Cyber: Drivers of Change

The role of regulators and state actors in the cyber market

September 2016

Table of Contents

Executive Summary

As cyber re/insurance experiences rapid growth, regulators and governments alike have taken action to both understand and effectively manage this emerging risk. Despite concern that such input may stifle a burgeoning market, new laws and regulation in Europe are deemed to have a positive impact on the standalone cyber market and actually accelerate its development.

This report outlines two key legal and regulatory changes – the General Data Protection Regulation Act (GDPR) and the cyber risk scenarios from Lloyd's – that will help:

- limit cyber provisions in all risk policies
- broaden knowledge about cyber beyond the standalone market, and
- help globally expand cyber premium beyond its traditional US domestic market.

Through practical policy wording, sensible risk transfer solutions and comprehensive analytics, re/insurers will continue to grow and expand in this emerging class while mitigating the challenges that come with a rapidly evolving risk.

Key findings

The ramifications of EU legislation will not be limited to European carriers: The (GDPR) will not only cover European companies but any corporation that handles data of European citizens. As a result, most international corporations will have to be aware of the GDPR and conversant in the potential sanctions from falling foul of the legislation.

Legal changes in the European Union (EU) are likely to drive growth in the cyber market internationally: New legislation designed to standardise the legal framework on the notification of data breaches will create the legal structure and, importantly sanctions regime. This will drive the growth of the European cyber market as demand for cover increases in line with the exposure to risk.

Meanwhile, the creation of mandatory cyber scenarios by Lloyd's show regulatory interest in the growth of the cyber market: Each syndicate must model and submit to Lloyd's the losses for eight cyber scenarios to help manage their own and the market's sustainability.

The scenarios impact multiple lines of business: These look at potential aggregation of "silent cyber" exposure that could impact all risk and specialty policies that do not explicitly exclude cyber. This emphasises the critical role of the standalone cyber market where the risk is well quantified.

Legal and regulatory changes in Europe should be seen as the start of a wider conversation globally: While this report focuses on the changes in Europe, the Notification of Serious Data Breaches Act in consultation in Australian or recent changes to Japanese breach legislation are also taking place and will have a profound impact on the insurance regime in local regions.

Aon Benfield's dedicated cyber team is partnering with re/insurers on legislative and regulatory changes to help grow their cyber books while avoiding pitfalls in the market:

- CyberMetrica to quantify potential aggregation risks and prepare for growth opportunities
- Standalone cyber stop losses and uncapped quota share reinsurance
- Cyber Risk Diagnostic Tool to identify your exposure as a firm with practical advice

Moving towards a common legal environment for cyber

An interesting characteristic of cyber as a peril is that it **geographically has less relevance** compared to traditional lines of business. For property catastrophe cover, an underwriter can make an educated guess about the susceptibility of a risk located in the Florida Keys or near a flood plain. Cyber is different as the risk is intrinsically detached from geography as an attack can take place anywhere, from anywhere and by anyone who is connected to the network.

However, from a risk management perspective, there are two key factors posing a challenge to a consistent global response:

- Inconsistent privacy laws across key insurance markets, in particular Japan and Europe
- Limited financial or legal penalties for failing to protect customers data

US market drivers

To start looking at remedies, it is important to understand the drivers in the US where recent estimates put the proportion of business against the rest of the world as at a 90-10% split. This differs greatly from mature classes of business such as property, motor or casualty risk which are more evenly spread across the world.

In the United States, 47 of the 50 States have state-wide breach notification laws [the three that do not are Alabama, New Mexico and South Dakota. These detail breach response procedures, stipulate fines and regulate corporate activity. This, combined with the punitive legal system in the United States, has created fertile ground for cyber insurance to take route.

Additionally, technology firms, financial services and private healthcare – three sectors that make up a large proportion of the economy – have a high demand for cyber insurance solutions due to the value of their customer data and intellectual property. As a result the cyber market has established itself in primarily in the US and is still to emerge as a significant class within other key global insurance markets.

