CHUBB®

Cyber Claims and Coverage Insights H1 2026

What we have bound lately

Recent cyber placements have continued to build steadily, reflecting the breadth and quality of business written across the portfolio. The latest bound accounts provide a useful view of where momentum has been strongest.

	Industry Class	Business Type	Revenue bracket	Country/Region	Limit
	Retail	Luxury Retail	US$1bn – 2bn	Singapore	USD$5m
	Manufacturer	Automobile Wholesalers	US$500m – 1bn	Philippines	US$3m
	Education	University	<US$100m	Malaysia	USD$1m
	Financial Institution	Credit Intermediation	US$2.5bn – 5bn	Vietnam	US$8.7m
	Professional Services	Computer Systems Design	<US$50m	Thailand	US$250k
	Real Estate	Lease Holder	<US$50m	Philippines	US$5m
	Social Club	Sports Club	<US$50m	Hong Kong	US$2m
	Transportation	Shipping/Logistics	US$500m – 1bn	Taiwan	US$3m
	Financial Institution	Asset Management	<US$100m	Hong Kong	US$2m

What we have paid lately

Chubb's Cyber Claims Specialists bring attentive, detail-focused expertise to every matter, drawing on insight into the trends and exposures shaping cyber risk. With experience managing claims across a wide range of industries, from public entities to retail, the team is well placed to respond when a cyber incident occurs and support clients through resolution with confidence and care.

Risk	Industry	Business	What was covered
Ransomware (The Gentleman)	General insurance	Commercial	Incident response expenses, ransom demand and expenses
Data breach	IT Services	Commercial	Defence costs
Ransomware (Bitlocker)	Professional Services	Commercial	Incident response expenses, legal costs and PR costs
Ransomware (Qilin)	Legal	Commercial	Incident response expenses
Data breach (Shiny Hunters)	Digital technology	Commercial	Defence costs
Ransomware (Dire Wolf)	Document processing and business communications	Commercial	Incident response expenses
US Class action	Sports Entertainment	Commercial	Class action settlement
Ransomware (Qilin)	Infrastructure / Transport	Private, not-for-profit	Legal and PR support
Cyber extortion (Shiny Hunters)	Financial Services	Commercial	Credit / ID monitoring
Unauthorised access	Automotive	Commercial	Incident response expenses
Ransomware (SEXI)	Education	Commercial	Legal support

What we have paid lately

Ransomware (The Gentleman)

A financially motivated group “the Gentlemen” accessed the Insured’s network and deployed ransomware. The Insured engaged IT Forensics to investigate and contain the incident. The investigation determined that the attacker likely gained access via the FortiGate SSL VPN using valid credentials and a firewall vulnerability, with Multi-Factor Authentication (MFA) not enabled at the time. After negotiation, the Insured paid a reduced ransom of US$100k. They also incurred costs for incident response, legal advice, forensic investigation, and recovery measures. The total claim exceeded the policy limit, and Chubb paid approximately US$185k for reasonable and necessary costs up to the limit.

Data breach (US Class action)

The insured was drawn into a US class action arising from a data breach in which it was alleged that the Insured had failed to implement adequate authentication and credential-security measures. This resulted in compromised credentials being used to access the school’s systems. Cover is available for Damages and Defence Costs arising from a claim first made during the Policy Period and Chubb has reimbursed more than US$128k of Defence Costs to date.

Ransomware (Bitlocker)

The Insured, which provides an extensive range of professional services, was unable to gain access to all their servers after they were encrypted by BitLocker tool. The Head of IT found a ransom note in the servers and contacted the threat actor using the email address provided. The threat actor claimed that more than 20 servers and over 160 laptops had been encrypted, and requested a ransom payment of $1.2 million. Chubb has reimbursed over US$90k for costs relating to incident response, public relations and legal fees.

