LLOYD'S

Lloyd's Cyber Risk Strategy

Introduction

This paper reviews and refreshes the Lloyd's Cyber Attack Strategy published in 2016.

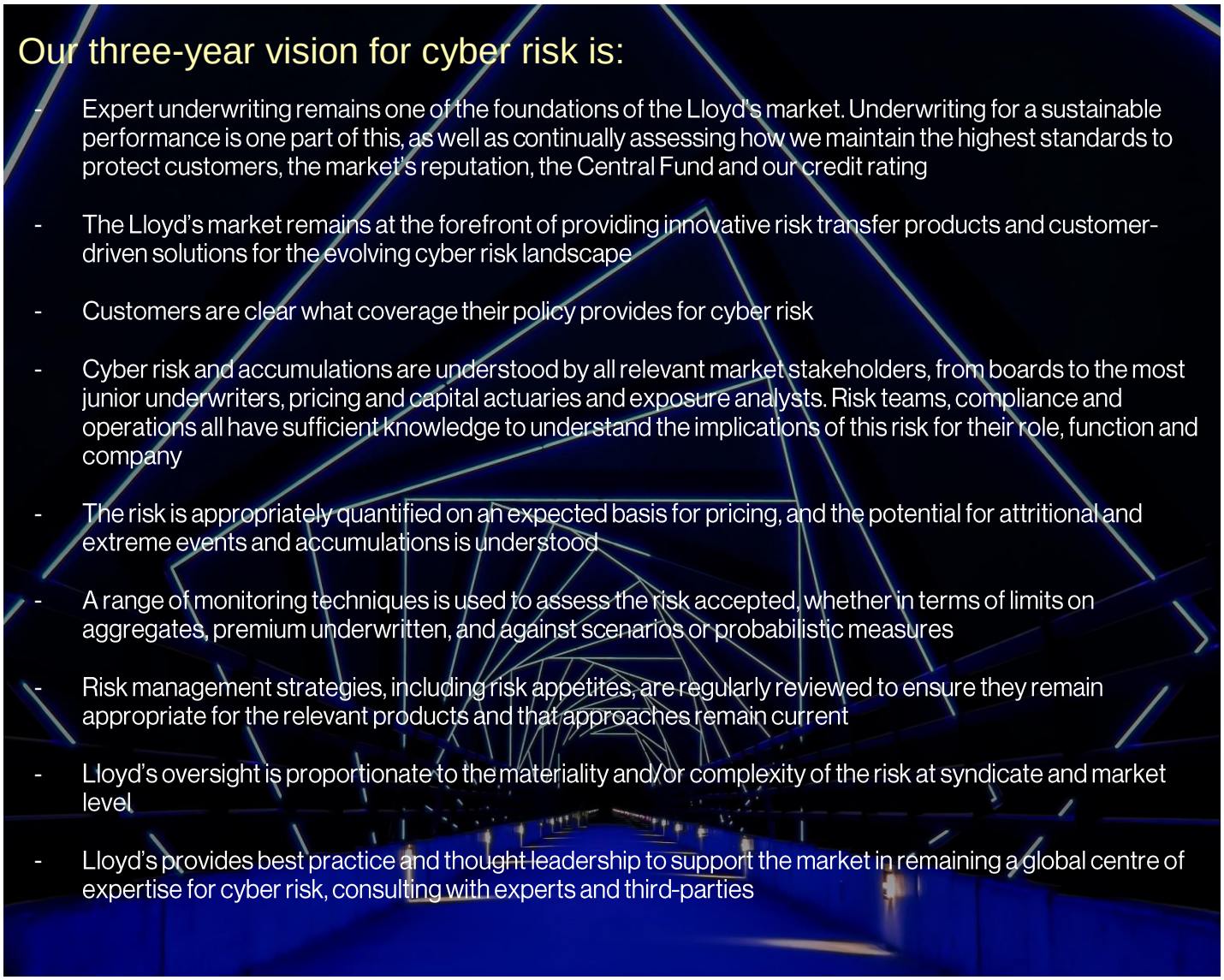
The updated strategy sets out Lloyd's vision and plans for the oversight of cyber risk so that all stakeholders understand our direction and the reasons for our actions.

