Microsoft

EastWest INSTITUTE

MARSH & McLENNAN COMPANIES

The Impacts of a Growing Cyber Insurance Market

Working Roundtable Report

Event Report

The Impact of a Growing Cyber Insurance Market

New York, February 10, 2017

Introduction

As advancements in technology enhance productivity, develop new businesses and enhance economic growth, malicious actors continue to advance as well, seeking to exploit technology for any number of criminal motives or nation-state directed attacks. In response to these threats, enterprises are improving their security, modernizing their risk management practices, and at times working within their respective sectors and with the government to share information.

Increasingly, enterprises are also incorporating the traditional practice of risk transfer into their management practices for technology risks. While this phenomena is still in its early stages, the insurance industry has been underwriting technology risks for more than a generation.

Complicating the insurance industry's ability to underwrite cyber risk is the presence of nation-states seeking to exploit enterprises. To date, cyber attacks have generally been seen as low-cost, high-yield endeavors for the average malicious actor, however, nation-state attacks against the private sector have the potential to distort cybersecurity costs across multiple markets. This dynamic threatens to drive the cost curve in ways criminals cannot, with devastating effects for enterprises.

Technology companies, the insurance industry and their customers are driving better cyber risk management across the ecosystem. Governments also play an important role, but that role is most effective when focused on defending the cyber ecosystem, not exploiting it. As technology platforms continue to drive change in areas like cloud computing, the Internet of Things (IoT), and even blockchain technology, it is even more important that governments commit to supporting the improvement of cyber risk management.

Executive Summary

The working roundtable on "The Impacts of a Growing Cyber Insurance Market," co-hosted by the EastWest Institute (EWI), Microsoft and Marsh & McLennan in October 2016 brought together industry and government experts to examine the current and potential roles of various constituents in increasing cyber resiliency. Questions examined included:

- What role can or should government play in encouraging cyber insurance as a means to improve cybersecurity?
- What role can technology companies play toward meeting government and customer expectations in reducing cyber risk?

- What are the greatest challenges to underwriting cyber risk?
- How do insurance carriers view the role of government policy for information sharing, education and regulation?

The working roundtable was conducted through two interdisciplinary panel sessions:

1. The "Role of Insurance in Cyber Risk Management and Resilience" panel discussed a number of key points associated with establishing effective cyber insurance policies. Some of these included: challenges in underwriting, absence of standards across the industry, government participation in malicious cyber activity and the status of small to medium sized enterprises (SMEs) in the cyber insurance world.

2. The "Underwriting Cyber Risk and the Insurance Industry's Future Trajectory" panel focused on how to improve cyber insurance in preparation for the evolving risk environment and market growth. Topics discussed included the need for increased technical awareness among stakeholders, the importance of continued reassessment and revision of models and practices and the expansion of risk areas covered by cyber insurance.

Experts on the two panels posed challenging questions and offered their insights on the cyber insurance market, resulting in the following key observations:

1. **Mitigating systemic cyber risk**: Nation-states could contribute to, or even trigger, systemic cyber risk regionally or globally. While systemic cyber risk is still a nascent term, it was understood that the potential for this type of event increases when nation-states engage in cyber attacks. This happens because nation-states can apply considerable resources to developing and deploying sophisticated malware and tools. The resulting effect is a contribution to systemic risk across the cyber ecosystem, rather than a reduction. The insurance industry has long examined and analyzed risks that can cause damage across large geographic areas or an entire sector. Historically, reinsurers have employed advanced modeling and complex analyses to aggregate complex risks that may, if left unmitigated, expose large groups of companies to serious risks . However, for cyber insurance, this process is still ongoing and maturing. The challenge lies in building an aggregation model that the insurance industry will find suitable. With this model, reinsurers will be able to increase capacity to meet, and keep pace with, technology adoption.

2. **The impacts of increasingly sophisticated threat actors:** For criminals and nation-states, cyber attacks are a low-risk, high-yield endeavor. This combination creates an unfortunate abundance of ongoing attacks, which in part drives greater demand for cyber insurance. The success of these attacks is largely a function of more sophisticated threats, and in some instances, poor cyber risk management. However, this problem of more sophisticated threats – some coming from or acting on behalf of nation-states – cannot be solved just by better security and cyber risk management. Government and law enforcement need to impose harsher penalties against malicious cyber actors and begin to reverse the cost curve. Increased risks for malicious actors reduce the frequency of these attacks and help create a healthier cyber risk management ecosystem.