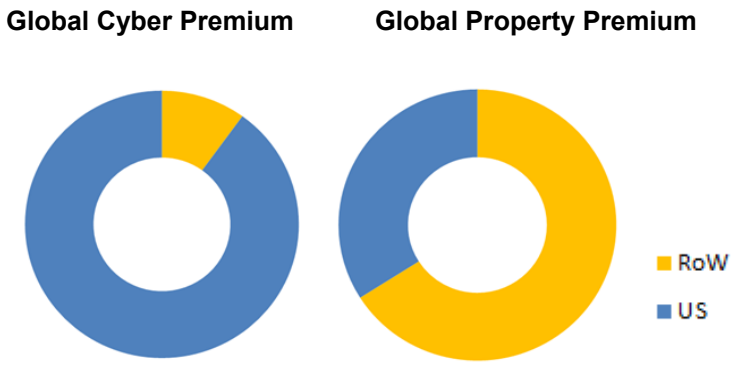

Figure 1: US cyber premiums dwarf the rest of the world compared the the traditional property market

This has a number of effects on the development of cyber products:

- Firstly, policies are overwhelmingly designed to deal with third party liability due to the litigious environment in the US – which is not as pertinent to a large proportion of the world
- Secondly, an overreliance on US policies is viewed as a potential aggregation risk and now, insurers are looking to diversify by broadening their geographical scope

Driving change in Europe: General Data Protection Regulation

The ratification of the General Data Protection Regulation in April 2016 should represent a sea change in the European cyber insurance market and will be a key moment in the trajectory of cyber risk as a peril. As in the US, this regulation should act as a trigger for growth.

The policy comes into force in May 2018 and helps to address some of the current shortcomings of the EU legal framework on cyber risk creating a common set of procedures, requirements and, importantly, sanctions. There are four elements worth highlighting at this stage:

1. The policy **standardises** the legal penalties and notification procedures for data breaches across the European Union

2. It covers **all corporations** that handle EU citizens' data and not just European organisations

3. All data breaches must be **reported to a designated supervisory authority** immediately upon discovery

4. Failure to abide by the GDPR can lead to fines of up to **4% of total worldwide annual turnover**

The development of a standardised framework should provide insurers with an opportunity to engage with European markets and provide comprehensive coverage to protect against falling foul of the GDPR, while diversifying their cyber portfolios. Insurers can also look to enhance their offering by providing breach response assistance to help communicate to supervisory authorities and European citizens whose data have been breached, PR companies to manage their media image and forensic teams to investigate the cause and remedy.

This will both stimulate the European cyber market space and act as an accelerant of cyber provisions in other developed markets such as US, Japan, Singapore and South Korea: As the policy covers all companies engaging with EU customers – in the largest single economic market – this will require all multinationals to be conversant in the GDPR.

Building data and analytics

In addition, mandatory breach notification will also address another key limitation of the current European cyber market by providing loss history. This will allow re/insurers to:

- assess the risk of certain subsections of the cyber market and lead to the development of more sophisticated products

- place further onus on analytics to help translate this loss history and develop useful metrics of risk such as risk scores, sector benchmarking and comparative analysis

- build on existing US data for more nuanced pricing tools, aggregation management systems and bespoke risk scenarios to improve capacity of the market and hopefully lead to the standardization of wording and pricing within this sphere.

Aon is working with re/insurers to guide them through the GDPR – both in terms of ensuring that they have protection in place in time for its 2018 implementation and how they can seize an opportunity to underwrite new business to protect against the legislation.

Driving change in Europe: Lloyd's cyber-attack scenarios

Along with changes to the legal environment, readers will be well aware that regulators have been taking a closer look at the cyber market. Lloyd's has been at the forefront of this effort. The Lloyd's market has seen a significant growth in standalone cyber premium of over 45% year on year since 2012 and as a result has taken a very keen interest in the levels of cyber risk for each syndicate.

In August 2016, Lloyd's published a list of eight market-level scenarios for cyber-attack that every syndicate is required to model as part of quarterly reporting. This suite of scenarios has resulted from a process of consultation with the market and external experts over the last two years.

In requiring syndicates to systematically consider accumulation risk for cyber-attack – including incidental or 'silent' cyber – Lloyd's has attempted to strike a balance between encouraging organic growth of this emerging specialist class of business, and creating an oversight structure that recognises the potential for systemic losses.

For each scenario, syndicates have to provide Gross and Net loss-estimates for all lines of business potentially affected, taking into account any exclusions. Syndicates must therefore assess the robustness of their cyber exclusions, and how these would apply to the hypothetical scenarios.

