LLOYD'S

Illuminating cyber crime

Systemic risk scenario: Major cyber attack

The threat of a cyber attack is ever present. Even the best-protected organisations can be stopped in their tracks, falling victim to the crippling cascade of digital disruption.

To help you understand the most severe impacts of this threat and the steps you can take to improve your resilience, we've created a hypothetical but plausible scenario that describes a major cyber attack on global payments infrastructure and analysed the potential impact that this could have on the economy over the next five years.

Picture the scene: A cyber attack infiltrates global payment systems

Seconds – Malicious code is planted in critical software used by the financial services industry to confirm transactions and verify payments. The update is sent to tens of thousands of partner and customer networks, infiltrating them simultaneously

Days – A back door from the attack allows hackers to initiate a major breach. Customers cannot pay for goods and services, banks can't clear payments, and inter-bank lending grinds to a halt

Weeks – The hackers scramble the data now in their possession and divert funds to a network of accounts under their control

Months – Entire teams are distracted from daily responsibilities, trying to recover from the attack

Years – Beyond immediate costs, confidence in financial institutions is shaken, existing trade and customer relationships suffer, and regulations tighten to prevent future breaches

How severe could the situation get?

Our scenario explores three potential levels of severity, listed in the table below. Whilst these have been inspired by historical references, all three severity levels represent highly sophisticated and novel attacks which have never been seen.

Level	Scenario severity descriptions	Historical reference
Major (1 in 30-year probability)	Targeted attacks lead to an increase in the failure of key IT functionality, including business-critical operational systems within financial services, like major payment platforms. This is an **availability** attack.	**None – yet to occur**
Severe (1 in 200-year probability)	A ransomware attack with self-replicating encryption malware infects large volumes of hardware. Businesses systems and services become disabled for a long time, and they experience minor disruption, but have a massive and severe data breach. This attack includes **confidentiality** and **availability** factors.	**None – yet to occur**
Extreme (1 in 1,000-year probability)	A targeted ransomware attack significantly infects hardware. Businesses systems and services are disabled for a long time causing extreme disruption. Fundamental transaction data and backups are severely compromised, resulting in a lack of trust in primary data sources. This attack includes **confidentiality**, **availability** and **integrity** factors.	**None – yet to occur**

$3.5trn

Modelled global economic loss from a major cyber event

How vulnerable is the economy?

If this cyber attack was to take place, the global economic loss could reach **$3.5trn** over a five-year period (the average loss across the three severities we have modelled), with an expected economic loss (the conditional loss multiplied by the probability of the event occurring) of **$140bn**.

Which sectors might be most at risk?

Financial sector: The financial sector can be a lucrative target for attackers and is likely to be the most disrupted during and after an attack. However, cyber security maturity levels in financial services are typically high and the industry recognises the impact that any interruption would have on their brand.

Information technology (IT): If a cyber criminal is seeking access to multiple victims, then the IT sector is the ultimate access point, where interlinking technology systems and complex digital supply chains guarantee far-reaching effects.

Goods and services: Inconveniencing the general public and destabilising society are often tactics used by malicious actors to pressure institutions into paying ransoms to resolve a cyber attack.

What can businesses do?

For organisations at risk from cyber attacks, preparedness is key:

Be vigilant: From staff training to password policies, to regular software updates and key patches,every action you take improves your hand against cyber criminals. Investing in business continuity planning by considering contingencies,mapping network flows and operational dependencies is also a fundamental building block to preparing for the unavailability of technology.

Be clear: Transparency is vital. Early, clear reporting and a proactive approach to identifying breaches before an attack improves society's awareness and resilience as a whole – this is our collective responsibility.

Seek risk transfer: The insurance industry is 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.

Next steps

Work proactively to build resilience in your risk management against these threats and connect with your broker to discuss risk transfer for security, prevention and recovery from cyber attacks.

Find out more lloyds.com/futureset

Lloyd's Futureset