Lloyd's Cyber-Attack Strategy

LLOYD'S

Lloyd's Cyber-Attack Strategy
Introduction

The focus of this paper is on insurance losses arising from malicious electronic acts, referred to throughout as "cyber-attack". The malicious act is the proximate cause of loss, although the consequences may include property damage, bodily injury, financial loss or other forms of damage.

Cyber-attacks are increasing in frequency across the world – reported attacks were up 48% on 2013 levels to 42.8 million in 2014, the equivalent of 117,339 attacks a day. The compound annual growth rate of detected security incidents has increased 66% year on year since 2009.[1]

Not only has the frequency of attacks increased, so too has the cost of managing and mitigating breaches. The estimated reported average financial loss from cybersecurity incidents around the world in 2014 was $2.7 million – a 34% increase on the 2013 figure.[2]

This increase in attack frequency and severity is reflected in the increasing amounts of business written by the Lloyd's market. In 2015, the Lloyd's market wrote £322 million-worth of cyber policies, up from £206 million in 2014; in 2016, this is expected to rise to £500 million. In 2013, the number of Lloyd's syndicates writing cyber was 22; in 2016, it is 63.[3]

Currently, more than 80% of Lloyd's market cyber premium income comes from the US, with 6% from the UK, 1% from the rest of Western Europe and the remaining from the rest of the world.[4]

The EU's Network Information Security Directive and General Data Protection Regulation, which were both agreed in 2015 and, in the case of the latter, will introduce mandatory incident notification and fines for the most serious breaches of the new rules. These are likely to raise Board-level awareness of cyber risks further and consequently drive demand for cyber insurance from European businesses.

Globally, some analysts estimate the worldwide cyber insurance market could be worth $18 billion by 2025 – up from $2.5 billion today.[5]

The Corporation of Lloyd's (Lloyd's) – the body that oversees the Lloyd's market – has a number of initiatives under way to ensure the Lloyd's market is well-placed to compete for the new business opportunities this growth is expected to generate.

One of these initiatives is the development of Lloyd's Cyber-Attack Strategy.

Notes:

1 The Global State of Information Security Survey 2015 – PwC US. http://www.pwc.com/us/en/press-releases/2014/global-state-of-information-security-survey-2015.html

2 The Global State of Information Security® Survey 2015 – PwC US. http://www.pwc.com/us/en/press-releases/2014/global-state-of-information-security-survey-2015.html

3 Lloyd's Class of Business data

4 Lloyd's Class of Business data

5 Swiss Re expects an increase of the global cyber insurance premium volume to about US$ 18 billion until 2025 – p21. http://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/studien/cyberrisk2016.pdf

Why a cyber-attack strategy is needed

The emergence of a new societal threat in the form of cyber-attack is creating the urgent need for appropriate risk-mitigation and risk-transfer mechanisms.

The Lloyd's market is well placed to offer risk-transfer solutions, building on its proven ability to innovate in response to the changing business environment. However, it is also necessary to consider the risks. Lloyd's must balance the need for fast-paced innovation with the need for appropriate oversight and control.

There are two main challenges. First, Lloyd's needs to ensure that cyber-attack insurance is not unintentionally given away "free" as part of standard policy wordings. This is not to discourage the inclusion of cyber-attack coverage – only to ensure that the risk is clearly identified and understood, and that potential costs are reflected in the premium. Only by pricing the risk appropriately can insurers offer a sustainable risk-transfer mechanism for cyber-attack.

Second, Lloyd's, and the insurance sector in general, need to understand the potential for large accumulations of cyber-attack risk. Put simply, what is the worst that could happen?

Lloyd's is leading the way in researching both areas.

The remainder of this paper focuses on the steps Lloyd's is taking to manage the second challenge: very large accumulations of (re)insurance exposure to cyber-attack risk.

As part of its Cyber-Attack Strategy, Lloyd's aims to develop good practice for the Lloyd's market for understanding catastrophic risk, and share insight that may be helpful in shaping future business planning and public policy more widely.

