


Cyber attacks on payment systems – counting the cost

30 November 2023  Tim Johnson

< Previous

Baby boom and gloom: Uncertainty for the life insurance industry

Next >

Last month, [Lloyd's published its systemic risk scenario](#) detailing the potential global economic impact of a hypothetical cyber-attack on major financial services payment systems. **Fixed Recoverable Costs – controlling claims**

The model set out the three ways in which an attack can impact businesses:

1. data breach;
2. compromising data accuracy and validity; and
3. prevention of access.

Detailed in the scenario, through the use of code attackers are able to infiltrate networks, providing access to perform a major breach. As the discovery and repair of a breach can be a lengthy task, throughout this period the attackers are able to divert funds.

The model highlights that the United States of America, China and Japan are the countries likely to experience the highest economic loss. Loss of confidence in the institution and an increase in costs to tighten regulations and increase resilience were also highlighted in the scenario.

In building the scenario, Lloyd's and the Cambridge Centre for Risk Studies considered previous historic events such as:

- 2017 - Wannacry: A ransomware attack impacting Windows systems by encrypting contents and demanding a payment to decrypt. It was reported that the attack impacted 99 countries, with the NHS and companies such as Telefónica in Spain, Renault in France and FedEx in the USA being affected.
- 2017 - NotPetya: A malicious data encryption tool hidden in legitimate software that spread rapidly through trusted networks, therefore bypassing the processes in place to prevent ransomware. The attack was destructive, with the malware not being designed to be decrypted. [An assessment by the National Cyber Security Centre](#) found that the Russian military was 'almost certainly responsible'.
- 2022 - Albania DDoS attack: A destructive cyber-attack against the Albanian government that disrupted government websites and public services. The attack involved the deployment of ransomware followed by wiper malware. [Microsoft stated](#) with 'high confidence' that the attack was carried out by actors sponsored by the Iranian government.

For further considerations for insurers in regards to cyber-attacks, please see our **CyberCube's Global Threat Outlook: The evolving threat of cyber operations** article in The Word's [September edition](#).

Contents

[The Word, November 2023](#)



[The road to automated vehicles - Automated Vehicles Bill](#)



[Baby boom and gloom: Uncertainty for the life insurance industry](#)



[Cyber attacks on payment systems – counting the cost](#)



[Fixed Recoverable Costs – controlling claims](#)



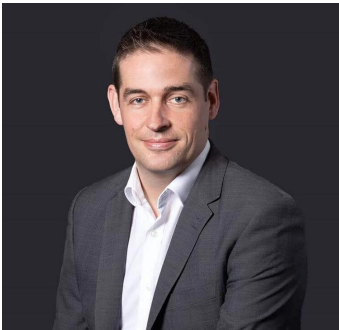
[PFAS exclusions updated](#)



[Artificial intelligence – How does AI think it can assist insurers?](#)



Key contact



Tim Johnson

Partner

tim.johnson@brownejacobson.com

+44 (0)115 976 6557

Related expertise

Coverage disputes and policy interpretation

Policy drafting and distribution