The exercise allows Lloyd's to accumulate returns across all syndicates to arrive at a preliminary market-level understanding of potential losses, including from 'silent' cyber exposure.

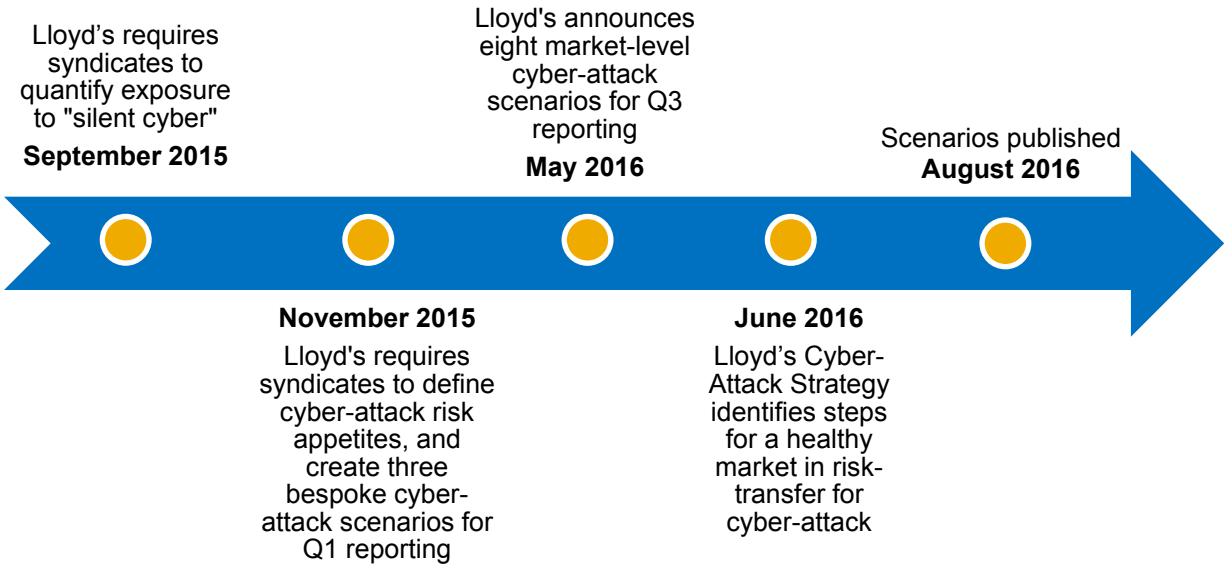

Figure 2: The evolution of Lloyd's cyber reporting requirements over time since 2015

Importantly, the eight scenarios should not be seen as the final word on Lloyd's oversight of the cyber-attack market. Lloyd's has been explicit that this is a process of enquiry, consultation and education which will evolve over time. A driver of change will be when data standardisation reaches a sufficient level to allow more nuanced scenarios and risk capture procedures.

Analysis of the cyber scenarios

When looking at the scenarios, several points are striking from the offset.

Identifying silent cyber exposure

Firstly, the scenarios are not confined to the standalone cyber market. Lloyd's has explicitly expressed concern about the capture of what it calls 'silent' cyber risk: exposure assumed by default (or lack of exclusion) within policies such as property, marine or liability.

The scenarios exercise reflects a concerted effort by Lloyd's to disseminate existing knowledge to all providers of this coverage within the market, forcing them to quantify the accumulation potential of the risks they have assumed. This may lead to sub-limits or exclusions for cyber-attack risk becoming common within traditional insurance lines, and the emergence of specialist classes allowing risk-transfer of these elements.

Such a development would increase the demand for standalone cyber coverage and allow Lloyd's and regulators to comprehensively monitor cyber risk and its growth while putting underwriting decisions in the hands of the individuals who best understand the peril.

Managing tail end events

Secondly, the events included are at the tail end of the spectrum in terms of severity. This may reflect the fact that the market remains in its infancy. We have limited loss history, analytics is still at its developmental stage and we have not seen the "hurricane Andrew of cyber events". As a result a cautious approach to monitoring this risk is not only sensible but necessary.

The scenarios include different types of events that could only be triggered as a consequence of a cyber-attack incident. Lloyd's is trying to put the scenarios in context for the market so they are not merely an academic exercise but encourage syndicates to think about and understand how cyber can have a severe impact on the their books in a different way to traditional threats.

