Chubb Cyber ERM – Version 2.2 Ignite

Key Features

CHUBB®

Who does it protect?

Cyber Enterprise Risk Management protects organisations of any size against disasters such as loss of availability, data breaches, data corruption, ransomware and online media events covering both third-party liability and first-party losses from malicious acts or negligence.

It includes a wide range of cyber risk assessment, post-event crisis management and risk transfer solutions to address the growing cyber and data privacy risks facing companies today.

Why do your clients need this cover?

Increasing Costs

Data privacy breaches are costing businesses up to $3.6m per incident depending on the severity of the attack.

Increasing Threats

Even companies with strong security and privacy controls are not immune to cybercrime.

Chubb's own claims data shows that the number of our insureds who have had records exposed in the last 20 years totals over 500 million records.

Ransomware, one of the most common attacks, has seen a significant increase in frequency and severity losses since 2019.

What does it cover?

Incident Response: Chubb policyholders have access to our network of Incident Response Management firms around the world via a hotline, the Chubb Cyber Alert mobile application, or the Chubb Cyber Alert website. We support clients throughout an incident using a network of forensic, DDoS remediation, cyber extortion, legal, notification, fraud remediation and public relations experts. This service is available 24 hours a day, 365 days a year.

Third-party liability coverage protects the insured for liability resulting from the loss of personal and corporate confidential information. Some highlights include coverage for:

- Privacy – failure to protect records and data in print or digital format
- Conduit – transmission of a cyber attack
- Content – intellectual property infringement through mismanagement of data or media negligence
- Impaired access – restricting customer access to the insured's computer systems, e.g. websites, due to a system attack
- Reputation – defamation or privacy intrusion through cyber activity.

First-party coverage is designed to minimise the effects of a cyber event. Some highlights include coverage for:

- Privacy notification expenses
- Business interruption income loss
- Data recovery and restoration costs including increased costs of labour and equipment
- Cyber extortion damages and expenses
- Crisis management expenses following an incident, our policy responds with a number of vendors that specialise in coordinating an appropriate and timely response.

Extensions will include emergency incident response, betterment costs, cyber crime, reward expenses, and telecommunications fraud.

We offer protection against regulator actions for data privacy breaches where insurable by law. This includes cover for defence costs, regulatory fines and consumer redress payments.

Our team of risk engineers in the UK and Europe provides clients with risk engineering and loss mitigation services.

What is the limit?

Up to £3m for certain industries on an aggregate basis.

Main benefits of cover

Cover/services	Benefit
Emergency response expenses	48 hours for costs to use incident response management and IT forensics to investigate a suspected cyber incident.
Cyber crime	Sublimit for when funds are lost due to cyber crime when committed by external parties.
Betterment	Sublimit for betterment costs to improve your computer software following a cyber incident.
Modular, flexible approach to cover	Clients can choose insuring clauses and limits to suit their needs, including full limits on privacy notification and crisis management expenses where relevant.
Voluntary notification	Privacy notification cover can be triggered even if it's not compulsory to notify the authorities or affected persons.
Corporate information covered	Our definition of 'record' is not just limited to natural persons; it also includes confidential corporate information.
Regulatory actions, fines and penalties	Chubb policies provide comprehensive cover for regulatory fines (where the law allows), regulatory action defence costs and consumer redress payments.
Insider and outsider threats	Our policy is not restricted to third-party threats; insider breaches of security from 'rogue' employees may also be covered.
Credit monitoring costs	Chubb's privacy notification expenses provide credit monitoring services to help protect people against fraudulent use of their records.
Worldwide coverage	Our policies are worldwide to respond to the multinational nature of cyber risk.
Cyber extortion	We provide cover for the damages and costs associated with mitigating a cyber extortion incident, including some ransom payments where the law allows.
Incident response	Our incident response offer is a 24/7/365 hotline in local language. It is supported by a turn key incident response plan with global and local experts, while maintaining the client's right to choose vendors best suited to manage the event. Clients can report a claim via our cyber alert app, website or with a single call.

