Technology Practice

Chubb Addresses Growing Cyber Risks with a Flexible and Sustainable Approach

The cyber insurance coverage section allows for policyholder flexibility regarding how much risk will be transfered and how much risk will be retained for Widespread Events, Ransomware Encounters and Neglected Software Vulnerabilities.

CHUBB®

Widespread events

The world is becoming more digitised and interconnected every year. Widely used software programmes, communication and technology platforms are leveraged and often relied upon by thousands or millions of companies. A single attack upon and/or failure of one of these widely used platforms or technologies could create an aggregation risk that exceeds the insurance industry's capacity to insure. In order to provide policyholders with coverage clarity and market stability, Chubb provides affirmative and specific limits, retentions, and coinsurance for such "Widespread Events."

Types of Widespread Event perils covered include:

Widespread Software Supply Chain Exploits
These are attacks that allow bad actors to enter systems through trusted, certified software and are effectively a Trojan horse to a system.

Real-world examples > Solorigate (2020), NotPetya (2017)

Widespread Severe Zero-Day Exploits
These are attacks arising from certain software vulnerabilities that are known by cyber criminals but not yet by anyone else – vulnerabilities that can be easily exploited, are severe, and often lack protection.

Real-world example > Hafnium (2021)

Widespread Severe Known Vulnerability Exploits
These are attacks arising from severe known software vulnerabilities that are not patched. The vulnerabilities are considered severe because they are easy to exploit, can be deployed remotely with limited access privileges, and can result in significant adverse impact.[1]

Real-world example > MSSP Attack (2021)

All Other Widespread Events
Certain types of cyber attacks can be carried out concurrently or automatically against a wide number of victims, ultimately causing a catastrophic cyber event. The Internet and some telecommunications services have risen to the level of critical societal infrastructure, and some large cloud computing firms are so widely used that an outage could impact the operations of thousands or even millions of companies.

Real-world example > Virginia Cloud Outage (2020)

1 NIST Security Vulnerability Trends in 2020: An Analysis (2021). Accessed at https://www.redscan.com/media/Redscan_NIST-Vulnerability-Analysis-2020_v1.0.pdf.

The Widespread Event language provides concise and sensible loss adjustment rules, including:

Incident response expenses do not erode Widespread Event limits until after it is determined that an incident is a Widespread Event, with no return of expenses incurred prior to that determination.

Policyholders can opt out of sharing certain types of investigatory data when it is mutually agreed that an incident is a Widespread Event.

To enable policyholders to purchase the coverage that best meets the needs of their organisation, all cyber incidents are categorised as either:

- Limited-Impact Events (e.g., a local event with "business as usual" loss rules); or
- Widespread Events (e.g., a systematic event with structural loss adjustment differences such as limit, retention, and coinsurance)

Ransomware

Ransomware attacks have grown dramatically in both frequency and severity. The loss implications to policyholders are far broader than just the value of the ransom amount. Whether the ransom is paid or not, policyholders often incur legal costs, forensic investigatory expenses, business interruption loss, digital data recovery costs, and, potentially, liability and legal defence costs.

The Ransomware coverage allows for tailoring of coverage limits, retention, and coinsurance for losses incurred as the result of a Ransomware.

Neglected Software Vulnerabilities

Keeping software up to date is an important aspect of good cyber risk hygiene. Many losses can be prevented by patching vulnerable software before cyber criminals have an opportunity to exploit it, but some organisations may not patch software right away. Sometimes there are legitimate reasons that software updates need to be tested before being rolled out, and compatibility, capacity, or simple logistics issues may prevent even a well-run information security organisation from deploying patches within the first day or week after they become available. For that reason, Chubb provides policyholders with a 45-day grace period to patch software vulnerabilities that are published as Common Vulnerabilities and Exposures (CVEs) within the National Vulnerability Database operated by the U.S. National Institute for Standards and Technology (NIST).

After the 45-day grace period expires, the Neglected Software Exploit risk is shared between the policyholder and insurer incrementally shifting to the policy holder, who takes on progressively more of the risk if the vulnerability is not patched at the 46-, 90-, 180-, and 365-day points.

For more information

Please visit chubb.com/uk/cyber

Chubb. Insured.℠

UK8124-MD 09/22