Understanding the impact on property damage

Thirdly, excluding the cloud and data theft scenarios, the other six scenarios include some element of property damage as a consequence of the cyber-attack. The history of cyber-attacks causing physical damage is relatively small with only a couple of high profile events such as the Stuxnet virus or the 2014 attack on a German Steel Mill so it is interesting that Lloyd's has chosen to prioritise this route.

One reason for this could be the growth of cyber property damage coverage over the last couple of years. While still relatively small and dwarfed by standard data breach products, the proportion of cyber coverage including property damage (CZ code) has increased roughly 100% since 2014. While other cyber products such as data breach protection (CY code) continue to increase its premium growth compared to 2014 is significantly smaller.

The negative trajectory of premium growth for other lines also raises another issue that regulators are trying to guard against: the poorly thought-out inclusion of cyber risks within other lines to shore up premium rates. This is problematic from the regulator perspective as it is difficult to quantify the risk but also raises issues if underwriters who do not necessarily deal with the cyber market on a day to day basis try to place business in their sphere.

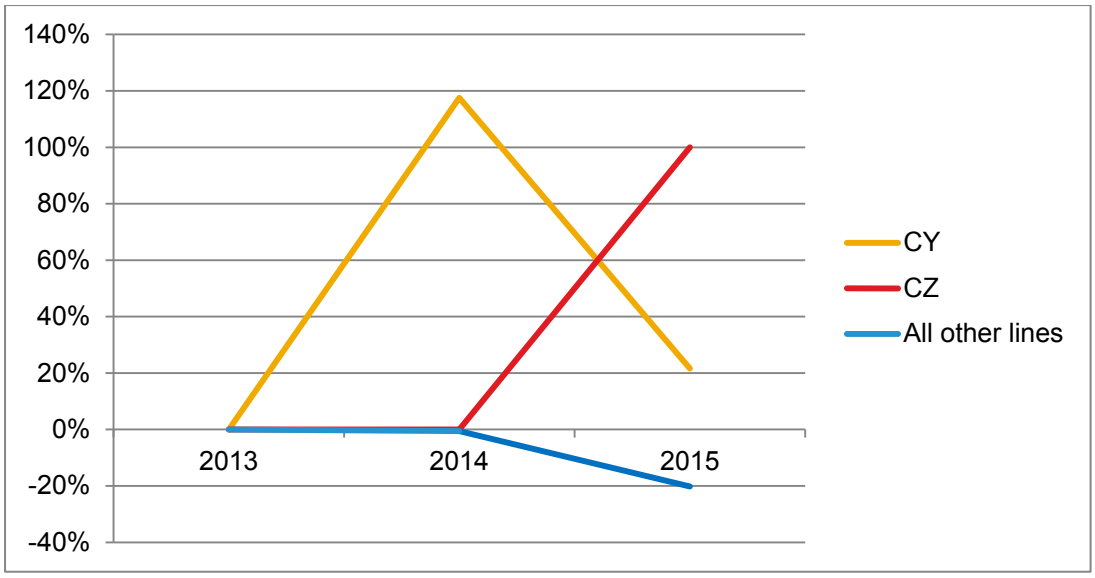

Figure 3: Premium growth within the Lloyd's market in the cyber market and other lines since 2013

This is particularly true given that there is very limited standardisation within the cyber market for terms and conditions, plus the relatively complex procedure for cyber claims. Complex factors such as breach response, notification, PR, regulatory response and forensics are vital and can drastically limit the scale of a claim. As a result it makes sense that cyber insurance sits solely within the cyber market or in the hands of relatively sophisticated Errors & Omissions carriers.

Understanding aggregations across lines

Finally, the scenarios do not simply focus on the property market but cover markets as wide as energy, aviation and marine. This touches upon a final point that Lloyd's is looking to emphasise: cyber-attack can be a major concern across all lines of business, all of which must have a rudimentary understanding of this risk in order to avoid significant potential aggregations. This will be a trend that will continue to crystallize over time.

An evolution in cyber modelling

Cyber cannot be modelled in the same way traditional natural catastrophe risk as geospatial information reduces in importance and other variables come to the fore. As a result insurers need to capture information such as revenue, sector, number of employees, cloud computing providers and security protocols in place at the insured risk. Not only is this information difficult to capture but it will require a cultural change amongst insurers to correctly identify this information.