Lloyd's is committed to delivering this strategy with the market, working alongside the London Market Association (LMA).

In this context, cyber risk[1] is any risk where losses are cyber-related, whether arising from malicious acts (e.g. cyber-attack, infection of an IT system with malicious code) or non-malicious acts (e.g. loss of data, accidental acts or omissions) involving tangible or intangible assets. 'Attack' has been removed from the new strategy title to include non-malicious acts, and align with the Prudential Regulation Authority's (PRA) cyber risk definition. The definition adopted is intended to capture standalone cyber products (coded CY and CZ in Lloyd's) as well as losses caused by cyber risks in other lines of business.

[1] Note that the treatment of operational cyber risk in insurance companies is not within the scope of this strategy paper

Vision for cyber risk at Lloyd's



Our three-year vision for cyber risk is:

- Expert underwriting remains one of the foundations of the Lloyd's market. Underwriting for a sustainable performance is one part of this, as well as continually assessing how we maintain the highest standards to protect customers, the market's reputation, the Central Fund and our credit rating
- The Lloyd's market remains at the forefront of providing innovative risk transfer products and customer-driven solutions for the evolving cyber risk landscape
- Customers are clear what coverage their policy provides for cyber risk
- Cyber risk and accumulations are understood by all relevant market stakeholders, from boards to the most junior underwriters, pricing and capital actuaries and exposure analysts. Risk teams, compliance and operations all have sufficient knowledge to understand the implications of this risk for their role, function and company
- The risk is appropriately quantified on an expected basis for pricing, and the potential for attritional and extreme events and accumulations is understood
- A range of monitoring techniques is used to assess the risk accepted, whether in terms of limits on aggregates, premium underwritten, and against scenarios or probabilistic measures
- Risk management strategies, including risk appetites, are regularly reviewed to ensure they remain appropriate for the relevant products and that approaches remain current
- Lloyd's oversight is proportionate to the materiality and/or complexity of the risk at syndicate and market level
- Lloyd's provides best practice and thought leadership to support the market in remaining a global centre of expertise for cyber risk, consulting with experts and third-parties

The dynamic landscape

Standalone cyber insurance is one of the fastest growing sectors of the insurance industry. In the next five years, various sources estimate that it could reach more than USD $25 billion in premiums, from around USD $4 billion in 2018.

Within Lloyd's, planned gross written premium (GWP) for cyber classes (CY and CZ risk codes) in 2019 is approximately GBP £1.2 billion, up from GBP £397 million in 2015. This represents an increase from 1.3% to 3.6% of total Lloyd's GWP. Although Lloyd's has a comparatively high global market share (approximately 33%), cyber is still a small proportion of the overall business underwritten within the Lloyd's market.

However, organisations of all sizes, geographies and industries are increasing their reliance on data analytics and technology, with continued advances in cloud computing, artificial intelligence, 5G, the Internet of Things (IoT), mobile devices, automated supply chains and distributed ledger/blockchain[2], amongst many others.

Each of these advances creates new and different cyber risks and exposures, as evidenced by the continued high profile of cyber peril events (e.g. Not Petya and WannaCry, both in 2017), and developments in data breach legislation (such as General Data Protection Regulation [GDPR] that came into effect on 25th May 2018). These changes in the risk landscape could impact insurance products written in conventional lines of business as well as the standalone cyber market.

Although large scale cyber-attacks rank sixth in a list of risks most likely to materialise in the next 10 years[3], and it is estimated that cyber-attacks cost the global economy USD $600 billion in 2017[4], only a fraction of these are adequately insured. This presents a significant opportunity to fill a protection gap. However, aggregated cyber exposures have the potential to cause losses that are multiples of any cyber losses seen to date[5] and there have been various reports published by Lloyd's and thought-leadership partners (see Appendices for details) to provide examples of these.

