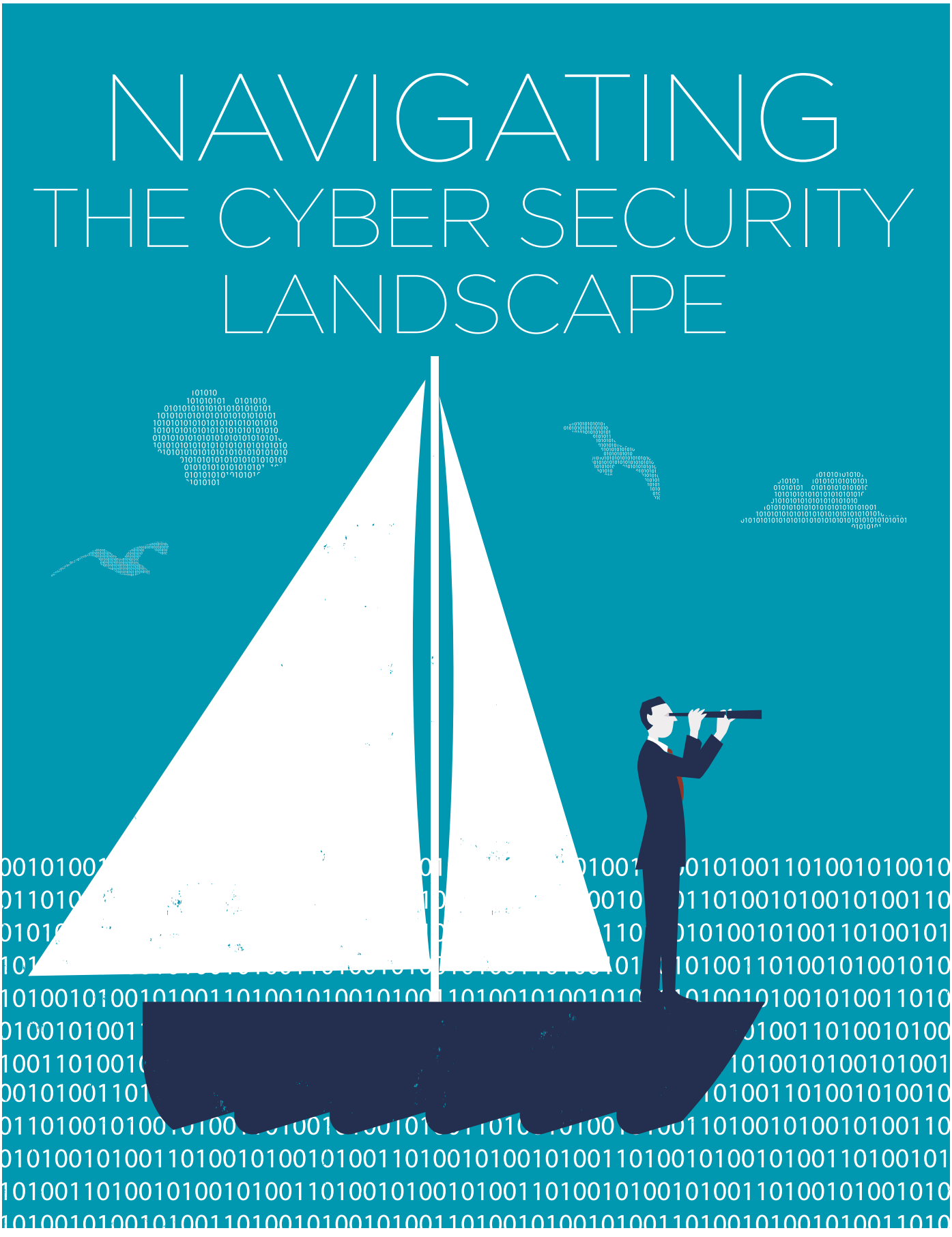
impact

ACTIONABLE INSIGHT FOR BUSINESS LEADERS / **CYBER RISK** / FEBRUARY 2016

NAVIGATING THE CYBER SECURITY LANDSCAPE



Cyber may yet prove to be a major opportunity for the industry, but insurers must first find ways to overcome the huge systemic and aggregate exposures inherent in this emerging risk.

By Stuart Collins

Today, cyber risk is one of the fastest growing lines of insurance. High-profile data breaches and tougher privacy regulation are making organisations take their cyber exposures more seriously, which in turn has been driving demand for cyber insurance.

In its 2015 cyber report, global insurer Allianz predicted that the worldwide cyber insurance market could reach $20bn by 2025, from around $2.5bn today.

