CHUBB®

Staying ahead of cyber risk.

Stack up your cyber protection with Chubb.

Contents

THE EVOLUTION OF CHUBB

Your cyber stack needs a strong foundation. Like global leader strong.

The globalisation and digitisation of business have created a highly interdependent economic environment — one that is full of risk.

Chubb has kept companies ahead of cyber risks for more than 25 years. Today, we are the global leader in cyber insurance[1] — a position earned by consistently innovating insurance coverage options and cyber risk management services to address evolving exposures. Our cyber claims specialists have handled more than 32,500 cyber claims globally and maintain close connections with best-in-class response specialists who assist policyholders in mitigating and managing cyber incidents.

Whether through definitions that contemplate the latest privacy and cyber laws, the discerning inclusion of insurance coverage enhancements, or the hand-selection of cyber risk services to mitigate risk, Chubb delivers what each client needs today — and tomorrow.

Our cyber claims specialists have handled more than **32,500 cyber claims**.

OUR HISTORY

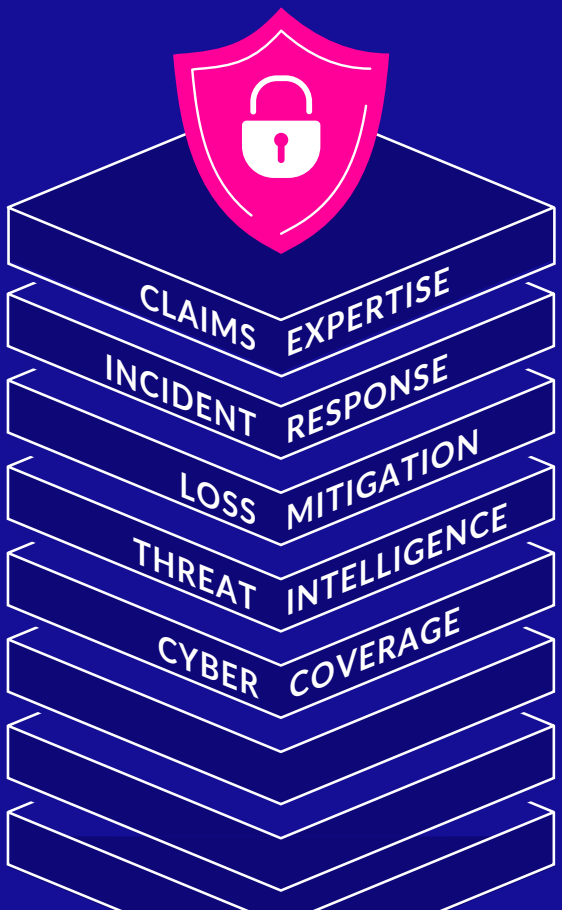
1998

Released our first cyber product.

2016

Launched Cyber ERM and the Technology Master Package, nearly 20 years after creating our original product.

Chubb is one of the leading providers of cyber insurance globally by gross written premium.[1]



5.4 Billion

internet users today compared to 2.6 billion 10 years ago.[2]

280,000+

registered Common Vulnerabilities and Exposures (CVEs) with **more than 100 being added every day.**[3]

Cyber insecurity

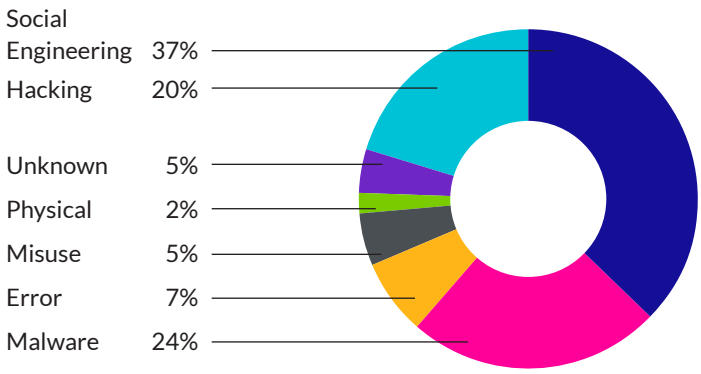
is ranked 4th out of 10 most concerning risks faced by society.[4]

When the odds are stacked against you, it's time to stack your deck.