3. **What will insurance cover:** Cyber incidents consist of four shifting "buckets." These are: out of pocket costs, lawsuits (including regulatory investigations, fines and penalties), business interruption and reputational damage. To date, the insurance industry has focused on indemnifying the insured for out of pocket costs and lawsuits resulting from data privacy exposure. In today's market, there is growing uptake in cyber insurance from companies concerned with loss of revenue and extra expenses associated with network interruptions. There is a practical difficulty to quantifying reputational damage, as coverage is often limited to reimbursing the cost of public relations. As enterprises increase their technology footprint, business interruption and reputational damage coverage should increase in relation to their significance. Expanding business interruption coverage requires a more thorough understanding of the technology used by the insured and the risk management policies that the technology provider has implemented.

4. **The need for better data:** Panelists recognized that a lack of historical loss experience data and actuarial data handicaps the insurance industry in accurately estimating the risk, which in turn, slows the maturation of the market. The insurance industry is built on data, which leads to strong modeling to enable more accurate forecasting for the likelihood and severity of events. Another challenge in the effort for better cyber risk models is that almost all of the actuarial data comes from data breaches. Looking toward the future, and IoT, data breaches will be only one of the many types of cyber incidents that will arise.

5. **Moving the needle:** The act of an insured applying for insurance forces an assessment of the applicant's cyber practices. Underwriting criteria are non-standard across insurance carriers and are less rigorous than for more mature policies, such as workers compensation or property. To varying degrees, the underwriting process scrutinizes a company's technical defenses, incident response plan, procedures for patching software, policies for limiting access to data and systems, monitoring of the vendor network and others. Collectively, these actions move the needle in the direction of improving the enterprise's cybersecurity posture. Going forward, the insurance industry is investing in automated technology tools that may provide more consistent and objective quantitative risk assessments of the insured.

6. **Building a common language across the cyber ecosystem:** Within enterprises, information security professionals and corporate risk managers need to develop a common understanding of not only their enterprises' risk, but also one another's role, terminology and responsibilities. Both sides are often unpracticed at actively proposing business technology agendas or communicating risk concerns. In short, many security professionals and risk managers have differing views on the nature of cyber risk, and how to address cybersecurity and cyber risk management. While both constituencies may understand the enterprise's compliance obligations, this is not the same as understanding the enterprise's risk.

7. **Bringing in more SMEs:** In addition to limiting financial damages, cyber insurance provides access to security and remediation vendor resources that the insured might not have on staff. Steadily, SMEs are beginning to see the value of cyber insurance, as seen in higher uptakes year over year. Yet relative to larger enterprises, SMEs still represent a small

percentage of the overall cyber insurance market. There are market and security benefits as more SMEs enter the cyber insurance market. Not only does coverage expand across diverse businesses, but a greater body of loss information may provide greater data and insight to support risk modeling.

8. **Internationalizing best practices and standards**: The benefits attached to cyber insurance can be explained in the context of the National Institute for Standards and Technology's (NIST) Cybersecurity Framework for Improving Critical Infrastructure. Buyers can map the components of a strong cyber risk management program to the five cybersecurity domains - assessment, prevention, detection, response and recovery - proposed in the Framework. The NIST Cybersecurity Framework provides a voluntary blueprint that enterprises and insurers of all sizes can use to evaluate, maintain and improve the resiliency of computer systems and reduce cyber risk. With respect to international efforts, the G7 recently published the *G7 Fundamental Elements of Cybersecurity for the Financial Sector.* The document contains a series of non-binding, high-level fundamentals to encourage regulators and enterprises to approach cybersecurity through a risk management perspective.

9. **Building a better way of identifying risk:** Many insurance carriers continue to underwrite cyber policies without fully understanding the extent of the cyber risk exposure of the insured. This is complicated by the fact that the insured may not always know the full extent of their own cyber risk. Remediating this lack of knowledge is difficult. However, underwriters can, and many are beginning to, apply more scientific and quantitative tools rather than relying on questionnaires that oversimplify the challenge of identifying and assessing cyber risk. Going forward, it may be more practical for the industry to reach a point where insurers can measure network activity against a set of criteria in real-time. In the meantime, insurance brokers and risk advisors must continue to assess threats and vulnerabilities and advise where additional mitigation investments and insurance are needed.

10. **Cross sector collaboration:** Information sharing is a vital part of cybersecurity risk management because it helps enterprises and governments improve and reduce cyber risks. Furthermore, organizations such as the Financial Services Information Sharing and Analysis Center (FS-ISAC) provide a platform for the global financial services sector to exchange information about cyber threats. This is one model for consideration across industry sectors.

Systemic risk, as framed several ways throughout the workshop, is one issue that poses greater challenges for the ICT and insurance sectors and government. Little work exists to understand systemic cyber risk to enterprises and how it can be measured and managed. EWI and its partners are therefore devoting more attention to this issue through the formation of a breakthrough group that will examine systemic risk beyond financial systems, its impact on general business continuity, its potential for cascading failures and the implications for the insurance industry. The group will develop and disseminate approaches to mitigating risk and improving loss prevention across key industries worldwide.