Further growth is expected as other countries enact more consumer-friendly data breach rules – the EU is due to implement stringent data protection laws early in 2018. Longer term, growth in the cyber insurance market is also expected with increased reliance on technology, in particular as physical industrial processes become digitalised.

In its report, Allianz predicted increasing demand for cyber insurance from a broader range of customers, not just those holding personal data. The insurer sees additional demand in the future from industry and manufacturing as both products and business models become increasingly dependent on technology.

Digital risks of the future

The insurance and reinsurance industry has recently started to consider the implications of new technologies on the risks it insures and its own business model.

Emerging technologies – such as the Internet of Things, greater automation, robotics and even artificial intelligence – will increase cyber security risks, and create new liabilities and dependencies. For example, automated cars should drastically reduce accidents, with the focus of liability and insurance potentially shifting from drivers to manufacturers. Automated production lines will see fewer employee risks but potentially increased supply chain risk.

According to Nick Beecroft, emerging risks and research manager at Lloyd's of London: "The coming digital revolution will increase the breadth of impact from cyber-attacks. Entire value chains will be connected and autonomous machines will open up a range of new exposures and interconnected risks, including data breach, physical damage, liability, business interruption and reputation.

"Cyber will reach into every corner of the modern economy, so we expect solutions will be tailored to a diverse range of solutions to meet the needs of clients. The starting point for cyber insurance products has been data breaches, but as industry becomes more connected and digital, we expect demand for a broader range of coverages," he adds.

The challenge ahead

While there is a clear need for cyber insurance, insurers are rightly cautious. Their ability to meet demand is currently restricted by their relevant expertise and understanding of the risk, and their ability to manage cyber exposures. A number of factors make cyber insurance difficult to underwrite and, as it becomes a more significant source of business, a potentially serious threat to solvency.

At an AM Best briefing in London late last year, Stephen Catlin, executive deputy chairman of XL Group, said that systemic risks and accumulations of exposures inherent in cyber were preventing insurers offering meaningful limits of cover to corporates.

While large companies will buy $2bn of property cover, insurers are only prepared to offer cyber insurance up to $500m for the largest companies, and this will challenge the relevance of insurers in the future, Catlin says. He called on the government to provide the industry with a backstop, much as it does with terrorism risk, to enable it to offer higher limits.

> *The coming digital revolution will increase the breadth of impact from cyber-attacks. Entire value chains will be connected and autonomous machines will open up a range of new exposures and interconnected risks, including data breach, physical damage, liability, business interruption and reputation.*
>
> Nick Beecroft, manager, Lloyd's of London

Systemic and accumulated risks are key risk characteristics that make cyber a particular challenge for underwriters. According to Beecroft: "Cyber is a truly globally systemic exposure that could trigger losses across many forms of economic exposures and classes of business. It is an intangible risk, but also one with a significant human element, where losses can be caused by negligence and accidents. The challenge moving forward is to manage exposures and understand the systemic risks and correlations inherent in cyber."

Cyber cat loss scenario

In July 2015, Lloyd's and the University of Cambridge's Centre for Risk Studies published a report, Business Blackout, which illustrated the problem faced by the industry.

The study shows how a cyber-attack against the US North East power grid – an extreme, yet possible, cyber loss scenario – could result in a multitude of seemingly uncorrelated claims. According to Lloyd's, the scenario is relevant to stress and scenario testing required under the Solvency II framework, representing an event with a return period of 1:200 years against which insurers must be resilient.

Such a scenario, says the study, could cost the US economy $243bn, rising to more than $1tn in the most extreme version of the scenario. The cost to insurers would be $21.4bn, rising to $71.1bn.

According to Beecroft: "This is a serious loss event, and comparable with a major natural catastrophe, to which the industry has shown resilience in the past. The difference with cyber, however, is the uncertainty attached to the business interruption and liability losses."

The high aggregation risk associated with cyber points to the potential for extremely large losses in the future. At the same time, difficulties in pricing cyber risk and limited opportunities to diversify the risk could exasperate the problem.

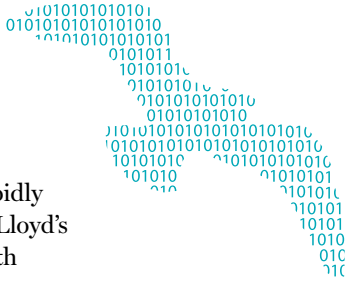
According to Graham Coutts, associate director at Fitch Ratings: "Cyber risks are very difficult to price using traditional actuarial methods, the scale and consequently the associated financial loss could be significantly higher than more traditional insurance risks. The interconnectedness of today's technology makes it possible to spread a computer virus around the globe relatively easily. In addition, consequences such as reputational damage can be very difficult, if not impossible, to measure and insure.