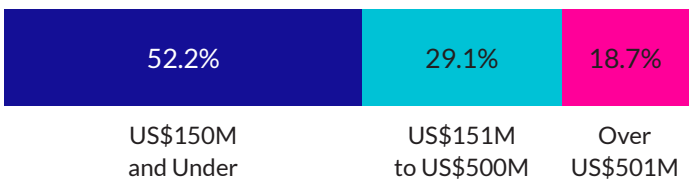
Cyber Claims Trends

Companies of all sizes are facing increasingly sophisticated social engineering attacks, which can lead to data breaches, debilitating ransomware events, and even reputational harm. Our **Cyber Index** has compiled an inventory of triggers leading to such cyber incidents and exemplifies why businesses should take advantage of Chubb Cyber Services, including the Chubb Cyber Stack for small businesses with 100 employees or less.

Actions Causing Cyber Incidents – Rolling 12 Months
USA, All Industries, Revenues Under US$150M



Percentage of Annual Claims by Annual Revenue since 2023



Chubb Cyber Index

Provides real-time access to Chubb's proprietary claims data and insight into current cyber threats, trends and costs. Users can set perimeters and view historical trends based on type of threat, size company and which industry the company operates within.

Accidents Happen:

According to the Verizon Data Breach Investigations Report (DBIR)[5]:

68% of breaches involved a non-malicious human element

28% involved errors

15% involved a 3rd party

The right cyber stack includes coverage for unintentional privacy violations, too.

Over the last two years, privacy-related claims have grown by 210%[6]

Not all cyber risk comes from hackers. As technology advances, regulations evolve as well. With operations in 50+ countries and one of the largest cyber underwriting teams in the world, we continually help our clients identify and manage the latest exposures, including coverage for privacy-related risks.

At Chubb, we not only help our clients identify and manage risks, but also offer comprehensive coverage that addresses a wide range of exposures. Our extensive insurance solutions are tailored to meet the unique needs of each business.

GDPR and BIPA

GDPR (the General Data Protection Regulation), came into force in 2018, governing the collection, use, storage and deletion of data. It's common for laws to exist which create a pathway for victims of privacy breaches to bring private actions for damages suffered, in some circumstances without having suffered any financial loss or evidence demonstrable damage.

Data categories such as Biometric information, remain in focus as a special category of data under GDPR, with consent often required for collection, use and handling of Biometric Information. For those companies who have US exposure, the Biometric Information Privacy Act (BIPA) enacted in 2008 in Illinois was the first to set an increasingly popular standard for private rights of action against organisations with fines for failure to comply.

Cookies, Web Beacons and Pixels

Cookies, web beacons and pixels are code used within websites to monitor the activity of users for customer profiling, targeted advertising, or data analytics. Consent to collect information via these tracking technologies is required, and failure to do so will breach the obligations under privacy regulations such as GDPR and PECR.

For policyholders with users in the US, we continue to see claims alleging privacy infringements under the Video Privacy Protection Act (1988). Across the globe we see lawsuits related to improper use of this technology or disclosure of video viewing habits becoming more common. These suits allege this activity disclosed personally identifiable information without the users' consent. This exposure is ubiquitous, and penalties can be severe.

Artificial Intelligence (AI)

While harnessing the full potential of AI remains a top priority for organisations around the world, effective AI regulation remains elusive — despite well-intentioned efforts by governments. Mitigating AI-related security risks has proven to be a process of trial and error. Whilst AI is embedded in some defensive security tooling, it is also weaponised by those wishing to cause harm.

Digital and Operational Resilience

Regulations for both digital and operational resilience continues to develop at pace. In the EU, we have seen the Digital Operations Resilience Act ("DORA") and NIS2 come into force in recent months. These regulations focus on the Financial Industry and Critical Infrastructure, with onerous reporting timeliness and potential fines for contravention.

LOSS MITIGATION SERVICES

Your business is too important to not have a strong cyber stack.

All ERM policyholders that purchase Cyber coverage have access to complimentary or discounted* loss prevention services that can help mitigate the most pressing exposures and reduce risk before a cyber incident happens.

The Chubb Cyber Services offering is a collection of services informed by Chubb's threat intelligence and claims experience:

1. **Cyber Incident Response**
   Creating, refining, or practicing a cyber incident response plan with all key stakeholders.

2. **Cyber Vulnerability Management**
   Identifying weaknesses in an organisation's network for proactive resolution of misconfigurations and vulnerabilities.

3. **Endpoint Security**
   Next generation anti-virus software and endpoint detection and response (EDR) capabilities that help stop cyber criminals from infiltrating an organisation's network.