Main benefits of cover

Cover/services	Benefit
Business interruption loss	Includes loss of profits and extra expenses arising from a cyber incident.
Data and system recovery costs	Includes costs to recover data and systems following a cyber incident, as well as other costs to mitigate business interruption loss.
System failure	For IT admin operator error, or human error, that leads to a business interruption or data loss event, and for programming errors leading to a business interruption or data loss.
Crisis system outsourcing	Our cover also includes the cost of crisis system outsourcing following a denial of service attack.
Contractual penalties	We cover the contractual penalties or assessments arising from PCI DSS (the payment card industry data security standard), as well as the costs of retaining an approved PCI Forensics Investigator to determine loss.
Media liability	We provide cover for media liability arising from the insured's online presence, including social media websites under their control.
Contingent Business Interruption Loss	Includes many scenarios where a cyber incident impacts an outsourced IT service provider (eg. backup, cloud, hosting)

What's changing in Enterprise Risk Management Version 2.2 Policy Wording?

1. **Covered & Shared Computer System:**
   There is now a clear split between cyber incidents impacting the computer network controlled by the policyholders and cyber incidents impacting their IT providers.

2. **Ransomware:**
   The loss implications to policyholders are far broader than just the value of the ransom amount. The Ransomware section allows for tailoring of coverage limits, retention, and coinsurance for losses incurred as the result of a Ransomware incident.

3. **Neglected Software:**
   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 right away. 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).

   The Neglected Software Exploit Endorsement provides coverage after the 45-day grace period expires, with the risk-sharing between the policyholder and insurer incrementally shifting to the policyholder, who takes on progressively more of the risk if the vulnerability is not patched at the 46-, 90-, 180-, and 365-day points.

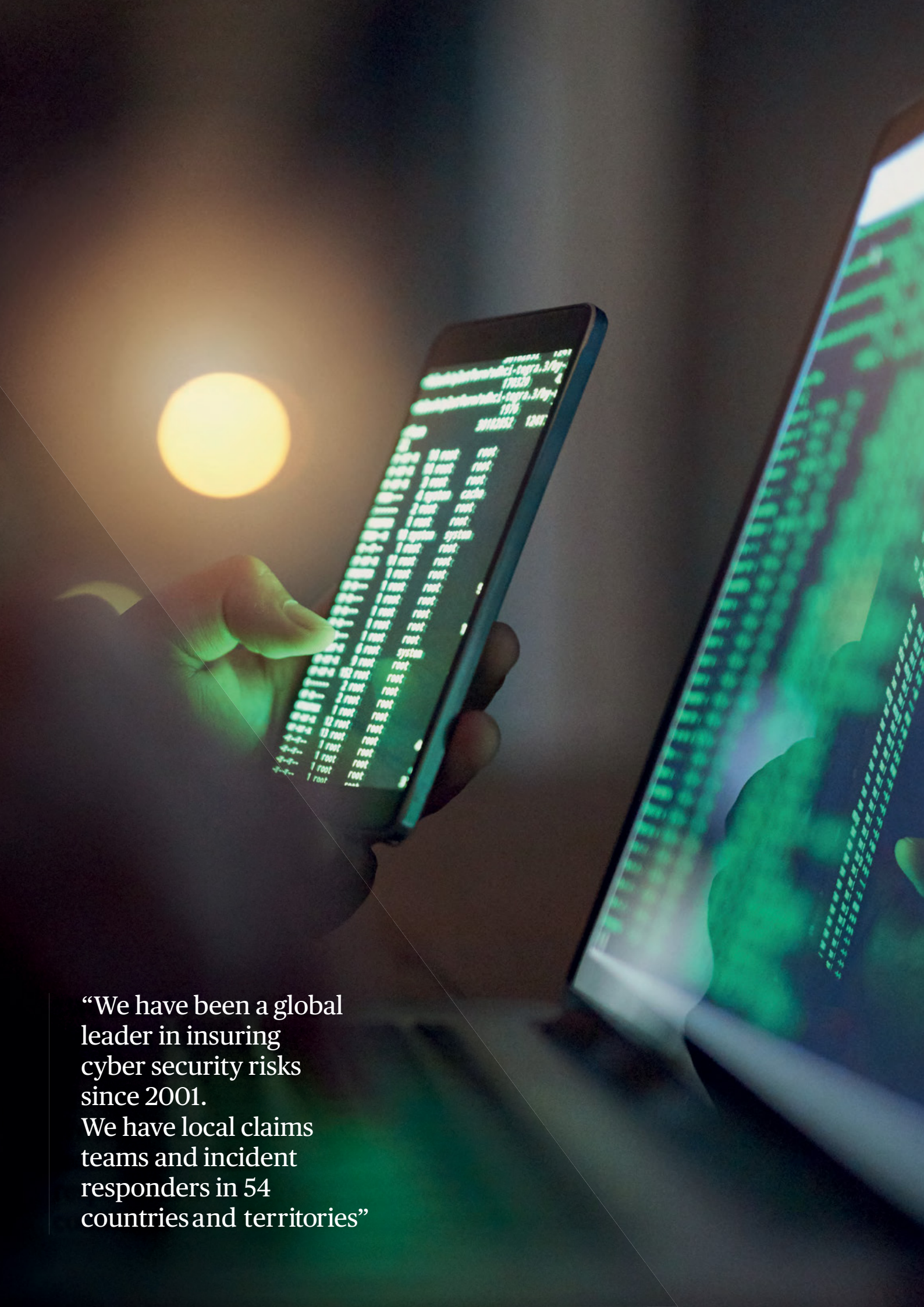
4. **Widespread Events:**
   The Widespread Event Endorsement provides concise and sensible loss adjustment rules, including:

   - Incident response expenses do not erode Widespread Event limits until after it is determined that an incident is a Widespread Event.
   - Policyholders can opt out of sharing certain types of investigatory data when it is mutually agreed that an incident is a Widespread Event.
   - Policyholders can purchase the coverage that best meet the needs of their organisation between limited impact events or widespread events

Watch our video to learn more >

5. **Updated Exclusions:** (Infrastructure, Government Actions, War, Specified US Laws, Professional Services)

   Standard exclusions have been updated in line with systemic risk trends and analysis.



"We have been a global leader in insuring cyber security risks since 2001.
We have local claims teams and incident responders in 54 countries and territories"

Our Appetite

We like to insure the following industries:

- Professional service and consultancy
- Manufacturing and construction
- Media
- Entertainment and hospitality
- Retail
- Wholesale operations
- Real estate

We are cautious of:

- Payment card processors
- Data aggregators/warehouses
- Payroll processing
- Online gaming
- Social networks
- Critical infrastructure
- Trading platforms

Why choose Chubb?

Specialist cyber risk expertise. We have been a global leader in insuring cyber security risks since 2001.

Global reach. Our policies provide worldwide coverage to respond to the ever changing, growing regulatory burdens. We have local claims teams and incident responders in 54 countries and territories, including dedicated cyber teams in key territories globally, meaning we can deliver consistent, high-quality services around the world.

Enterprise risk management. Our holistic approach to cover allows us to provide first party and third party protection as well as offering pre -bind cyber risk assessment, post-event crisis management and risk transfer solutions.

Additional cover
We have a wide range of financial lines products including:

- Crime insurance
- Directors and officers liability
- Pension scheme and benefit plan liability
- Corporate legal liability
- Kidnap, ransom & extortion expenses

This factsheet is intended for use by professional insurance brokers only.
It is for information purposes only, please see the policy document for full terms, conditions and exceptions.

Contact

To find out more please go to Chubb.com/uk

Chubb. Insured.℠

UK8194-MD 05/22