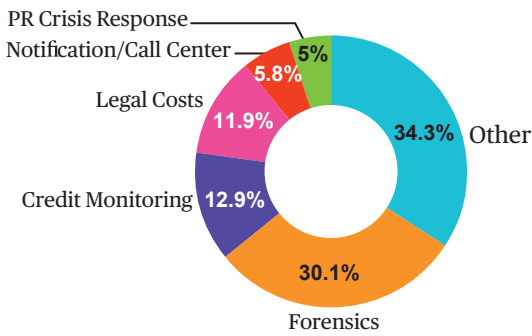


Commercial Cyber Policy Guide for Agents and Brokers

Total Cyber Claims Costs Since 2009

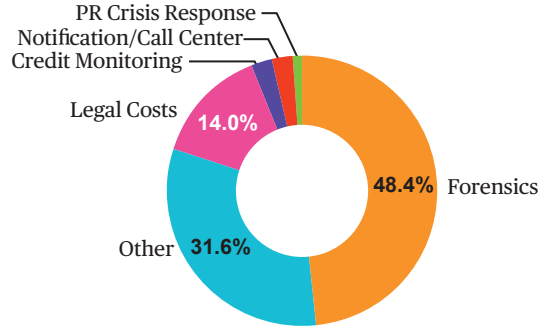
Global, and All Industries



The "Other" category may include several other types of losses, including business interruption loss, network extortion payments, PCI assessments, regulatory fines, and settlements of third-party matters.

Total Cyber Claims Costs - Last Three Complete Years

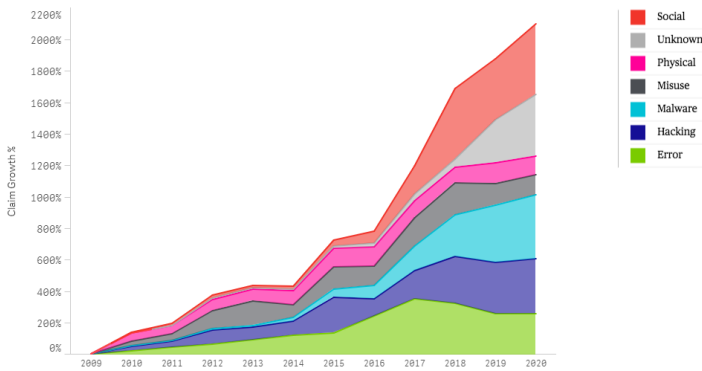
Global, and All Industries



Chubb Cyber Index™

Incident Activity Growth Compared to 2009, by Actions*

Global, and All Revenue Sizes



* The current year is a projection based on year-to-date claims as of the most recent update.

Access our proprietary global claims and policy data

Chubb has handled cyber claims for over two decades. As part of the claims process, we track key metrics such as actions causing a cyber loss, whether a cyber incident was caused by an internal or external actor, the number of impacted records, peer purchasing insights, and more.

Use our tools to see targeted data filtered by industry, company size, and region.

We analyze these metrics along with public trend data to help us continuously improve our business, provide insight to our broker and agent partners and policyholders, and help reduce exposures to future losses.

The Chubb Cyber Index is a free digital tool available to the public. To access, visit www.chubbcyberindex.com

Incident Response Services

The Chubb Cyber Incident Response Team is available 24/7/365 and offers a holistic approach to managing cyber incidents.

The Cyber Incident Response Team is comprised of a diverse group of experts in the legal, computer forensics, notification, call center, public relations, fraud consultation, credit monitoring, and identity-restoration services areas that help organizations limit exposure to a loss when a cyber incident occurs.

There is a \$0 retention on the Cyber Incident Response Coach (if terms are quoted as such).



If policyholders are experiencing a cyber incident, they can get immediate assistance from a Cyber Incident Response Coach:




- Call 1-800-817-2665
- Access the Chubb Cyber Alert® App on any mobile device
- Email cyberclaimreport@chubb.com

Already have a team of partners you know and trust? Your policy may allow you to continue to use them; all firms are subject to review and approval by Chubb.

Loss Mitigation Services

We provide cyber policyholders with access to tools and resources needed to address and gauge key areas of cyber security risks before an event occurs.

Some of the tools provided include:

-  Password defense, hygiene and monitoring tools for policyholders' employees (up to a certain number) from Dashlane
-  Online employee security training from Skillbridge (up to a certain number)
-  Access to our eRisk Hub

Signature Loss Mitigation Services

Cyber security education training, risk assessments, planning exercises, and other cyber loss mitigation services are available for cyber policyholders in certain regions. These consultative assessments are provided directly to your organization by a panel of Chubb pre-approved vendors at a pre-negotiated flat rate.

Policy-Wide Definitions

Protected Information – includes “...other non-public personal information as defined in any Privacy or Cyber Laws.” Therefore, there is no need to endorse specific regulations.

Cyber Incident – with respect to Cyber Incident Response Fund, includes “any actual or reasonably suspected failure by an Insured [...] to properly handle, manage, store, destroy, protect, use, or otherwise control ‘Protected Information.’”

Privacy or Cyber Laws – includes regulations that require the adoption of specific privacy or security controls, not just those that require the notification of individuals post-breach.

Insured’s Computer System – includes “computer hardware, software... mobile devices” that are “leased, owned, or operated by an Insured” to address telecommuting exposures.

General Terms and Conditions

- Non-cancellable, except for nonpayment of premium.
- No revenue or assets-based thresholds for newly acquired entities.
- Most favored jurisdiction applicability to punitive, exemplary, and multiplied damages.
- Notice requirements are provided on a “Claims-Made” basis, as opposed to a “Claims-Made and Reported” basis.
- Blanket waiver of subrogation wording.
- Defense and Settlement section provides for an 80/20 hammer clause.
- Exclusion for Bodily Injury contains “for” lead-in and contains an affirmative carveback for mental injuries resulting from an Incident.
- Rogue employee coverage.

First-Party Incident Response Coverage

- Cyber Incident Response Coach retention of \$0 (if terms are quoted as such).
- Limits available for Insured selection of “Non-Panel Response Providers.”
- Criminal Reward expense is included up to the full limit applicable to “Cyber Incident Response Expenses”
- Voluntary notification, with Insurer’s prior consent
- Credit monitoring services coverage applies as “required to comply with Privacy or Cyber Laws,” without a limitation of time (no cap of 12 or 24 months).

First-Party Business Interruption Coverages

- “Business Interruption Loss” and “Contingent Business Interruption Loss” (BI/CBI) include continuing normal operating and payroll expenses.
- “Interruption in Service” means a “detectable interruption or degradation in service...” without any further requirement that such interruption or degradation render the company incapable of supporting their normal business function.

First-Party Digital Data Recovery and Network Extortion Coverages

- “Telephone Fraud Financial Loss” is included up to the full limit applicable to “Digital Data Recovery Costs.”
- “Extortion Expenses” uses reasonable and necessary threshold for payment, rather than requiring the Insurer’s prior consent.
- Extortion Expenses definition extends to cryptocurrencies, including Bitcoin.
- Network Extortion Threat definition extends coverage to threats directed at an Insured through either the Insured’s Computer System or Shared Computer system, thus addressing cloud based extortion scenarios.

Other Cyber Third-Party Coverages

- Regulatory coverage includes Regulatory Proceedings, Regulatory Fines, and Consumer Redress Funds.
- “Payment Card Loss” includes monetary assessments, fines, penalties, chargebacks, reimbursements, and fraud recoveries, including card reissuance costs.

Chubb. Insured.SM