One avenue to accelerate this process has been the development of a common data capture framework that was agreed alongside the two major catastrophe modelling firms, AIR and RMS, giving re/insurers a template to capture this risk. As a result Lloyd's is likely to expect insurers to improve their data capture over time which will be reflected in the increased sophistication of cyber scenarios over the next few years.

This puts the onus on modelling firms, brokers and start-ups to develop analytics that provide a common language to quantify cyber risk and help new and established players in this field understand the risk in a comprehensive manner. Indeed, the Lloyd's report has been shared with a number of modelling firms including RMS, AIR and Cyence emphasising the central role these groups will play in the future of cyber reporting.

Conclusion

The growth of cyber as a class of business within the insurance and reinsurance market has given regulators and government agencies significant food for thought over the last couple of years. The changes that have been implemented thus far represent sensible interventions by both the European Union and Lloyd's to help improve both the sophistication and standardisation of the market.

By improving the legal framework, the EU has laid the foundation for a more expansive and diverse cyber insurance market to take hold and allow the traditionally large insurance markets in France, Germany, Italy and the UK[1] to pull their weight in the cyber sphere. It will also create a new catalogue of products designed to deal with the GDPR specifically and help non-European multinationals navigate this space.

Additionally Lloyd's has taken steps to steer the cyber market in London towards the more robust standalone cyber market and away from silent cyber policies. This will improve both the demand for cyber specific products and help drive the sophistication in the market. They have also laid the groundwork to pre-empt the growth of the cyber-linked property damage market that could develop into a significant product in the manufacturing, heavy industry and energy sectors.

The added benefit of Lloyd's activities is also the wider education of the market. By taking a broad brush to cyber exposure management Lloyd's is insuring that every sector must have at least a rudimentary awareness of this peril. This can only be a good approach and will put cyber risk at the centre of the insurance market for years to come.

Finally, this is only one snapshot of an overall trend. The actions of Lloyd's in the London market and the EU Parliament will not necessarily by replicated globally as other agencies deal differently with their own local insurance markets according to their appetites for cyber insurance risk. As a result it is critical for major players in this market to be aware of global regulatory changes and their impact.

Take action now to build for future resilience and growth

Aon Benfield's Cyber Practice Group is helping re/insurers to navigate Lloyd's scenarios and future regulatory developments. Using our dedicated cyber analytics resources, Aon can efficiently calculate the losses incurred from such events and develop bespoke scenarios to help exposure management teams deal with this emerging risk. Using our analytical capabilities we can help clients understand accumulation risk, pricing and the quantification of "silent cyber" exposure to be better placed to take advantage of this growing class of business.

Our cyber broking team can advise on current market strategies to mitigate this risk and enable re/insurers to grow their books in a sensible and controlled manner – plus obtain protection from standalone cyber stop losses and uncapped quota share reinsurance to deal with the systemic threat.

[1] Initial soundings from Downing Street and the Prime Minister regarding the implementation of the GDPR post-Brexit suggest that the UK will comply with this legislation even if they are outside the union in 2018

Notes

Contact Information

Mark Lynch
Cyber Analytics
Aon Benfield | Global Re Specialty
+44 (0) 7714 180 176
mark.lynch@aonbenfield.com

Tom Wakefield
Head of Marine, Specialty, Composite
Aon Benfield | Global Re Specialty
+44 (0)20 7086 3625
tom.wakefield@aonbenfield.com

Jonathan Laux, FCAS
Head of Cyber Analytics
Aon Benfield | Cyber Analytics
+1 312.381.5370 | m: +1 708.908.0807
jonathan.laux@aonbenfield.com

Bill Henriques
Co-head of the Cyber Practice Group
Aon Benfield | Cyber
+ 1 973.966.3565 | m +1 917 374 3622
bill.henriques@aonbenfield.com

About Aon

Aon plc (NYSE:AON) is a leading global provider of risk management, insurance brokerage and reinsurance brokerage, and human resources solutions and outsourcing services. Through its more than 72,000 colleagues worldwide, Aon unites to empower results for clients in over 120 countries via innovative risk and people solutions. For further information on our capabilities and to learn how we empower results for clients, please visit: http://aon.mediaroom.com.