[2] Aon: Perils in a Growing Market, Feb 2019

[3] The Global Risks Report 2017, 12th Edition. World Economic Forum. Available at: http://www3.weforum.org/docs/GRR17_Report_web.pdf

[4] McAfee and The Center for Strategic and International Studies (CSIS). Economic Impact of Cybercrime No Slowing Down. Available at: https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf

[5] Revealed: the Cyber Achilles heel for huge companies. https://www.insurancebusinessmag.com/us/news/cyber/revealed-the-cyber-achilles-heel-for-huge-companies-109864.aspx

Why Lloyd's has a cyber risk strategy

Cyber perils are growing as a societal threat; this is creating an urgent need for appropriate risk mitigation and risk transfer mechanisms.

The Lloyd's market is well-placed to offer these risk transfer solutions, building on its proven ability to innovate in response to new opportunities.

However, it is also necessary to consider the risks which come with these opportunities. Lloyd's must therefore continue to balance the need for fast-paced innovation with appropriate oversight and control. To respond to these challenges, in 2016 Lloyd's published a cyber strategy with the six objectives listed below:

Lloyd's Cyber Attack Strategy 2016 – Six Objectives

- Support the continuing evolution of cyber insurance and reinsurance products within the Lloyd's market, appropriately underwritten and capitalised
- Encourage the development and use of appropriate exclusions and/or sub-limits for cyber risk, perhaps by extending existing war and terrorism exclusions
- Develop a structured understanding of cyber accumulation risk, including metrics to measure loss potential, including silent cyber
- Establish good practice for representing cyber risk (including catastrophe risk) in syndicates' capital models and Lloyd's internal model
- Reduce the potential for silent cyber claims accumulation by:
  - Identifying classes of business and policy types particularly subject to residual silent cyber loss leakage
  - Developing approaches to pricing and capital setting for silent cyber risk
- Develop Lloyd's global brand for cyber risk expertise with existing policyholders, new customers, government agencies and regulators

Progress since 2016

As part of its cyber strategy, Lloyd's has developed good practices for understanding the dynamic landscape of cyber risk to date, and has shared insights to help shape future business planning and public policies more widely. Activities undertaken include:

- Lloyd's Market Insight (LMI) reports[6] published by the Class of Business team:
    - Cyber risk cover, physical damage
    - Monitoring of cyber-attack risks
    - Cyber-attack survey results and other cyber oversight feedback
    - Cyber underwriting: A good practice guide
- The innovation team has partnered with a range of organisations to produce the following reports[7]:
    - Counting the cost: Cyber exposure decoded
    - Cloud Down: Impacts on the US economy
    - Bashe Attack: Global Infection by Contagious Malware
    - Lloyd's Digitalisation Series
    - Shen Attack: Cyber risk in Asia Pacific ports
- Lloyd's has aligned its oversight stance with the PRA's Supervisory Statement SS4/17 'Cyber insurance underwriting risk' (July 2017), as detailed in Market Bulletin Y5147 'Cyber Insurance – PMD updated approach to oversight' (Dec 2017).
- Data collection exercises since 2016 have allowed the Lloyd's risk aggregation team to gain a broad oversight of cyber risk activities, determine which classes of business each syndicate considers to be most at risk from cyber claims, and how syndicates build and use scenarios to assess aggregate cyber exposure.

  From this process a set of scenarios was produced, in conjunction with third-party subject-matter experts, to cover each of the Lloyd's 10 main classes of business. Over time this has been condensed to the three "plausible but extreme" scenarios that are currently reported, as detailed on page 6 of Market Bulletin Y5131, and detailed in Cyber-Attack - Scenario Specifications[8] (Jan 2018), specifically:

  1. Cloud service provider hack
  2. Northeast US blackout - standard
  3. Northeast US blackout – extreme

  Cyber scenario accumulation is a relatively new discipline for many syndicates, therefore these stress-test scenarios have not been considered 'fully-fledged' realistic disaster scenarios (RDSs) and are not currently used formally for planning and capital. They are reported twice per year as part of RDS exercises. At the same time, syndicates provide three of their own additional scenarios so that Lloyd's can continue to gather information on market trends and loss patterns, as well as the risk to individual syndicates.
- There has been continual oversight of syndicates' representation of cyber risk in their capital models which has informed the parameterisation of this risk in the Lloyd's internal model (LIM).
- Lloyd's has formed a cross-departmental cyber working group to improve communication and coordination across the organisation.

