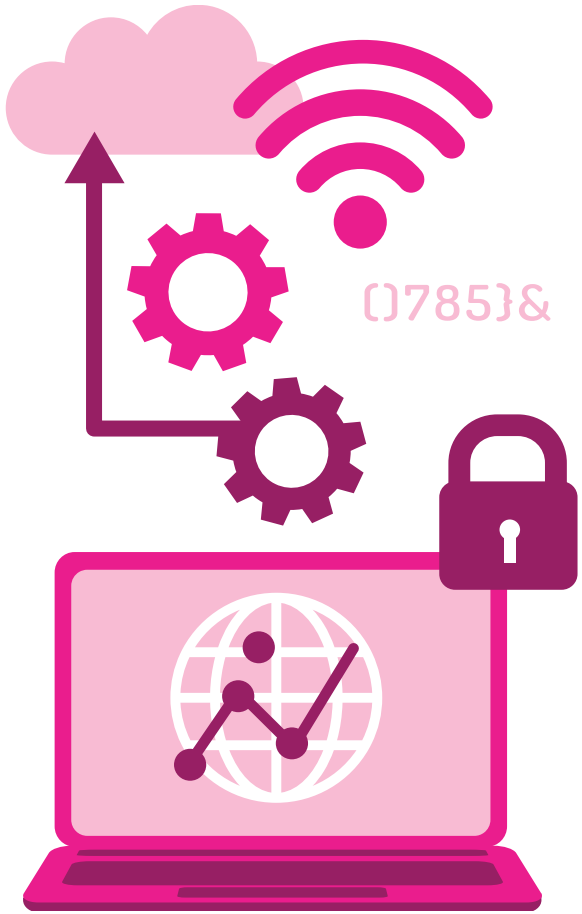
CHUBB®

Cyber Risk Management Guide for Our Agents and Brokers

For Broker Use Only

This guide includes information on:

Why Is Cyber Important?



The information and digital age allows us to collect more data, collaborate more efficiently, streamline business processes, and extract information around the globe 24/7.

Increased reliance on computer systems and access to information can significantly increase a company's exposure to cyber security threats. Outages, mistakes, or attacks on these new processes can result in significant out-of-pocket costs that can devastate an organisation's bottom line. So when it does happen, you'll need broad protection from an insurer that specialises in handling cyber risks, offers a full suite of integrated insurance solutions to help minimize gaps in coverage, and understands how to tailor coverage to your business. **Chubb has been committed to providing our insureds with cyber solutions since 1998.**

Gaps in Traditional Insurance

Businesses may be operating under the belief that their existing insurance policies are enough to cover their data security and privacy exposures. Unfortunately, this is not always the case and traditional insurance policies may be inadequate to respond to the exposures organisations face today. Consider these traditional policies:

General Liability	Property	Crime
General Liability policies are typically triggered in response to Bodily Injury (BI) and Property Damage (PD) claims. A cyber event will not usually involve either BI or PD and General Liability policies typically don't offer coverage for any first-party costs.	Property policies typically respond to destruction or damage to tangible property resulting from a physical peril. The tangible loss then permits the business interruption and extra expense coverage to respond. A cyber event, on its own, may not result in physical damage, yet the event can shut down a business resulting in substantial expense costs and loss of income.	Crime policies typically respond to direct losses from employee theft of money, securities, or tangible property. Computer crime extensions usually exclude any third-party liability coverage and may not sufficiently cover the loss of confidential information.

Exposures by Industry

Financial Institutions

Financial institutions are highly exposed to cyber risk due to a combination of factors. Cyber crime, hacktivism and sophisticated attackers carrying out espionage on behalf of a beneficiary are just some of the risks to consider. Vulnerabilities to cyber events can be high as many financial institutions are dependent on highly interconnected networks and critical infrastructures. With a high dependency on technology, most financial institutions will continue to see increased exposure to cyber risk.

Common claims:
Social - Phishing and
Human Error

Healthcare

A broad movement toward digitisation of medical records has resulted in the increased reliance of healthcare companies on computer systems to collect and transact highly sensitive personal health and medical data. There is a high exposure to administrative errors due to the reliance on employees to input accurate information into systems. Legacy computer systems are often unsegregated, which increases the potential that one event could have a severe impact on operations.

Common claims:
Human Error and **Misuse**

Retail

Whether online or brick and mortar, Chubb's claims data shows that the retail industry is significantly exposed to cyber losses. Retail companies often have many locations that may or may not operate on centralised IT systems, a reliance on a complicated network of critical IT service providers, a potential dependency on websites due to the increasing number of online sales, and an aggregated amount of sensitive personal information due to the high frequency of financial transactions and loyalty programmes.

Common claims:
Hacking and
Social - Phishing

Hospitality

The hospitality sector covers a wide range of operations from hotels to bars and restaurants. Across the industry, cyber related exposures include large volumes of consumer and employee information, an often heavy reliance on websites for customer bookings, and loyalty programme information that can lead to privacy issues as it can be a target of social engineering and phishing attacks.

Common claims:
Social - Phishing
and **Hacking**

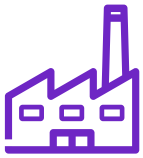
Professional Services

With the amount of confidential data collected, the professional services sector is a popular target for cyber attacks. For example, the information and funds a law firm or an accountant holds can be lucrative for an attacker, and the reputational consequences for a firm suffering a breach can be highly damaging. The aggregation of sensitive client information has fueled an increase in cyber events impacting professional service firms in recent years.

