks can happen to any number of organisations simultaneously and repeatedly. And having experienced a malicious cyber attack (such as the WannaCry attack), does not rule out re occurrence. This will depend on the speed of identification, analysis, and mitigation measures being put in place, and whether the second attack targets the original vulnerabilities or new unidentified ones.

One of the foremost challenges in the cyber security landscape is accumulation risk.

More and more companies are using common platform software (e.g. SAP) and they rely on third-party solutions such as the cloud to support their businesses. This creates common exposures and it increases interconnectivity. This makes them vulnerable to failures in or malicious attacks on the common platforms and support systems provided by third parties. Insurers call this accumulation risk, which according to 90 per cent of senior industry executives is seen as a critical challenge. As a first consequence, a large number of insurers have decided not to cover risks associated with cloud or software vendors.

If the industry wants to be in a position to successfully manage the potential of extreme losses associated with accumulation risk, it needs to create better risk models and educate customers to help them understand their accumulation risk exposure. This requires, among other factors, the collection and sharing of incident data which could help in building more sophisticated cyber risk models.

There are several efforts facilitated by governments and the insurance industry to create a common data repository and to standardise the classification and reporting of cyber incidents. One of the most important initiatives is CIDAR, led by the Department of Homeland Security in the U.S.

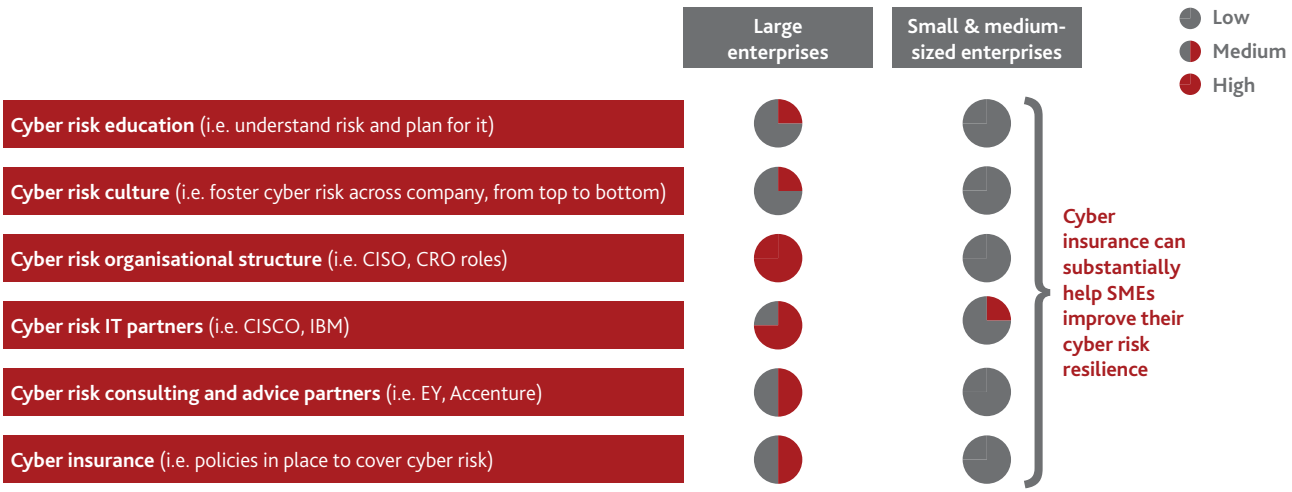
In addition to supporting a common data repository, insurers could assume an important role in the propagation and enforcement of minimal IT-security and information-security standards.

1 Survey of clients (2015)
2 PwC survey of clients (2016)

THE ROLE OF INSURANCE IN CYBER RISK TRANSFER

According to recent estimates, the size of the global cyber insurance market is believed to fall in a range from USD 2.5 billion to USD 3.5 billion in gross written premiums (estimates for 2016). Industry participants reckon that the market may grow to USD 10 billion by 2020 and up to USD 20 billion by 2025.

Figure 1: Cyber risk readiness by customer segment



Source: Interviews

In order to secure their market share, underwriters must seek to better understand their customers. From interviews with industry executives, it has become clear that insurers already distinguish between large companies and small and medium-sized enterprises (SMEs), each with different needs and degrees of exposure to cyber risk (Figure 1).

Parts of the market are populated by large firms, such as financial institutions, with their own big IT departments and dedicated resources to managing risk. Large firms also usually have cyber insurance policies in place, and they work with external consultants to reduce exposure.