[6] Requires a lloyds.com account, and only available to Lloyd's Managing Agents' employees. More report details available in Appendix 1

[7] More report details available in Appendix 2

[8] Requires LMA full-member log-in

The new strategy, 2019 and beyond

To update the 2016 strategy, and to implement Lloyd's cyber vision, we consulted with managing agents that write high levels of cyber premium, some who contribute most to the Northeast US blackout scenario, and others to get a balanced level of input. Over the six-month period we also spoke with cyber model and tool vendors, expert advisory groups and other experts in this field to understand how the landscape and challenges have changed since our last strategy document.

This research showed two main challenges remain:

1. The market must do more to ensure that cyber exposures are specifically underwritten and priced, regardless of lines of business, or excluded. This is not to discourage the inclusion of cyber coverage; rather it is to ensure the risk is clearly identified, understood and reflected in the premium. Only by identifying, quantifying and pricing the risk appropriately can insurers offer a sustainable risk transfer mechanism for cyber perils, and provide clarity for the customer.

2. The market needs to understand the potential for large accumulations of cyber claims. This includes work on better data capture and quantification methodologies, so that cyber "cat" exposure and risk management evolve as a discipline.

We have updated the strategy accordingly to support our vision (on page 3) for cyber risk.

In the next three years, our goals to achieve our vision are that:

- The Future at Lloyd's will supercharge innovation, allowing development of new products that specifically address customers' cyber risks
- Innovative cyber lines and products will be supported through Lloyd's planning process
- All policies will be clear on coverage for losses caused by cyber risks. This will be introduced on a phased basis from January 2020, starting with first-party property damage
- Aggregation scenarios will undergo a thorough review and update so that we are confident we are assessing true market-level risk aggregation
- The adoption of best practice will continue to be promoted, and best practice guidance will be developed, communicated and its adoption monitored as part of Minimum Standards oversight, including:
  - Underwriting: coverage, evaluation, pricing, appetite, and expertise
  - Data standards and data capture
  - Representation of cyber risk in capital models
- Cyber will no longer be regarded as a "new" risk. Oversight of cyber will be more closely integrated into business-as-usual oversight, including review work and the planning process
- Lloyd's will provide annual updates of progress against these items, and our strategy will be updated as appropriate to reflect the rapidly evolving cyber risk landscape

Delivering the new cyber risk strategy

To deliver these goals tactically, Lloyd's has defined high-level themes with associated workstreams. These are listed below. Due to the dynamic nature of cyber insurance this is not an exhaustive list and will change.

RDS, aggregation scenarios and exposure management

- The existing RDS and other scenarios will be reviewed to update and enhance them where required. We want up-to-date methodologies that are sufficiently prescriptive so the potential losses submitted by each syndicate can be aggregated at market level. This work will be done in close collaboration with the LMA cyber risk strategy group and relevant class-specific sub-groups. Lloyd's will consult with cyber experts and model vendors to identify the newest and most relevant threats. It is anticipated that the bulk of the work will take place in Q4 2019/Q1 2020 so that details of new and/or revised scenarios will become available in time for 2020 mid-year data collections. The use of these scenarios in business processes and planning will also be reviewed.

- Playback packs are being prepared based on 2019 RDS cyber scenarios, for distribution in Q4 2019. These will contain exhibits to help managing agents assess performance against their peers. Lloyd's will collate feedback to enhance the packs for future data returns.

- A review will be undertaken of the use of existing cyber exposure data standards and how exposure data is being captured in policy systems.

- Lloyd's will continue to engage with vendors of cyber exposure management tools, keep up to date with developments, and will monitor the use of these tools in the market with a view to develop best practice and validation guidelines.

Underwriting best practice

- Earlier in 2019, a sample of syndicates was reviewed to assess how affirmative and non-affirmative cyber exposure in their property and energy lines of business was being assessed. The review focused on coverage, evaluation, pricing, strategy, appetite, and cyber expertise, as well as establishing compliance with the PRA Supervisory Statement SS4/17. The results of this exercise include a set of measurable recommendations that will form part of future Lloyd's Minimum Standards assessments. A Lloyd's market insight report providing further detail will be produced and distributed in Q4 2019.

