LLOYD'S AON

Placing the client at the heart of cyber insurance

Lloyd's Futureset Cyber Innovation Forum – run in partnership with Aon

Executive Summary, London
26 November 2024

Lloyd's Futureset

Foreword

John Neal
CEO
Lloyd's

As little as 15 years ago, it would have been impossible to imagine the role technology plays in our lives today. Whether it be grocery shopping, socialising, purchasing a property, driving a car or even finding a life partner, digital technology enables and underpins so many of our interactions. This is why cyber is the fastest growing class of business at Lloyd's, with over one-fifth of global cyber insurance placed here. But this rapid growth has carried us into unchartered territory for cyber risk, with the potential for systemic or 'domino-like' global impacts.

Events like the CrowdStrike outage have given society a taste of what is possible. This is why we partnered with Aon to stage this forum and to explore how we can build innovative and tailored solutions as we adapt and respond to the evolving cyber risk landscape. The forum is also an opportunity to put our customers right at the heart of this conversation and hear about their unique challenges and experiences.

Tracy-Lee Kus
CEO
Global Broking Centre, Aon

Cyber resilience is no longer optional. For businesses, governments and society at large, it is essential. We have learned this lesson the hard way – through a litany of events including the WannaCry ransomware attack, the SolarWinds supply chain breach, and the disruption of the Colonial Pipeline. Incidents like these have taught us just how quickly and devastatingly these risks can escalate, with consequences that ripple across borders and industries. This is why Aon is committed to the innovation and collaboration necessary to creating cutting-edge solutions that help clients better understand, quantify and manage their cyber risks.

My gratitude to John Neal and the Lloyd's team for bringing this forum to life. Lloyd's has always been at the forefront of tackling emerging risks. Together, we are addressing one of the defining challenges of our era.

The threat landscape

The evolution of cyber threats is occurring at an unprecedented pace, with their impacts extending beyond traditionally vulnerable sectors. The increasing digitisation and connectivity of essential services, such as healthcare, energy, transportation and telecommunications means these sectors are increasingly exposed to both malicious and non-malicious cyber incidents.

This ongoing development has transformed cyber risks from a digital risk squarely in the domain of IT and security teams to a Boardroom priority. For the Lloyd's market, this is a challenge that demands a thoughtful and robust response.

Confronted by an ever-changing landscape, businesses find themselves in what is understandably an unfamiliar world. While 20 years ago a medium-sized company could realistically hope to avoid the attention of hackers, now automated attacks probing every internet-facing aspect of a business's operations mean that any vulnerability can be seen and exploited. This ever-present threat compels businesses to invest in their security and resources to maintain cyber defences and improve their cyber resilience. As a result, many have grown highly proficient in securing their digital infrastructure, but the distraction is both unhelpful and unwanted.

What is clear is that businesses are neither defenceless nor passive in the face of cyber threats. The Lloyd's market has a wealth of experience to help customers pragmatically respond to cyber challenges. Insurance has a broader role to play than simply paying claims. Having supported clients through thousands of cyber events, working alongside cyber security experts, those who operate in the Lloyd's market have developed an in-depth knowledge of how to prepare for and manage a cyber-attack. Against this backdrop, Lloyd's and leading international broker Aon convened the market's second Cyber Innovation Forum, bringing together customers, insurers and cyber experts to address a fundamental question:

How can we put the customer at the heart of cyber insurance?

The event's moderator, technology author, broadcaster and researcher Dr Stephanie Hare, opened with the message that combining industry-specific expertise and insurance know-how would lead to greater resilience and new solutions. "Cyber risk has rapidly become one of the most urgent challenges of our time," she observed. "Gaining a greater understanding that risk and its interplay with today's geopolitical landscape will be a positive step towards the resilience society needs."

Cyber, an evolving threat

Unlike what might be described as ‘traditional’ business risks – like fire, flood, or theft – cyber threats are rapidly evolving and adapting to both technological advances and the tactics adopted by cyber defenders. In short, cyber threats are getting smarter. This restless adaptation means that businesses must always be alert to potential new attack vectors.

The first session at the forum began with a question directed at the audience: what is the most common cyber threat we face today? Ransomware, social engineering and phishing were all prominent responses, but data and modelling limitations also hint at risk and exposure management challenges.

