

Lloyd's Cyber Summit

A critical threat:
The case for tackling
cyber risk today

**Executive Summary, London
1 November 2022**

Introduction

Cyber is one of the most complex and critical risks threatening national security and businesses today. Tackling this ever-evolving threat requires continued action, collaboration, and an agile approach.

This unique summit saw senior business leaders, policy makers and cyber risk specialists discuss creative solutions for this emerging and interconnected threat.

For cyber criminals, one of the clearest lines of attack is lying right in your pocket. Lord Sedwill, the former Cabinet Secretary and National Security Adviser, told the Lloyd's Cyber Summit that our mobile devices are one of the main "touchpoints for cyber risk".

Yet smartphones and watches are far from the only threat to our cyber safety. The cost-of-living crisis has created fertile territory for criminal activity to flourish, with the number of attacks by company insiders rising.

On the horizon, there's a looming threat of AI algorithms being harnessed for nefarious ends and quantum computers will sooner or later be able to break today's encryption software in a matter of seconds.

"Lloyd's Cyber Summit was borne from a compelling need to gather the experts and trusted actors from across government, industry, capital providers, security agencies and the insurance market to address the current and future threats of Cyber.

The responsibility for tackling the cyber challenge can't fall to the industry alone; it's important that as a collective we collaborate, educate, and intelligently create awareness of the risks associated with cyber.

The work at Lloyd's doesn't stop here. Our market share, expertise and unique syndication model means our whole market is not only focused on, but also best placed, to mature the class of cyber insurance and ensure a more resilient tomorrow."

Patrick Tiernan, Chief of Markets, Lloyd's

All this leaves companies and consumers exposed to a worrying amount of risk. We know it's crucial to work in partnership to expand the insurance market with simple and affordable products. As Patrick Tiernan, Lloyd's Chief of Markets, told delegates, greater penetration of cyber insurance will create a virtuous circle. As underwriters gather more data on cyber risk, prices will fall, driving higher demand.

- 01** Cyber has been the fastest growing class of business at Lloyd's in the last two years.
- 02** Lloyd's predicts the cyber market is going to treble in size from £12bn in 2022 to £35bn by 2030.
- 03** The global economic losses due to cyber-crime per year are estimated to rise to \$10.5 trillion by 2025.



Who are the threat actors challenging our cyber resilience?

With global economic losses from cyber-crime estimated to rise to \$10.5 trillion by 2025¹, in this session cyber-intelligence leaders shared their views on the criminals behind this rapidly increasing cyber threat.

From nation states to criminal groups, to rogue individuals, US intelligence veteran Rhea Siers, warned against damaging misconceptions that there is a hierarchy in each group's capability. "Everyone is getting better, and our response has to match this, we cannot be complacent."

Chris Painter, an expert in cyber diplomacy, said "a broader array of actors are targeting cyberspace than in the past". He noted that the lines had blurred between the malevolent actors and it was now difficult to distinguish between transnational criminal groups and government hackers.

Painter believes the motivations behind attacks can help attribute responsibility for individual attacks. "Nation states want access to intellectual property for intelligence purposes, while criminals are incentivised by money and they desire exposure", said Painter.



1. According to a 2020 report from Cybersecurity Ventures

Laurie Mercer, Security Architect at HackerOne, singled out a "young, motivated" group, typically between 16- and 25-years-old, as some of the "most interested actors in this space".

Following the pandemic and Ukraine-Russia conflict, James Stokley, CEO of Morpheus Risk, said security of supply chains has become a "big issue" both in the physical and online worlds. "Networks are only as strong as the weakest link," he said.

"What's changed and developed is the aggressive nature of the attack. The pandemic forced many traditional criminals online and while many are using ransomware clumsily, they're getting better."

James Stokley, CEO, Morpheus Risk



Rhea Siers, who chaired the session, advised that sound cyber hygiene needs to be married with "supply chain diligence" to respond to the global, interconnected and complex threats that the corporate world faces.

Companies should first identify their "crown jewel" assets before drawing up plans to protect them. "Whilst most people don't care where the attack has come from and they just want to recover from it quickly, understanding who is behind the targeting can help with resolution", according to Siers.



What are the critical cyber-threats looming on the horizon?

In this session, a series of leaders from the worlds of business, academia, national security, and insurance, set out the key trends challenging global cyber resilience in 2022 and beyond.

Paul Bantick, Head of Global Cyber and Technology at Beazley, highlighted the increased threat from insider attacks which have risen this year as employees turn to cyber-crime due to the cost-of-living crisis. "People are willing to do things they would not have two years ago," he said.

Insiders are only one of four main threats to resilience according to Bantick. He warned that activism is growing and that artificial intelligence, if used malevolently, could unleash the most serious cyber-attacks we have yet seen. Russian criminal gangs are also returning to the fray.

"As a result, companies will need to spend more on protecting and insuring their networks, driving up overheads," he said.

Siân John, Chief Security Advisor at Microsoft, said cyber hygiene is more important than ever, as the pace of digital transformation accelerates, and that businesses should prioritise multi-factor authentication and good data governance. She said "80% of cyberattacks would have been stopped by doing the basics well."

Dr. Bhavani Thuraisingham, a leading cyber academic from the University of Texas in Dallas, outlined three critical challenges looming on the horizon; malware that can adapt in seconds, machine learning and quantum computing, which has the ability to break all encryption software instantaneously.

To counter these challenges, machine learning algorithms will need to adapt as quickly as malware changes. She said: "Trustworthy machine learning is a key requirement for us."

Lauren Van Wazer, Vice President, Global Public Policy at Akamai, said an aggregation of multiple threats will define our cyber future.

