INSURANCENEXUS

Quantifying Cyber: How Insurance Carriers are Meeting the Challenge of Covering an Ever-Changing Risk Landscape

INSURANCENEXUS

Quantifying Cyber: How Insurance Carriers are Meeting the Challenge of Covering an Ever-Changing Risk Landscape

Author

Morag Cuddeford Jones

Editor

Kamilla Rakhmat
Project Director
Insurance Nexus
T: +44(0)20 7375 7523
E: kamilla.rakhmat@insurancenexus.com

Quantifying Cyber: How Insurance Carriers are Meeting the Challenge of Covering an Ever-Changing Risk Landscape

Quantifying Cyber: How Insurance Carriers are Meeting the Challenge of Covering an Ever-Changing Risk Landscape

Cyber security is being driven into the spotlight by a number of high-profile data breaches and denial of service (DoS) attacks. These attacks are affecting global companies and small businesses alike and involve millions of data points and dollars. Yet, within the insurance sector, cyber security remains a largely untapped opportunity.

It might seem counterintuitive to align the word 'opportunity' with a risk that has the potential to expose carriers to huge losses. The WannaCry ransomware attack has been estimated to have caused global financial losses of up to $4bn[1], having infected 300,000 machines worldwide.

These losses can be large, but they are on par with other insured risks such as catastrophic weather events (Hurricane Michael, $4.5bn to $8bn estimated loss)[2] covered by most standard carriers in the US. In terms of premium potential, experts are projecting cyber insurance premiums to rise to more than $8bn by 2020, a substantial increase from $1.87bn in 2017. Premium growth will continue to rise over the next decade as the concept of cyber insurance becomes more entrenched across the sector. For comparison, Deloitte found that US P&C premium revenues rose only 4.6% in 2017 and this was the most such premiums had risen year on year in a decade. It makes sense that carriers looking for growth should be looking to cyber.

Adapting to customers' cyber security needs is a clear opportunity for carriers to achieve rapid growth in a sector that is otherwise at capacity. However, carriers face many challenges before they can begin to maximize the potential in covering cyber risk. *Insurance Nexus* spoke to a panel of senior insurance executives and cyber risk experts to discover what the landscape looks like for carriers moving into cyber coverage.

In this paper, you will learn:

- Why underwriting for cyber risk poses challenges
- The contribution made by catastrophe modeling
- How to anticipate exposure to risk
- The threat of quantum computing
- The importance of customer education

The Challenge of Underwriting Cyber Risk

Experts estimate that cyber risk has been an insurable risk since 2009. However, in remaining relatively niche over the past decade, it lacks the standardization that makes other risks easy to define and insure.

Most still understand cyber security to involve a data breach but experts would suggest it involves much more than that. A lot of issues concern business interruption or extortion events that are unrelated to data. There is an added layer of

1 https://www.reinsurancene.ws/total-wannacry-losses-pegged-4-billion/

2 https://www2.deloitte.com/us/en/pages/financial-services/articles/insurance-industry-outlook.html

Quantifying Cyber: How Insurance Carriers are Meeting the Challenge of Covering an Ever-Changing Risk Landscape

confusion when it comes to connected devices – from wearables to cars to industrial machinery. When these items go wrong as a result of an attack or software/hardware failure, it can have wide-ranging implications including user health, building integrity and so on. It also makes for a large diversity in the policy language around cyber, which can make it confusing for the customer.

One expert warns: "Coverage clarity across insurance lines is really complex and it's difficult to understand how policies interact with one another. It's a confusing area for everybody – the insured, the insurer and the reinsurers."

Since carriers are aware that cyber risk is something that they increasingly have to cover explicitly (as opposed to general coverage under another policy), many are pressing ahead with underwriting stand-alone cyber policies. Some are concerned that there is not enough due diligence; "we're going down a path and I don't know how thoughtful we've been about it. Coverage has been significantly expanded but I'm not sure we have the controls in place to understand how this could impact our profitability," said a reinsurance expert.

The issue is that the coverage is too broad, so a balance clearly has to be struck between being too hesitant allowing competitors to steal the march, or overconfidence which exposes the carrier to risk. Without tight policy wording, every claims scenario and scope becomes possible. This is the core reason why many carriers are currently focusing their efforts on modelling; but many question: when it comes to cyber, what does future risk really look like?

Cyber Borrows from Catastrophe Modeling

Experts agree that cyber risk in the insurance sector is unprecedented. There have been one or two prominent incidents to learn from, such as the aforementioned WannaCry, but these are few and far between. The sector has a habit of evolving rapidly. New threats don't closely resemble what has gone before, making modelling for the future a challenge.

"Climate change and cyber risk are probably the two biggest exposures faced; not only by the insurance industry but by the world as a whole. They're both emerging phenomena that are really difficult to model and changing constantly. If you don't know what you're doing, it can certainly cause a lot of problems."

Another senior reinsurance professional adds: "The threat is continually changing. It's not necessarily true that past experience predicts future experience." There is plenty of data in the industry, even on cyber risk, but it is all historical. While it can aid in carriers understanding how a past event happened, due to conditions changing so rapidly, this learning is rarely applicable to future events. Another downfall of using historical modelling to model cyber insurance is that it cannot form a predictable pattern that carriers can use to anticipate risk.

There is a real need to take a different approach to risk management and mitigation in cyber but, while difficult, some would suggest it is not impossible: "The challenge we face is that technology changes extremely quickly. New vulnerabilities arise that are impossible to foresee ahead of time, no matter how expert you are. That doesn't mean it's impossible, you just have to bring a certain discipline and pragmatism to understanding that potential exposure."

