

CHUBB®

Staying ahead of cyber risk.



Stack up your cyber
protection with Chubb.

Contents

The Evolution of Chubb	P3
Cyber Risk Landscape	P4
Current Trends	P5
Pressing Privacy Issues & More	P6
Loss Mitigation Services	P7
Threat Intelligence & Cyber Risk Advisory Team	P8
Incident Response Team & Claims	P9

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 insurance¹ — 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 globally.**

OUR HISTORY

1998

Released our first cyber product.

2016

Launched Cyber ERM and PremierTech, 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

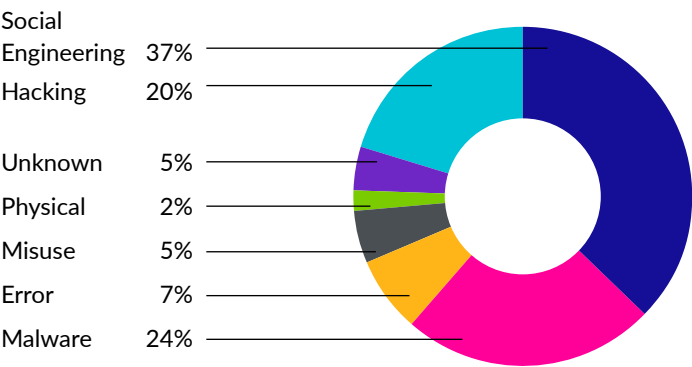
CURRENT TRENDS

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

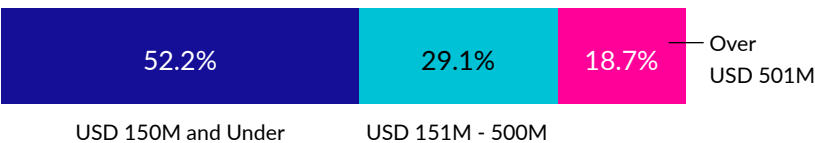
Cyber Claims Trends

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 USD 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.

Australian Privacy Act

The Australian Privacy Act was recently amended in 2024 and is the primary legislation that addresses how companies, individuals and governments handle personal information and data. The legislation provides a structure and framework for civil penalties to be levied against organisations and individuals for serious invasions of privacy with the civil penalties available being up to: \$50m AUD, 3 x the value of the benefit obtained through the invasion/misuse of data or 30% of annualised turnover. The legislation further provides the Office of the Australian Privacy Commissioner (OAIC) with increased regulatory powers and scope to investigate organisations that have been alleged to breach the legislation through investigative, enforcement and public inquiry powers.

Security of Critical Infrastructure Act Australia

The Security of Critical Infrastructure Act 2018 (Cth), which was amended in 2024, is a key part of the Australian Government's plan to implement improved controls, requirements and obligations for certain industries and organisations. The legislation identifies and defines certain industries and organisations within Australia that are critical to the Australian 'society, economy and security' and imposes minimum data security and reporting obligations as well as providing civil penalties for non-compliance, or even criminal penalties.

Artificial Intelligence (AI)

While harnessing the full potential of AI remains a top priority for organizations 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, AI is also weaponised by those wishing to cause harm.



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

All ERM and PremierTech 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 organization'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 defenses.
- 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



A curated collection of services, worth up to \$45,000 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



Dedicated cyber experts focused on stacking up your defenses.

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 are comprised of experienced third-party service providers that provide legal, computer forensic, notification, call center, public relations, crisis communications, fraud consultation, credit monitoring and identity restoration advice and services.

Chubb Cyber AlertSM



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:



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.





Protect your business with Chubb.

Learn more about Chubb Cyber solutions at chubb.com/cyber



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)

⁴ World Economic Forum – Global Risks Perception Survey, 2024

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

⁶ Chubb Cyber Index

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. Review specific terms and conditions of each service provider to ensure eligibility and to stay updated on any changes that may occur. Average savings converted from USD to AUD and based on a US-wide survey of participating vendors from 15 June to 15 July 2025 who reported pricing for their services without cyber insurance in place.

Chubb is the marketing name used to refer to subsidiaries of Chubb Limited providing insurance and related services. For a list of these subsidiaries, please visit www.chubb.com.

Chubb's cyber services cannot be construed to replace any provisions of your policy. You should read your policy, including all attachments, for complete information on the coverage provided. Chubb has no obligation to provide any cyber services for loss mitigation. The policyholder is under no obligation to contract for services with any of the Chubb pre-approved cyber service providers. The selection of a particular cyber service provider is the independent choice of the policyholder. Chubb is not a party to any agreement entered into between any cyber service provider and the policyholder. It is understood that cyber service providers are independent contractors, and not agents or representatives of Chubb. Chubb assumes no liability arising out of any services rendered by a cyber service provider. Chubb also assumes no liability arising out of a delay in user access to any cyber service provider portal, or delay in services rendered by a cyber service provider, during any complimentary trial period. Chubb shall not be entitled to any rights, or subject to any obligations or liabilities, set forth in any agreement entered into between any cyber service provider and the policyholder. Any rights and obligations with respect to such agreement, including but not limited to billings, fees and services rendered, are solely for the benefit of, and borne solely by, such cyber service provider and the policyholder, and not Chubb. Neither Chubb nor its employees or agents make any warranties or assume any liability for the performance of any cyber service provider, including any goods or services received. Chubb does not endorse the cyber service providers or their respective services. Before a policyholder engages with any cyber service provider, the policyholder should conduct its own due diligence to ensure the company and its services meet the policyholder's needs.

This content is brought to you by Chubb Insurance Australia Limited ("Chubb") as a convenience to readers and is not intended to constitute advice (professional or otherwise) or recommendations upon which a reader may rely. Any references to insurance cover are general in nature only and may not suit your particular circumstances. Chubb does not take into account your personal objectives, financial situation or needs and any insurance cover referred to is subject to the terms, conditions and exclusions set out in the relevant policy wording. Please obtain and read carefully the relevant insurance policy before deciding to acquire any insurance product. A policy wording can be obtained at www.chubb.com/au, through your broker or by contacting any of the Chubb offices. Chubb makes no warranty or guarantee about the accuracy, completeness, or adequacy of the content. Readers relying on any content do so at their own risk. It is the responsibility of the reader to evaluate the quality and accuracy of the content. Reference in this content (if any) to any specific commercial product, process, or service, and links from this content to other third party websites, do not constitute or imply an endorsement or recommendation by Chubb and shall not be used for advertising or service/product endorsement purposes. ©2025 Chubb Insurance Australia Limited ABN: 23 001 642 020 AFSL: 239687. Chubb®, its logos, and Chubb.Insured.SM are protected trademarks of Chubb.