"The cross-border nature of cyber-crime, particularly given the increased popularity of cloud services, undermines the potential for geographic diversification through reinsurance.

"For these reasons, cyber risk has the potential to cause significant losses which could lead to a reduction in risk-adjusted capitalisation. In an extreme case this could adversely affect ratings, depending on the magnitude of the losses," he says.

The way forward

With the transition to a digital world, corporates are likely to demand high limits and broader cover, but, given the risks outlined above, insurers will want to delineate cyber risk, and potentially carve out certain risks – for example, using pools to deal with systemic risks.



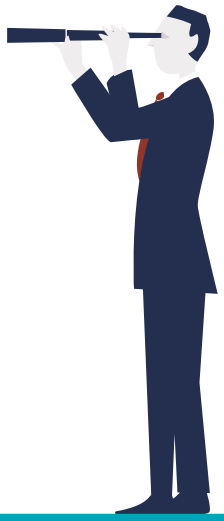
According to Beecroft: "At present, cyber is a rapidly growing but relatively small class of business, but Lloyd's would like to see the pace of cyber insurance growth linked to insurers' ability to reduce uncertainty."

Regulators, which are growing increasingly interested in cyber risk, are also likely to share this view.

Kathryn Morgan, director of regulatory operations, Gibraltar Financial Services Commission, gives some insight: "If an insurer writes more cyber business I would expect them to start in a relatively small way, testing wordings, policies and getting to understand the language of cyber risk. Underwriters will be expected to be entrepreneurial, but they need to learn and test policies, rather than put their life savings on the line."

Reducing uncertainty

As the cyber insurance market expands, insurers will need to focus on reducing the uncertainties of cyber risk, such as those that currently exist around policy wordings.



CYBER LIABILITY

Cyber litigation is likely to become a significant issue for companies and their insurers as people increasingly demand reparation for loss of privacy, data and potentially physical damage, resulting from a cyber breach. At the same time, cyber insurance wordings, as well as any potential for cyber-related cover under property and casualty policies, have yet to be fully tested in courts.

According to James R. Woods, Co-Leader Insurance Industry Group, at US law firm Mayer Brown LLP, cyber coverage litigation in the US has mostly focused on testing wordings under commercial general liability policies. Such case law is still relatively limited. However, on balance, cases suggest that US commercial general liability insurance does not extend to cyber.

"Cyber lawsuits are occurring just now but this is an area where we still do not have a significant amount of case law," says Woods.

However, there have been cases that have addressed consumers' "standing" to bring claims, for example, when a breach has affected their personal data. The trend appears to favour consumers, with many lawsuits being allowed, even when consumers have not suffered a loss, he adds.

For example, when US health insurer Anthem suffered a breach in January 2015, it faced over 90 lawsuits and almost $360m in cyber security and breach response costs, despite there being no evidence that anyone had suffered any financial loss as a result of the breach.

"This is an emerging area of the law, and one where there is not enough case activity, but it will be essential for insurers to watch whether courts move in the direction of compensating consumers in the future," says Woods.

There is likely to be many years of litigation and legal battles ahead in determining the scope of traditional property / casualty policies and standalone cyber insurance. As they did with asbestos and pollution cover, policyholders and lawyers are likely to take every opportunity to push the boundaries of general liability insurance cover.

For example, cyber insurance policies are only now beginning to be tested in court, while there is only limited experience of how traditional property and casualty policies would respond to a cyber loss. Insurers have included cyber exclusions in some markets – such as marine and energy – while other lines of business remain largely silent on cyber risks, such as aviation.

According to James R. Woods, co-leader insurance industry group at US law firm Mayer Brown LLP: "Insurers need to be careful on policy language and pay close attention to legal developments regarding cyber. They need to clearly exclude parts of the risk that they do not wish to underwrite."

Writing cyber exposures under standalone policies or extensions should help reduce coverage uncertainties and the potential for litigation.

Woods explains: "It should be clearer and cleaner to underwrite cyber exposures in separate cover, while drafting cyber cover within commercial general liability policies would create potential issues.

"Achieving certainty of coverage will be challenging, so insurers should look to limit their exposure. Make sure that there are clear limits on liability."

There can also be uncertainties around claims, according to Derek Newton, principal and consulting actuary at Milliman.

"A cyber breach might only be discovered some time after a company's security has been compromised, when actual costs have started to emerge and checks trace the cause back to a breach. But even were it possible to see when breaches actually occurred it might not indicate when a claim event actually happened," he says.