The story so far...

The Lloyd's market currently insures cyber-attack risk in two main ways:

- Specific cyber insurance policies, covering risks such as data breach, data-loss and cyber extortion

- "Traditional" policies (e.g. Property, Marine, Casualty) where cyber-attack has the potential to cause a loss

Catastrophic losses from cyber-attack can arise from any line of business, including from policies that do not state whether cyber-attack is covered or not (known as "silent cyber").

The first stage of Lloyd's Cyber-Attack Strategy involved asking syndicates to provide details of the risk-management frameworks they have in place for cyber-attack, their risk-appetites, and the factors they take into account when underwriting and pricing this business.

The second step involved syndicates developing and reporting their own internal "cyber-attack scenarios" as a means of considering worst-case accumulations of risk. Scenarios are widely used to estimate catastrophic (re)insurance losses of all kinds. These techniques are broadly applicable to cyber-attack.

To encourage a plurality of views and approaches, Lloyd's provided minimal guidance on scenario development – it was up to the syndicates themselves to define what they did, and how and why.

The requirement was for syndicates to create at least three internal "plausible but extreme" cyber-attack scenarios as stress-tests for catastrophic cyber-attack losses[6] and to calculate the total gross aggregate exposure to each scenario across all classes of business, including silent cyber.

For the first reporting cycle, syndicates had the option of including loss estimates for the scenarios as well as total gross aggregate exposure. In future, this will be a compulsory part of their returns to Lloyd's.

From this information, Lloyd's has determined:

- Syndicates' appetites for accepting cyber-attack risk across all lines of business
- Which classes of business each syndicate considered to be most at risk from cyber-attack
- How syndicates build and use scenarios to assess cyber-attack aggregate exposure

Lloyd's Cyber-Attack Strategy

By 31 December 2017, Lloyd's will have:

- Supported the continuing evolution of cyber-attack (re)insurance products within the Lloyd's market, appropriately underwritten and capitalised
- Encouraged the development and use of appropriate exclusions and/or sub-limits for cyber-attack, perhaps by extending existing War and Terrorism exclusions
- Developed a structured understanding of cyber-attack accumulation risk, including metrics to measure loss-potential including silent cyber
- Established good practice for representing cyber-attack risk (including catastrophe risk) in syndicates' capital models and Lloyd's Internal Model
- Reduced the potential for silent cyber-attack accumulation by:
  - Identifying classes of business and policy-types particularly subject to residual silent cyber-attack leakage
  - Developing approaches to pricing and capital-setting for silent cyber-attack risk
- Developed Lloyd's global brand for cyber-attack expertise with existing policyholders, new customers, government agencies and regulators

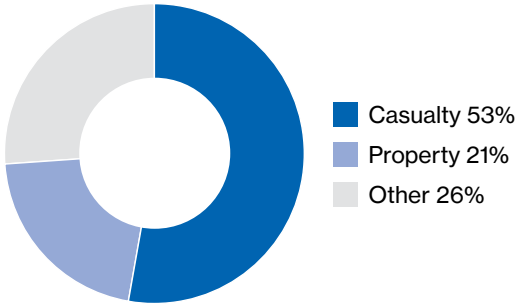
Notes:

[6] A number of syndicates already use internal scenarios for stress-testing cyber-attack, in which case they can adapt them for Lloyd's reporting

Key findings

The syndicates' cyber-attack scenarios showed that the Lloyd's market is bringing a wide variety of techniques to bear on the problem of systematically considering catastrophe risk.

Out of the total reported aggregate exposure, for all scenarios combined, business classed[7] as Casualty contributed 53% and those classed as Property contributed 21%.[8]



Types of event considered in the scenarios included:

- Interruption to online services
- Widespread electricity blackout
- Business interruption following property damage
- Marine collision
- Damage to healthcare infrastructure
- Aviation collision
- Leaking of private information
- Breaching server security
- Damage to industrial facilities
- Widespread dedicated denial of service attacks

All Lloyd's 10 classes were referenced to some degree in the scenarios submitted.