The theme of change and adaptation was explored by Dr Melanie Garson, Cyber and Tech Geopolitics Lead with the Tony Blair Institute for Global Change; “We are about to enter an age of upheaval,” she told the audience. “We’re seeing the convergence of the digital and physical in the way geopolitics actors are evolving.”

Dr Garson explained how threat actors are increasingly using digital attacks to disable physical capabilities by targeting connectivity infrastructure including undersea cables, telecoms networks and GPS systems. She noted that this ‘blurring’ of the physical and the digital can also be seen though the impacts of natural perils, such as the disruption caused by recent solar storms on critical GPS navigation systems used by modern tractors. This failure occurred during a critical point of the corn planting season, threatening crop yields and causing a sharp spike in corn prices.

As highlighted in a recent report from Lloyd’s Futureset, Generative AI: Transforming the Cyber Landscape, the proliferation and reduced costs of advanced Generative AI models has raised debate amongst cyber experts about its potential to aid both threat actors and defences. Darktrace’s Head of Threat Analysis Toby Lewis was measured in his assessment of AI’s capabilities.

He felt it was more realistic that AI might be used to “turbocharge” small parts of a cyber-attack rather than mastermind the entire process.

This includes AI’s ability to enhance social engineering attacks, a concern highlighted by the audience in the opening poll, to target individual members of staff, informed by their social media profiles and other online data. Lewis noted that there had been a three-fold improvement in the linguistic quality of phishing emails since ChatGPT’s rise to prominence, and that observations of the IP addresses of known bad actors indicate they are using these emerging models.

> “Resilience is like going up on an escalator instead of in an elevator. If an elevator stops, you’re stuck, but if an escalator stops, you can keep walking up.”
>
> *Dr Melanie Garson*
> *Cyber and Tech Geopolitics Lead*
> *Tony Blair Institute for Global Change*

The need for businesses to build resilience and contingencies into their operations and crisis plans was a closing thought. Faced with the very real prospect of cyber threats disrupting activities, designing processes and protocols that either failover or have non-digital alternatives was sound planning, the panel agreed.

Insurance as a strategic enabler

Cyber insurance has been available since the late 1990s and has evolved dramatically over the decades since to offer a broad ecosystem of support for businesses at their time of greatest need. This session focused on the nature of that support and how the quality of the relationship between a client, its broker and its insurer can positively impact the outcome of a cyber incident.

Aon's Global Chief Claims Officer Mona Barnes opened by noting that 59% of mid-market businesses had experienced a cyber-attack during 2023, according to the UK's Cyber Security Breaches Survey, with education, healthcare and the military the most frequently targeted industries. Overall, cyber-attacks had increased by 30%, she said, with the largest number targeting African and South American organisations. This chimes with recent reports suggesting that hackers are using less developed economies as testing grounds for new methods of attack.

Transparent and open communication between businesses and their insurers is one way to address this challenge. Beazley's International Cyber Claims Lead Sandra Cole felt this was of paramount importance. She recounted incidents in which customers had failed to notify insurers of a breach, thus creating delays while attacks escalated. She emphasised that insurers' immediate priority during an ongoing incident is to help stabilise the crisis.

One valuable piece of advice emerging from the debate was for customers to get to know their brokers' and insurers' claims team prior to any attack. Having managed a huge number of cyber events over the years, insurers have amassed considerable expertise that can be of value to the client, saving time and resources, with Cole noting that "a policy provides money, expertise provides value".

> "Insurers have significant experience in this area. You've had one attack, we've seen hundreds. You're buying that experience, that intelligence, sharing that information. Get to know your broking and insurer claims teams. You don't want the first time you speak to your insurer to be when an attack happens."
>
> *Sandra Cole*
> *International Cyber Claims Lead*
> *Beazley*

Another focus for the discussion was supply chain risk, as exposed in the recent CrowdStrike and Blue Yonder events. Baker Tilly Principal Ben Hobby felt that businesses should pay greater attention to the potential effects of an attack on a critical supplier that could leave them unable to operate. "Do you have the right to audit your suppliers' IT systems? is an important question to ask yourself," Hobby added, highlighting the importance of businesses asking 'hard questions' of their suppliers and examining their supplier contracts in forensic detail.