For example, it can be difficult to establish exactly how and when a cyber-attack first took place. On average, hackers spend more than 200 days inside a system before they are discovered, according to cyber-threat assessment company FireEye. Research from the company also revealed that just 31% of organisations discovered the breach themselves last year, while 69% were notified by a third party.

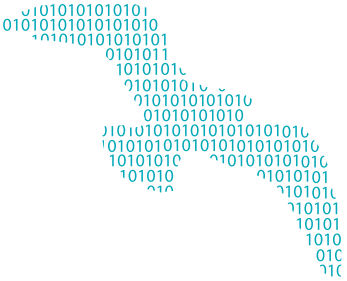
Data sharing

Even after tightening contract wordings, with limited understanding of cyber risk and little historical data to rely on, insurers face major challenges in pricing cyber risk, as well as setting capital and reserving.

According to Graham Coutts at Fitch Ratings: "With modelling for cyber risks still in its infancy, the lack of expertise and inadequate understanding of cyber risk remains a major obstacle for growth. In addition, loss data and profitability related to underwriting cyber risks remain relatively opaque." A key aspect of insurers' ability to provide a solution to cyber risk will be the degree to which they can get a detailed view of the risk and reduce uncertainty around extreme events.

According to Fred Eslami, senior financial analyst at AM Best: "It is a given that insurance needs reliable data and dependable actuarial analysis for accurate pricing and reserving. As it relates to cyber insurance, the quantification of risks and rewards has not yet reached such reliable levels as currently exist for other lines of business that insurers are writing."

> *With modelling for cyber risks still in its infancy, the lack of expertise and inadequate understanding of cyber risk remains a major obstacle for growth. In addition, loss data and profitability related to underwriting cyber risks remain relatively opaque.*
>
> Graham Coutts, associate director, Fitch Ratings



The lack of historical data will require insurers to find alternative sources of information to better understand cyber security risk. Some insurers have begun to seek partnerships with cyber security experts to understand risks and the effectiveness of mitigation. For example, in May 2015 ACE Group announced a partnership with FireEye.

There has been progress on the development of cyber models. In January, catastrophe modelling firms AIR Worldwide and Risk Management Solutions (RMS) published cyber data and exposure standards. The standards were the product of collaboration with Lloyds and are intended to help the cyber insurance market establish common core data requirements and definitions.

According to Beecroft, collaboration is becoming a key theme: "There will need to be a significant degree of collaboration between various parties – government, business, insurers and technology companies – including the sharing of data to give a shared understanding of the risk."

Cyber criminals are known to collaborate, sharing information and pooling resources. In contrast, most businesses are reluctant to share their experiences and information on breaches or cyber security, says Newton. "A loose federation of individual hackers thus becomes more powerful than any individual business, however big, if it acts in isolation," he says.

Both the UK and US governments have publicly recognised the need for better data sharing, and the potential role of insurance in encouraging better risk management. A 2015 report from the UK government and broker Marsh recommended a forum be established to exchange data and improve the information available for underwriting and for determining aggregation risk.

Big data analytics

The speed of technological change means that insurers will need to make decisions much faster and based on less historical information, explains Newton. The challenge for the actuarial profession is to keep analysis sufficiently quick and useful in an instant world, he says.

The UK motor insurance sector offers a glimpse of what may lay ahead, according to Newton.

"The introduction of comparison websites and increased competition led motor insurers to embrace big data, automated underwriting and real-time pricing. In motor, we have seen the first tentative steps towards using big data, using publicly available data sources, such as the electoral register, land registry and court records, to rate motor risks," he says.

But while there is a huge amount of additional data available to insurers, the industry has yet to understand fully which are relevant to risk factors," according to Newton. "The ability to generate, collect and store data has been increasing at a rapid pace, but insurers' ability to process it and to recognise which data is most relevant has lagged," he explains.

Some believe that big data, and emerging intelligent analytics technology and cognitive computing will offer a solution. Swiss Re recently signed a deal with IBM to use its cognitive computing technology, Watson, a cloud-based computer system that can learn and interact with humans. Such technology could be used to evaluate large amounts of data, including big data and unstructured information, like risk assessment reports and insurance submissions. This in turn could be used to support underwriters, especially for complex data reliant risks like cyber or supply chain disruption.

"In the future, insurers will need to take a more holistic approach to data and analytics, using multiple sources of information, pulling them together to create more dynamic pricing models that learn by experience," believes Newton. "Even more than they already are, better data and systems will be a competitive advantage to insurers," he says.

Find out more

Derek Newton
+44 20 7847 1606
derek.newton@milliman.com