"In the next decade we'll experience more than a hundred years of technological change. We're in the midst of the fourth industrial revolution."

Lauren Van Wazer, Vice President, Global Public Policy, Akamai

She noted how Covid-19 significantly changed the cyber risk environment and how boards not just need to ask the right questions but conduct risk assessments and scenario plan to increase their resilience.

She argued that building cyber resilience must start at the bottom of organisations and that education and awareness would be crucial to increasing immunity.



"However much you're doing, it's not enough."

"It's not just about your organisation, it's about who you fund and who you're integrated with."

"You need to game your own company and find your vulnerabilities."

Sir Ciarán Devane, Chairperson, Irish Health Service Executive (HSE), speaking about the HSE's experience with a major cyber-attack in May 2021.

What collaboration is required to achieve cyber resilience?

Host Kevin Kajiwara called the final session “the key question we need to answer today” asking delegates to consider who is responsible for tackling this ever-evolving threat.

Ross Anderson, Professor of Security Engineering at the University of Cambridge, began by calling for a central effort, including a better equipped police force. “They’ve been grossly starved of resources and as a result, there are not enough bad guys getting caught. With ransomware, there have been many criminals acting with impunity and now it’s morphed into a huge industry”

Charlie McMurdie, former head of the National Cyber Crime Unit, argued that while the police had built up crucial capability in tackling cyber-crime, it was industry partnerships that are key to enabling the forces success.

“Cyber criminals are exceptionally collaborative, and we need to learn from that. We need to look at who is responsible for addressing the threat. The simple answer is we all are.”

Charlie McMurdie, Former head of National Cyber Crime Unit, Metropolitan Police

She said. “Industry owns the intelligence and that is why we need to work better together, to build our resilience.”

Munich Re’s Chief Underwriter in Cyber, Jürgen Reinhart, addressed the role of the insurance industry and whether cyber risk is uninsurable. “Munich Re decided to offer cyber insurance not because we thought it was easy to earn more money, but because we need to help manage the risk and to do that, we need to understand it. We will do that by covering it”, he said. He argued that it is then critical that any learnings are shared with industry.

Patrick Tiernan, Chief of Markets at Lloyd’s, called for faster action. “Cyber is such a clear and present danger. We need to work together across the board to bridge the protection gap. If 71% of people have experienced an attack, only 9% of people have cover,” he said. “Let’s think in a pre-war mentality and do that work now.”

With a consensus that greater collaboration is required, the panel discussed how to drive engagement across business and government. “We need to speak in plain English about the level of the threat,” Tiernan said. “Alongside making a compelling case for economic action. The risk we’re talking about, if they’re on the wrong balance sheet, prevent growth.”

“There are many smaller companies who haven’t accepted cyber risk is relevant to them – more education is needed to show that cyber insurance is not an extra.”

Jürgen Reinhart, Chief Underwriter, Cyber, Munich Re



The role of Lloyd's in building cyber resilience

Cyber is a complex, real and imminent threat that we all face and which we all must play a role in tackling.

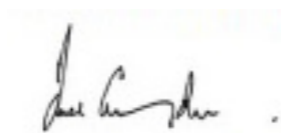
A key takeaway from our discussion at our Cyber Summit was the idea of society being a series of links – businesses, governments, consumers, employees – that together form a system; and a weakness in any one of those puts us all at risk. But collaboration across the system allows us to thrive.

At Lloyd's, we know that insurance is embedded across society so we need to keep pioneering new ideas and supporting the growth of cyber solutions while working in partnership with customers and governments to tackle this evolving and highly unpredictable threat.

We'll work with others for the solutions. But, here at Lloyd's, we will commit to:

1. Developing our modelling and scenario planning to give a clearer picture of potential outcomes; and importantly, linking those insights to the products we provide for customers so they're adequately covered and protected.
2. Convening the knowledge from across the intelligence and technology community that can ensure a more informed response. To support this, we'll be working in collaboration with the Lloyd's Market Association to drive engagement within the market on cyber best practice – and to boost awareness outside the market on the breadth and depth of expertise and solutions available within the Lloyd's market.
3. Putting ourselves in the customer's shoes: connecting businesses with the advice and technology that helps them build resilience, while developing and evolving cyber risk solutions aligned to their needs.

Supporting a cyber resilient society might seem like an impossible task – but if anyone has the expertise and ability to face that challenge, it is our market; in collaboration with policymakers, customers and all the stakeholders that collectively make up our ecosystem.



Bruce Carnegie-Brown, Chairman, Lloyd's



Thank you to our speakers



Sir Ciarán Devane
Chairperson, Irish Health Service Executive



Siân John MBE
Chief Security Advisor, Microsoft



Charlie McMurdie
Former head of National Cyber Crime Unit, Metropolitan Police



Ross Anderson
Chair of Foundation for Information Policy Research



Patrick Tiernan
Chief of Markets, Lloyd's



Robert Hannigan
Former Director, GCHQ



Chris Painter
Former Deputy Assistant Director, FBI Cyber Division, U.S. Department of Justice



James Stokley
CEO, Morpheus Risk



Laurie Mercer
Security Architect, HackerOne



Dr Bhavani Thuraisingham
Leading Cyber Security and Data Science Researcher



Lauren Van Wazer
Vice President, Global Public Policy, Akamai Technologies



Paul Bantick
Head of Global Cyber and Technology, Beazley



Tiago Henriques
Head of Research, Coalition



Kevin Kajiwara
Media commentator and Political and Risk Advisory Co-President, Teneo



Jürgen Reinhart
Chief underwriter, Cyber, MunichRe