4. **User Security & Awareness**
   Tools and training to help employees be the first line of defence.

5. **Privacy Risk**
   Manage consumer privacy risk and regulatory compliance across an enterprise's ecosystem.

Where allowed by law.

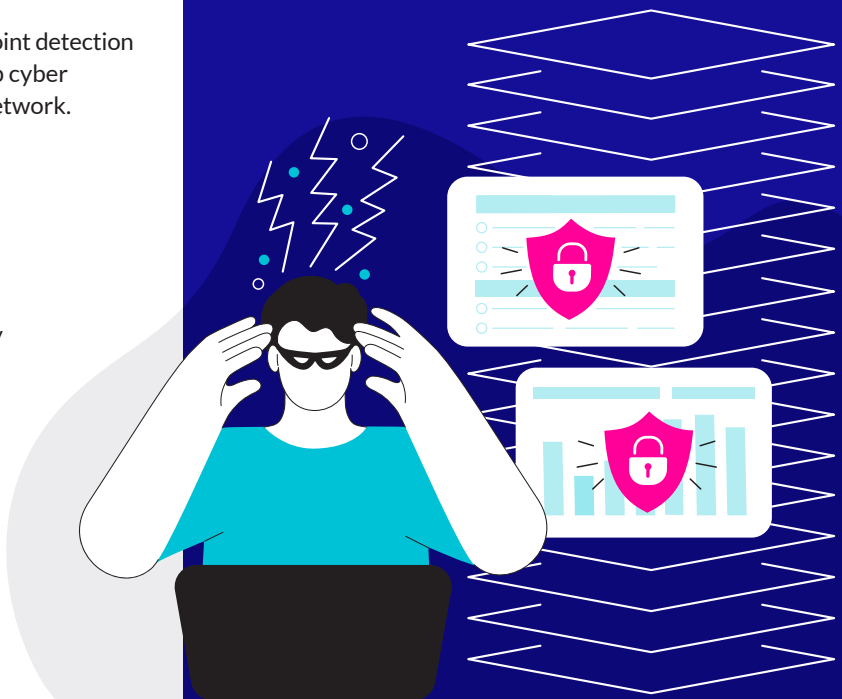
52%

of cybercrime targets are small- and medium-sized enterprises.[6]

COMPLIMENTARY CYBER PROTECTION FOR SMALL BUSINESSES

Chubb Cyber Stack

A curated **collection of services**, worth up to US$28,000 in annual savings, delivered by a network of trusted cybersecurity providers. Specifically designed for small businesses with 100 employees or less, these services are geared towards preventing cyber incidents and empowering effective cyber risk management and incident response.[7]



THREAT INTELLIGENCE & CYBER RISK ADVISORY TEAM

Dedicated cyber experts focused on stacking up your defences.

Vulnerability Management Outreach

Our Cyber Intelligence Team routinely monitors, scans, and identifies vulnerabilities and new critical threats to help safeguard our policyholders. Policyholders are informed by:

Outreach Program
Proactive notification to Cyber insureds and their brokers if known critical vulnerabilities with a high probability of exploitation are detected in their environment during their policy period.

Breaking Alerts
Sent to Cyber insureds and their brokers when new vulnerabilities with a high probability of exploitation are discovered and may impact their environment.

Cyber Risk Advisory Team
Our knowledgeable Cyber Risk Advisors are available to recommend the right services to minimise each policyholder's exposure and assist in integrating services into their risk management approach. Appointments can be scheduled on our **website**.

A good cyber stack doesn't just protect, it responds.

Incident Response Team

If a cyber incident does occur, our knowledgeable Incident Response Team is readily available to provide swift, efficient support. Our teams comprise experienced third-party service providers that provide legal, computer forensic, notification, call centre, public relations, crisis communications, fraud consultation, credit monitoring and identity restoration advice and services.

Chubb Cyber Alert℠

Our free Incident Response Mobile App swiftly connects policyholders 24/7/365 to a Chubb Incident Response Coach and enables them to submit photos to help in the assessment of the event, notify their broker and more.

Download the app now:

Download on the App Store

GET IT ON Google Play

The Chubb claims difference

Our experienced claims specialists understand that the handling of every claim is the most critical test of our service, our support and our reputation.

We provide expertise that is sensitive to our customers' cultures, markets and the diverse regulatory environments in which they operate.