An example of a multi-class scenario is as follows:

> A large industrial facility in the US, housing multiple companies, workers and physical assets is targeted by terrorists who launch a cyber-attack against the industrial control systems used to operate the facility. Instantly, the plant's temperature monitoring controls fail and the facility continues operating at incorrect temperatures. An explosion severely damages the plant, causing fire to spread to nearby property. Workers, first responders and members of the public are injured in the blaze, and harmful chemicals are released into the atmosphere.

Notes:

[7] Lloyd's 10 classes of business

[8] Casualty includes standalone cyber policies as well as other broader Casualty products

Conclusion

From the cyber-attack scenarios submitted by the syndicates, Lloyd's was able to identify common themes. In particular, analysis showed that three primary considerations are being taken into account when syndicates are designing scenarios:

1. What is the motive for the attack?

2. Which sectors in society are being targeted?

3. Who is carrying out the attack?

It is clear that the Lloyd's market is developing a robust understanding of the catastrophe risk posed by attacks aimed at cyber infrastructure for financial gain – in other words, attacks on data itself (e.g. hacking, denial of service, data-breach, theft of personal information). These types of losses are – at least theoretically – capable of being quantified and controlled by appropriate underwriting and accumulation-management. Not coincidentally, they are also the risks primarily covered by existing cyber insurance policies provided in the Lloyd's market.

By contrast, it is far more challenging to quantify exposure to cyber-attacks launched with wider political or social aims, or against national physical or cyber infrastructure. Again, not coincidentally, there are fewer specific products and greater incidences of silent cyber exposure. This has the potential to expose syndicates to greater risk from unexpected accumulations.

In the light of these findings, Lloyd's has defined the next steps within the Cyber-Attack Strategy so as to understand in greater detail syndicates' exposure to accumulation and the factors they take into account when assessing potential catastrophic losses.

Next steps

1. Understanding and pricing cyber-attack risk
   Lloyd's will continue to consult the market and the Lloyd's Market Association to determine the extent to which existing exclusions for acts of war and/or terrorism may cover cyber-attacks.

2. Market oversight and regulation
   Lloyd's Exposure Management team regularly reviews syndicate performance against the Minimum Underwriting Standards. These will now include specific reviews of syndicates' cyber-attack risk-management frameworks.

   Independent reviewers have been asked to focus on cyber-attack coverage provided at case level and look at how this fits within syndicates' cyber-attack risk management frameworks.

   Lloyd's will work with the regulator – the PRA – to ensure its response to Lloyd's cyber work is considered and proportionate.

3. Reporting
   As part of Q2 reporting on 30 June, Lloyd's will ask syndicates to split their internal cyber-attack scenario reporting for Casualty classes of business between cyber policies (CY/CZ risk codes) and other casualty exposures.

4. Lloyd's intends to publish eight to 10 new cyber-attack scenarios in September 2016
   Following the review of the syndicates' cyber-attack scenarios, Lloyd's is consulting market participants and working with other experts, including the modelling company Cyence and colleagues working on the CYRIM initiative in Singapore.

This work is designed to help Lloyd's develop a series of cyber-attack scenarios, each centred on one of the Lloyd's 10 main classes of business.

These scenarios should allow, for the first time, the possibility of gaining a consistent view of accumulation risk – including silent cyber – across the market, in a way that is relevant for the broad business classes underwritten by the Lloyd's market.

These cyber-attack scenarios will not be considered Realistic Disaster Scenarios or be used formally for business-planning and/or capital setting purposes at this stage. Franchise Guidelines will not apply. In particular, the scenarios will not in any way constitute the Corporation's formal, final, considered view of cyber-attack risk.

However, the scenarios will be a next important step, and Lloyd's may develop them further in consultation with the market and its evolving network of expert colleagues around the world (including government agencies).

Many thanks to the many syndicates and managing agents who's modelling and insights contributed to this report.

Published June 2016