Coverage and exclusions

- Underwriters, Lloyd's and the PRA[9] all agree that losses due to a cyber event could be seen in most lines of business. In February 2019 the Performance Management Division (PMD) consulted the market, with the assistance of the LMA, to obtain its views on Lloyd's intention to mandate the removal of non-affirmative cyber risk on all lines of business. Feedback supported implementing the requirements through a phased approach. In July 2019, Lloyd's issued Market Bulletin Y5258 mandating clarity of cyber cover in all lines of business. Phase 1 of this intitiative will address clarity in first-party property damage and is effective for new business and renewals from 1st January 2020. Further details for other lines will be advised during 2020.

- Lloyd's is working with the market to clarify rules surrounding the reporting of aggregations where the war and terrorism exclusion is amended, relating to cyber exposures.

- Lloyd's will work with the LMA and market experts to assist managing agents in understanding all facets of

[9] 'Dear CEO' letter from Anna Sweeney, Director, Insurance Supervision, PRA dated 30th January 2019

cyber risk, including current exposures and coverage across all lines of business.

Research and development

- Building on the reports produced over the past four years, Lloyd's will continue to commission industry and class-specific work to raise awareness of potential sources of cyber risk and losses. Work on the following report is already underway:

    - 'Project Turbulence' – cyber-related risks in the aviation industry, produced in collaboration with Xcyber and SIS Risk Management, to be released Q1 2020.

In conclusion...

The reason for this work is to ensure Lloyd's continues to provide the best cyber risk products and services for its customers, as well as ensuring that all those that offer cyber insurance through the Lloyd's market understand the risk well enough to be capitally resilient and able to pay claims.

As previously stated, Lloyd's is committed to delivering this strategy with the market, working alongside the LMA. Lloyd's will continue to work with the PRA to ensure cyber risk related activity undertaken is aligned, considered and proportionate. This allows us to support underwriting where the insured risks are both controlled and understood.

Updates will be provided to ensure the market is kept informed of the outcomes of the various workstreams and initiatives outlined in this report.

We will review progress, aims and interim deliverables of this strategy in Q3 2022.

Appendices

Appendix 1 – Details of Lloyd's Market Insight (LMI) reports[10]

- Cyber Risk Cover, Physical Damage (Dec 2016) – outlines the increased likelihood of physical damage arising from a cyber-attack, and ways to better understand and mitigate the risk
- Monitoring of Cyber-Attack Risks (Feb 2017) – highlights best practice for monitoring cyber risks at board level
- Cyber-attack survey results and other cyber oversight feedback (Jun 2018) – summarises the findings and evidence of good practice observed in the Lloyd's market through cyber oversight work undertaken during 2017
- Cyber Underwriting: A good practice guide (Feb 2019) – contains continued guidance on good practice following a thematic review exercise

Appendix 2 – Details of innovation reports

- Counting the cost: Cyber exposure decoded (Jul 2017) – in partnership with Cyence, the report provides insurers who write cyber coverage with realistic and plausible scenarios to help quantify cyber risk aggregation
- Cloud Down: Impacts on the US economy (Feb 2018) – in partnership with AIR, the study analyses cloud service provider failure risk, highlighting the expected financial impact of such an event in the US
- Bashe Attack: Global Infection by Contagious Malware (Jan 2019) – a report published as part of the Cyber Risk Management (CyRiM) project led by NTU-IRFRC in collaboration with industry partners (including Lloyd's) and academic experts (including Cambridge Centre for Risk Studies). The study explores the economic and insurance implications of a global ransomware cyber attack
- Lloyd's Digitalisation Series (Oct 2018 - Apr 2019) - four reports covering new technologies (IoT, virtual reality, AI and robotics) and exploring cyber-related risks using sectoral scenarios
- Shen Attack: Cyber risk in Asia Pacific ports (Oct 2019) – a second report published as part of the Cyber Risk Management (CyRiM) project, in conjunction with Cambridge Centre for Risk Studies. The study explores the economic and insurance losses arising from a cyber-attack on port management systems in the Asia Pacific region.

[10] Requires a lloyds.com account, and only available to Lloyd's Managing Agents' employees