Cyber insurance products are on a maturity journey. The panel agreed that tremendous progress has already been made and the scope of cover available is broadening, with the greatest leap being the insurance industry's ability to advise and offer practical assistance to clients.

The potential impact of cyber on critical infrastructure

Critical infrastructure is defined as those national assets essential for the functioning of society. Chief among these are energy supply, water supply, transportation, healthcare and telecommunications. Businesses in these sectors face very specific challenges as criminals and bad actors pose what the UK's National Cyber Security Centre (NCSC) calls an 'enduring and significant' threat.

The potential for cyber attacks to cause physical impacts is highly pertinent to critical infrastructure. Brit's Head of Global Cyber, Privacy and Technology Ben Maidment spoke of the need for businesses to address potential protection gaps around this risk. Traditionally, physical damage has been the domain of property insurance policies but the evolution of cyber perils is shifting this approach. "This needs input from both sides of the underwriting fence to work," Maidment said. "Physical damage resulting from cyber is a less developed part of the insurance market, which is why it benefits from the Lloyd's market's consortium approach."

> "We're one of the most attacked companies out there... and we identify 2,000 potential attacks every second."
>
> *Paul Rogers*
> *Head of Pensions and Risk*
> *BT Group*

Another area of interest to the panel was the role that governments play – or could play - in enabling a more effective response to cyber threats. The harmonisation of regulation internationally was one example highlighted by the panel. "Reporting claims in Europe is very complex," Airbus Head of Cyber Insurance Management Philippe Cotelle explained. "We have country-specific rules as well as European rules. Simplification and increased efficiency should be promoted in cooperation with the authorities."

Intangible risks were also high on the panel's agenda. Philippe Cotelle felt that cyber insurance products needed to evolve to address the true value of a business's data. With the development of Artificial Intelligence applications, he urged that a more effective way of valuing the corruption or loss of vital data is needed. In a similar vein, BT Group's Pensions and Insurance Director Paul Rogers noted that a high profile cyber-attack on an organisation could result in customer losses.

Most importantly, the panel stressed that a one-size-fits-all approach to designing insurance products is not appropriate. Aon's Head of Cyber Broking UK Alistair Clarke felt cyber risks were well suited to Lloyd's ability to innovate, syndicate risk and build meaningful capacity for insureds.

While the debate recognised the scale of the challenge, there was cause for optimism. By recognising that a collective threat requires a collective solution, businesses and the insurance industry can mount a robust defence of their physical, digital and intangible assets. This effort would be underpinned by what Lloyd's Chief Underwriting Officer Rachel Turk described as a willingness on the part of clients and the insurance market to engage and share knowledge and experience. This, she said, would ensure that insurers develop products that customers want to buy, and ultimately strengthen the sector's long-term resilience.

Thank you to our speakers

John Neal
CEO
Lloyd's

Tracy-Lee Kus
CEO
Global Broking Centre,
Aon

Dr Stephanie Hare
Technology researcher,
broadcaster & author

Dr Melanie Garson
Cyber and Tech
Geopolitics Lead
The Tony Blair Institute
for Global Change

Toby Lewis
Head of Threat Analysis
Darktrace

Mona Barnes
Global Chief Claims Officer
Aon

Sandra Cole
International Cyber
Claims Lead
Beazley

Ben Hobby
Principal
Baker Tilly

Alistair Clarke
Head of Cyber
Broking UK
Aon

Philippe Cotelle
Head of Cyber
Insurance Management
Airbus

Paul Rogers
BT Group
Pensions and
Insurance Director

Rachel Turk
Chief Underwriting Officer
Lloyd's

Ben Maidment
Head of Global Cyber
Privacy & Technology,
Brit

Building societal resilience through research, insight and education

Futureset is Lloyd's global research platform and community designed to share risk insight and convene expertise to address some of the world's most challenging problems.

The platform is a catalyst for action and utilises cutting-edge risk research (like its recent Systemic risk series), events, insight and access to leading experts to spark innovation, build understanding and drive forward resilient solutions.

Contact the Lloyd's Futureset team should you have any questions about the content in the report.
futureset@lloyds.com

Instagram Lloyds of London
LinkedIn Lloyds of London
YouTube Lloyd's Insurance