Ransomware (Qilin)

An insured in the professional services industry discovered that a financially motivated ransomware group, Qilin, had gained access to its network and attempted to deploy ransomware. While the attempt to encrypt data on the Insured’s network was unsuccessful, the threat actor had placed ransom note text files on several systems, exfiltrated approximately 1TB of data, and demanded a substantial ransom. After several rounds of negotiations, the Insured paid a reduced ransom. Cover is available for incident response expenses and Chubb reimbursed the Insured for the ransom amount.

What we have paid lately

Data breach (Shiny Hunters)

A Delaware-incorporated digital technology services company provided technical support and network operations services to a school. This school offers a cloud-based student system used by schools across the US and holds Personally Identifiable Information (PII) data of millions of pupils. Threat actor Shiny Hunters gained unauthorised access to its system through a customer support portal, leading to the exfiltration of students' and teachers' PII. A US class action was filed by individuals and US School districts in the District Court of Southern District of California against the school, its owner and the Insured, alleging that the data breach resulted from an employee's compromised credentials. Chubb has reimbursed Defence Costs, and further costs are currently being incurred in defending the class action.

Ransomware (Dire Wolf)

A data handling service provider with customers ranging from banks, financial institutions, insurance companies, telecommunication companies and government agencies suffered a ransomware attack by the threat actor group, Dire Wolf. Three servers were encrypted and a ransom note was found in multiple folders in the Insured's systems. The threat actor exfiltrated data from the Insured's servers and threatened public release after 30 working days. A ransom of US$79.8k was paid by the Insured. A third-party claim was also made against the insured following the data breach. Chubb paid Incident Response Expenses, and Defence Costs are currently being incurred.

US Class Action

A global entertainment provider faced multiple claims from subscribers alleging violations of the Video Privacy Protection Act (VPPA) due to the unauthorised collection and disclosure of personal data through tracking technologies. The claims include class actions and a large-scale arbitration with plaintiffs seeking statutory damages and injunctive relief. Chubb has paid more than US$3m in damages to date and continue to indemnify defence costs in relation to the other ongoing claims.

Ransomware (Qilin)

A not-for-profit entity suffered a ransomware attack by Qilin, a Ransomware-as-a-Service group known for double extortion. The threat actor deployed ransomware and exfiltrated data from the entity's systems. Incident response and forensic support teams were engaged immediately to contain the threat, restore operations, and assess the extent of the breach. Cover is provided for the incident response expenses incurred, including legal and public relations costs.

What we have paid lately

Ransomware (Shiny Hunters)

A financial institution was targeted by ShinyHunters, a cybercriminal group known for large-scale data breaches and the sale and leakage of stolen data. The threat actor gained unauthorised access to the bank's network and exfiltrated 1.4TB of data, threatening to leak it unless a ransom of US$950k was paid. The local financial regulator requested daily updates and regular in-person meetings with the bank's appointed vendors, increasing costs in managing the incident. Chubb has paid more than US$600k in incident response, legal, forensic, and identity monitoring costs.

Unauthorised access

A conglomerate detected unauthorised access to a service account. It found suspicious activity traced to an overseas IP address, and customer reports that were generated by the unauthorised actor. Chubb paid more than US$5,200 in Emergency Incident Response Expenses incurred within the first 48 hours of the incident, and further expenses are currently being incurred in investigating and responding to it.

Hacking

A school discovered that four virtual servers containing personal data were encrypted by SEXI ransomware, deployed by the SEXI ransomware group, known for targeting large organisations and critical infrastructure. The affected servers were disconnected immediately, and the school promptly notified local police, the privacy regulator for personal data, and around 1,000 affected students and parents. Through Chubb's incident response platform, urgent technical support was provided to the Insured to help restore their IT systems and resume daily operations. We covered more than US$77k of costs incurred in IT forensic investigations, incident response, legal support as well as system recovery work.

Chubb's cyber insurance enables businesses to better manage and respond to cyber threats. Explore our cyber solutions and discover a wide selection of tools and services you can customise to fit your needs.

Get started today by browsing our offerings here: **www.chubb.com/hk-en/business/cyber.html**

CHUBB®

Published 08/2026.

chubb.com