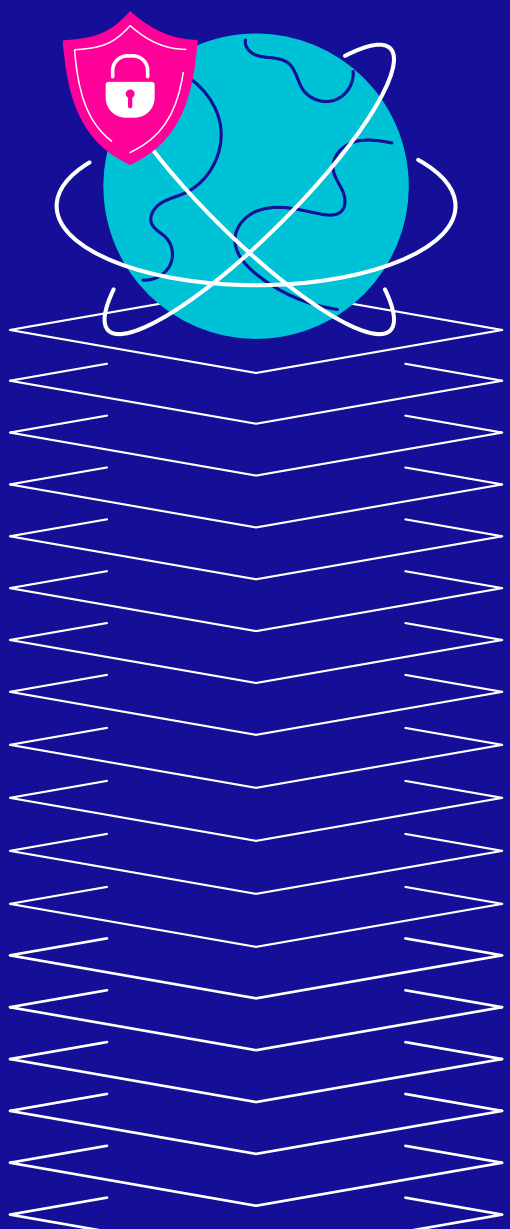
Flexibility when you need it most

Whether reporting an incident through the hotline or Cyber Alert App, you are empowered to decide if you want the incident tendered as a Claim to Chubb.

This team has handled more than

32,500 cyber claims

and is committed to helping you through yours.



CHUBB®

Endnotes

[1] Beinsure (https://beinsure.com/global-ranking-cyber-insurers)

[2] Forbes (www.forbes.com/home-improvement/internet/internet-statistics)

[3] NIST National Vulnerability Database (nvd.nist.gov/general/nvd-dashboard) (as of March 2025)

[4] World Economic Forum – Global Risks Perception Survey, 2024 (https://www.weforum.org/publications/global-risks-report-2024)

[5] Verizon Data Breach Investigations Report (www.verizon.com/business/resources/reports/dbir/)

[6] Chubb Cyber Index (chubbcyberindex.com)

[7] Terms and conditions are subject to change. The complimentary cost is a one-year period and is applicable only to policyholders who are net new subscribers/customers to the respective services. Furthermore, eligible policyholders must meet the size limitation of having 100 employees or less to qualify for select services.

Protect your business with Chubb.

To learn more about Chubb Cyber, please click or scan the QR code:

All Cyber services are subject to change. Any changes to the service offering will be reflected on the local Cyber services webform. Policyholders are responsible for reviewing specific terms and conditions of each cyber service provider to ensure eligibility and to stay updated on any changes that may occur.

Breach Response Plan Builder, External Vulnerability Monitoring, Supply Chain Risk Management, Secure Password Manager, Security Awareness Training, Cyber Risk Resource Library, Phishing Simulator, Identity Assessment are cyber services offered by third party vendors at no additional cost to Chubb policyholders for the stated initial period, provided the policyholder is a new subscriber/customer to the cyber services on offer by the chosen third-party vendor and the policyholder otherwise meets the stated eligibility requirements. After expiration of the stated initial period, policyholders may have the option to continue their cyber services at a discounted rate upon renewal. Please note that the specific discount may vary between products and services. Discounts on products and services offered by cyber services vendors are available only to Chubb policyholders with current in-force policies and are subject to applicable insurance laws. The products and services provided by third party vendors will be governed by contract terms the policyholder enters into with the third-party vendor. Chubb will not be involved in the policyholder's decision to purchase services and has no responsibility for products or services that are provided by any third-party vendor.