ANNEX: Summary of Events "Working Roundtable: The Impacts of a Growing Cyber Insurance Market"

New York, October 21, 2016

Welcome Remarks
Paul Nicholas, Senior Director, Trustworthy Computing, Microsoft
Bruce W. McConnell, Global Vice President, EastWest Institute
Thomas Fuhrman, Managing Director, Cyber Security Consulting & Advisory Services, Marsh Risk Consulting

The speakers emphasized the timeliness of the discussion and the need to move beyond the technical community when discussing cybersecurity. In the past, cybersecurity was largely defined by technical aspects. Today, other factors such as cyber insurance, regulations and law (both statute and case law) will be shaping the cyber environment just as much as technology. Cyber risks will eventually be normalized by regulations and law that will allow it to be managed like any other type of risk. Nonetheless, cyber insurance and the role of business and government in the cyber insurance market require more systematic examination. A deeper understanding of cyber risk is also key to developing the cyber insurance market. Government has worked with industry to make standards before. Is there a similar role that government can take in cyber and in the field of cyber insurance? Is this something that the EastWest Institute can help facilitate?

Panel I: Role of Insurance in Cyber Risk Management and Resilience
Moderator: Bruce W. McConnell, Global Vice President, EastWest Institute

Panelists identified two major barriers when it comes to successful cyber risk management: lack of actuary data and lack of underwriting standards. For the former, the largest data available comes from data breaches, but overall even that is imperfect. On the latter, no cross industry standards have been developed and although the voluntary National Institute of Standards and Technology (NIST) Cybersecurity Framework is a good starting point, progress has been embryonic.

The multiplicity of standards poses challenges. There are few standards for how cyber insurance products have to work. This also feeds into a general vocabulary problem across industries. For example, as panelists underlined, IT security professionals view risk very differently than risk managers and the insurance industry. Whereas they may share an understanding of compliance obligations, views differ on standards. For IT security professionals, the standards are of control, not action or policies.

Governments have in fact contributed to making risk management more difficult given their investment in offensive cyber weapons. This is highly disruptive of the private sector's sense of risk management control. These developments also take investment away from defensive tools, which are critical. It also makes it more complicated to assess the emergency response skills of a company when exposed to threats unknown.

Panelists noted that the government has been trying to incentivize the private sector with a new framework to prop up security (e.g., Executive Order 13636). However, some viewed insurance to be more of a tool than an incentive, while others saw insurance as a driver. Furthermore, most policies are written without realizing the full exposure of an enterprise's cyber risk. Cyber risk posture is so dynamic that it changes almost every day. The public sector has generally been supportive of the cyber insurance market because the process of purchasing insurance provides a new set of eyes on a company's cybersecurity. Indeed, the process of applying for cyber insurance and ensuring it meets the insurer's underwriting standards reduces an enterprise's cyber risk. It also gives companies access to resources they may not have without the insurance protection. This is particularly true for small and medium enterprises (SMEs). Views, however, diverged whether lax cybersecurity by SMEs could lead to systemic risk.

Panel II: Underwriting Cyber Risk and the Insurance Industry's Future Trajectory
Moderator: Matthew McCabe, Senior Vice President, Marsh & McLennan

Panelists explained that although EO 13636 and NIST have helped facilitate the spread of cyber insurance (upward of 20 percent annual growth rate), macroeconomic solutions remain the key to growing the insurance market. A fundamental question remains how insurance companies can develop effective aggregation models for the fastest growing insurance market in the United States, given the lack of actuarial data and rapidly changing cyber threats.

There was agreement that insurers need to improve their understanding of risk, and that underwriting needs to be more scientific, rather than relying on simple questionnaires. There is a push (particularly when dealing with smaller companies) for third party analytics.

One big issue is whether insurers will start using all-in-one cyber policies or use multiple policies to cover individual components associated with cyber. For example, data breach, property damage and bodily damage are already covered under casualty insurance; however, this insurance is not designed to address cyber incidents (questions also arose what would happen if one cloud provider were to go down). Standards, as participants pointed out, also quickly turn into compliance checklists and this is not the answer, because incidents can still happen. There was also broad consensus that governments should not be dictating standards, but rather act as educators. Insurance companies and government have similar postures in wanting consistent and repeatable methodologies. Standardization of policies will come in time.

The issue of sharing information was also raised. Company sharing agreements help firms share risk information. Participants disagreed over voluntary versus mandatory sharing. On the one hand, mandating reporting could mean that companies will give the least amount of information possible, whereas others argued that it could offer some protection through the government.

Closing Remarks
Paul Nicholas, Senior Director, Trustworthy Computing, Microsoft
Bruce W. McConnell, Global Vice President, EastWest Institute