The SME landscape is quite different. While there are notable exceptions, SMEs as a group lack the expertise and resources to deal with cyber risk effectively. They are usually unaware of vulnerabilities and risk exposures, they do not have dedicated teams to deal with cyber risk, and when they do, the teams are neither large nor diverse enough to provide adequate protection. As a result, SMEs tend to outsource much of their IT and cybersecurity functions. While this market has an attractive potential for cyber insurance, underwriters find it difficult to demonstrate the value proposition of insurance to SMEs. The time required to sell insurance to SMEs can be substantial. Premiums are not big enough to cover risk engineering services, and returns can be compressed.

GROWING THE MARKET

What can be done to attract customers? First, insurers must clearly define which insurance policies address cyber risk. Current practice is to either include cyber cover as a part of existing policies or in stand-alone insurance products. It is often difficult to understand which policies cover which events, and that more clarity is needed. Second, the industry should offer more standardisation and simplification of cyber insurance language, and underwriters and brokers should be better educated to address customer needs more effectively.

Figure 2: Reasons to offer value-added services

# of respondents (10 respondents, multiple answers)

Source: Interviews

Once these elements are in place, insurers should endeavour a transformation of their business model to include more services along the value chain. In the past, insurers were present only after a breach had occurred. Underwriters helped with claims and coverage, but did not actively engage with customers on how to improve cyber risk practices. In the future, insurers are likely to partner increasingly with customers to reduce cyber exposure and the potential losses associated with it. This leads to a two-stage business model for the reasons summarised in Figure 2:

- **Pre-breach:** Insurers work to design appropriate cyber insurance policies for their customers. They work with them to better understand risks and prevent breaches based on appropriate risk management. Insurers offer also consulting services to train and assist organisations in best practices for responding to and limiting damages from a cyber attack or incident.

- **Post-breach:** Insurers provide services that evaluate the impact of an attack, help implement response and recovery plans, provide public relations and communications support, and identify appropriate mitigating actions.

The addition of new services along the cyber risk value chain increases the attractiveness of cyber insurance for customers and potentially improves the profitability of insurers. Offering additional services also increases customer retention.

As demand increases, new insurers are likely to enter the cyber market, eventually lowering prices due to competition. This situation could have a positive impact on the way customers perceive value, which in turn could translate into more demand for cyber insurance.

The reality is, of course, more complex. For example, as the price of insurance drops, there is a risk of (i) lowering the quality of the service offered and (ii) reducing the breadth of coverage of current policies. If the cyber insurance offer is downgraded, the perceived value of the product could decrease and demand for cyber insurance could decline.

TOWARDS CLOSING THE KNOWLEDGE GAP

The purchase of cyber insurance is just one of the steps toward reducing cyber risk. Insurers not only need to train and educate their customers in cyber risk, they must also involve key decision makers on the purchasing side. Cyber security needs to be championed from the top down, starting at the CEO level and extending to all employees. Special attention should be given to the roles and involvement of the Chief Risk Officers (CROs) and the Chief Information Security Officers (CISOs). There must be clear signals throughout the organisations that cyber security is a top priority.

The short history of cyber insurance, incomplete and untested risk models and the likelihood of system-wide attacks have so far dampened the dynamics of an already vigorous market. The industry must develop an even better understanding of future market dynamics. Research can help close the knowledge gaps in a number of areas, including:

- *Identifying solutions to the greatest challenges* – Insurability, accumulation risk, capacity constraints, modelling capabilities, etc.

- *Understanding market dynamics* – Better tracking and prediction of cyber insurance market movement, entry and exit of players, market pricing, cyber risk metrics, and impact of cyber events.

- *Understanding cyber in terms of other insurance* – What can be gained by looking at other insurance markets and products (e.g. extreme natural catastrophe risk, terrorism and war)?

- *Creating an effective value chain* – Finding the right mix of services, in-house vs partnerships, charging for services, requirement vs voluntary, etc.

- *Understanding the political, and micro- and macroeconomic impacts of cyber risk* – Many of the aspects of cyber risk are playing out in the international community in terms of policies, politics, regulations, and trade policies. How these will impact insurers today and in the future is an important aspect of the insurance marketplace.

Insurers are in a unique position to help their customers improve cyber awareness and better understand and deal with cyber risks. A robust offering provides greater protection to customers and also allows for the collection of valuable data by insurers regarding cyber risks, cyber attacks, successful mitigation strategies, and the financial impact of cyber attacks.

While risks and opportunities of the nascent cyber market have been identified, the policies developed so far by global standard setters such as the Financial Stability Board and the International Association of Insurance Supervisors have not kept pace with recent market dynamics. There is more work to be done. The industry should see this as an opportunity to reach out in a cooperative spirit, helping policymakers design regulation that effectively supports the evolution towards a mature cyber insurance market.