Quantifying Cyber: How Insurance Carriers are Meeting the Challenge of Covering an Ever-Changing Risk Landscape

Experts are drawing parallels with tactics used for anticipating and mitigating damage from hurricane events and other catastrophic phenomena. These share cyber risk's speed and spread, along with similar large potential losses. "We've invested a lot with cat modelling capabilities to make sure we fully understand our exposure - where the new threats are relative to technology, and how that actor is trying to capitalize on vulnerabilities," says one executive. The implication is that carriers acknowledge they cannot stop new attacks from happening, but they can put in place measures to mitigate exposure and provide relevant coverage.

Anticipating Exposure to Cyber Risk

But how one business is affected is not the end of the story in risk modelling. Carriers have a wider consideration when it comes to cyber risk, insofar as risk does not stop at the door of a single business. Risk spreads like a virus (indeed, some risks may be viruses), weakening everyone it comes into contact with.

A single business may be first to experience an attack, data breach or some other way in which their operation is compromised. However, this can have a knock-on effect on their customers and other partners. Carriers are currently struggling with the 'how': how to define the limits of their coverage or indeed how to work with the insurers of other affected entities. This can be seen from a global insurance executive revealing the current struggle of insurance carriers: "How do you manage accumulation, how do you understand where some of those interconnected activities are and how do you best address it?"

For now, experts suggest that watchfulness may be the best approach, fully plotting out just how far-reaching the carrier's obligations might be in the event of a claim: "You need to stay on top of how coverage is expanding, how the pricing is working to make sure it's adequate. Figure out what your aggregation is and the frequency of losses. At this point, these are subjective."

Planning for the Threat of a Quantum Event

Carriers have seen the impact catastrophic events such as hurricane and wildfire have on payouts, put at an estimated $52bn[3] in 2018. Clearly, carriers cannot prevent these natural disasters from happening, but they can advise their clients on ways to mitigate the impact. The same applies to the cyber risk of a so-called Quantum event.

Future losses may be subjective, due to the ever-evolving nature of cyber risk, but a Quantum computer threat would be, as one industry expert puts forward, something of a 'doomsday scenario'. 'Quantum' refers to an attack so sophisticated that it is, as the expert suggests, it is "likely to smash through all existing cryptography".

Needing years of planning and migration, preparations for a quantum computer threat are only really being made in a handful of banks and big telecoms organisations. "Quantum computer threat is like cyber hurricane events where there are

3 https://www.iii.org/fact-statistic/facts-statistics-us-catastrophes

massive claims against insurers. It hits everybody who is unprepared which could be many, if not most, businesses. The solution exists in the form of quantum-based cryptography, which is being standardized now by the main government agencies around the world," states the security expert on our panel.

While a solution is being worked on, this may not be fast enough or in a form most companies can adopt easily. So, he adds: "If I were in the insurance industry I would be educating my customers about this to try and avoid massive losses or, I would be looking at ways to compel customers to sufficiently plan for these events."

The Carrier's Role as Educator to Prevent Risk

The notion of 'compelling' insurance customers may seem harsh, but there is a sense that customers do need to take some control over their exposure to cyber risk. However, experts do recognize that if carriers find it difficult to understand and quantify potential exposure, it will be twice as difficult for customers to do so.

One cyber security insider tells us: "What customers do internally is going to have a big impact on the likelihood that they're going to make a claim. It's very difficult to get a true picture of an organisation's security profile because sometimes they might actively overstate their capabilities to lower their premium. They make these statements in good faith, they just don't know enough about their own infrastructure."

He suggests that this may be down to the evolution of technology outpacing the IT education framework. "A lot of students would prefer to do what I would call less critical functions in the IT world like apps, and they're not going into security engineering. The skills shortage is worsening while the hackers are getting smarter."

When a niche skill is required, most companies will seek expert advice from third parties, such as a consultancy. Although, even then, some insurance carriers and brokers struggle to close the education gap. "Quite a few of our clients have tried to work directly with cyber security firms and it was like talking two different languages,"[4] explains one security-focused reinsurance broker.

Education will be at the heart of driving a more mature approach to cyber risk, both in terms of the products carriers offer and in the ways their customers can make the best decisions in relation to their exposure.

An industry insider explains: "There's a lot of opportunity for innovation and for the introduction of services that complement the insurance policy. With cyber, given that it evolves so rapidly, there's a real chance to educate customers that there's a lot we can do to help companies have a better relationship with cyber risk. To make our customers a better risk overall."

One key part of that education is to help customers understand the need for comprehensive cyber coverage in the first place. Many of the experts spoken to by *Insurance Nexus* expressed concern that clients didn't appreciate the scope of cyber risk until it happened to them, or someone close to them.

Quantifying Cyber: How Insurance Carriers are Meeting the Challenge of Covering an Ever-Changing Risk Landscape

Carriers need to work closely with customers to help them understand how to work on cyber risk, in the same way a P&C carrier may discuss home security or energy efficiency. This is the way to grow the market: "Opportunity number one would be a new revenue stream but it is also an opportunity to display the industry's value in terms of being a key part of the mitigation process" says a reinsurance expert.

The future potential of cyber risk as a business line for carriers is a moveable feast. Unlike much that has gone before it, cyber is proving harder and harder to quantify and predict. This is forcing carriers to focus on the impacts of cyber risk as a yardstick for underwriting, pricing and policy scope in a way that they have not had to before. It is forcing a new way of thinking about the value of insurance overall, the extent to which technology and its impacts affect every aspect of personal and commercial life. As one expert concludes: "We don't know where the industry will be in five or even two years' time but that's not necessarily a bad thing. The industry will continue to evolve and should continue to evolve by addressing the needs of its customers."