Common claims:
Human Error
and **Hacking**

*Common causes of cyber claims come from the Chubb Cyber Index®

Exposures by Industry



Manufacturing

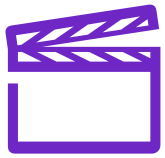
Manufacturing is one of the largest industries being targeted by cyber criminals. Significant technology integration is changing how manufacturers operate their businesses. To improve productivity and cost efficiencies, many manufacturers are leveraging the Internet of Things (IoT), digitalisation, and cloud services, which all increase the impact of certain cyber events. Recent events impacting Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems have had crippling effects on operations.

Common claims:
Malware and **Social - Phishing**

Education

Educational establishments are at risk due to the sensitive data they hold on students and staff. Schools and universities often have limited IT budget and resources. Threats are both external and internal, whether it is from a student introducing malware into their network either maliciously or inadvertently, or a staff member not following protocol, leading to a data breach.

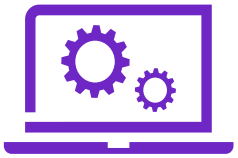
Common claims:
Social - Phishing and **Hacking**



Media/Entertainment

Media and Entertainment companies often face cyber extortion threats that may target sensitive material and content. Distributed Denial of Service (DDoS) attacks or computer system outages may significantly impact broadcasting activities and timely content delivery. The possession of sensitive personal information of subscribers compounds the exposure.

Common claims:
Human Error and **Social - Phishing**



Technology

Technology companies are trusted by their clients and customers to be industry leaders in the cyber security and protection of data, increasing the reputational damage that could follow a cyber event. Cyber events experienced by technology providers can also have an impact on Technology Errors and Omissions (E&O) coverage - please reach out to your Chubb underwriter for more information on our market-leading combined Tech E&O and Cyber insurance offering.

Common claims:
Hacking and **Human Error**

*Common causes of cyber claims come from the Chubb Cyber Index®

See what Chubb can offer to small, medium, and large businesses to address these exposures:

Small Businesses | **Middle Market** | **Large Businesses**

Small Businesses - Overview

Despite greater media attention given to cyber events at large organizations, Small and Midsized Businesses (SMEs) are frequently impacted by cyber threats and vulnerabilities. Small businesses are often seen as easier targets for cyber criminals due to often limited IT resourcing and investment.

In addition, they may be less likely to have invested in measures such as staff training on data security, guidance on password setting, and two factor authentication. SMEs often represent a lucrative opportunity for cyber criminals compared to larger organisations that may be harder to crack. They also have to consider they may not be the initial target, but can simply be impacted by an event experienced by an outsourced IT provider or a commercial business partner.

Small Business Claims - Chubb Cyber Index®

The best way to illustrate the cyber risk that small businesses face is with data. Chubb has handled cyber claims for more than two decades. As part of the claims process, we track key metrics such as actions causing a cyber loss, whether a cyber event was caused by an internal or external actor, the number of impacted records, and the size and industry of the affected insured. Through the Chubb Cyber Index®, we share this data publicly to help businesses better understand the risks they face.

The Chubb Cyber Index® provides users with a means of identifying the leading cyber risks their business may face based on the real-world examples of cyber attacks and data breaches. Users can set parameters and view historical trends based on type of threat, size of a company, and which industry that company operates within.

To find out more, visit the Chubb Cyber Index® at: **https://chubbcyberindex.com**

Small Businesses - Claims Scenarios

Ransomware

Our insured, a construction company, was the victim of a targeted ransomware attack. The insured's systems were breached following an employee clicking a malicious link on an email. The insured's systems and servers were encrypted and a demand for £800k of bitcoin followed. The insured utilised Chubb's incident response managers to instruct IT forensics to establish the method and scope of the attack. Despite not paying the ransom, the total business operations were disrupted for more than six months.

Applicable coverage section:

Data and System Recovery, Business Interruption, Incident Response Expenses and Cyber Extortion.

Mitigation

Regular review of IT security, employee training, regular back up of data and have Disaster Recovery Plan and Business Continuity Plan in place.

Disgruntled Employee

Our insured was the victim of a rogue employee who stole in excess of 700 clients' personal data records, including names, addresses and contact details. They were supplied to the new employer for the new employer's benefit. To comply with GDPR requirements, notice had to be provided to the local regulator's office and the affected data subjects.

Applicable coverage section:

Privacy Liability and Incident Response Expenses.

Mitigation

It's incredibly difficult to prevent rogue employees seeking to cause harm. More often than not they have the requisite system access to enable theft of either personal or corporate sensitive data. On current case law, it is likely a company would be liable to their clients. A Chubb cyber insurance solution provides the tools needed to respond when this occurs.

Employee Error

Our insured, a regional UK housing association, inadvertently suffered a data breach as a result of an employee error. When posting a new advert for a vacant property, the employee mistakenly included an image of a separate client's medical records within the online property brochure.

Applicable coverage section:

Privacy Liability and Incident Response Expenses.

Mitigation

It is important to have an enterprise-wide privacy policy detailing protocol for handling sensitive information. Employees should be accountable for understanding and acknowledging compliance with the policy at least annually.

Small Businesses - Claims Scenarios

Unauthorised access – Phishing

Our insured, a logistics firm, was the victim of a malware phishing attack. An employee in the insured's HR team had a pop-up on their computer after clicking a malicious link within an email. The pop-up stated the computer was infected and to call the number provided. Fraudsters then gained remote access to the employee's computer by further deceiving the employee during the call.

Applicable coverage section:

Privacy Liability, Network Security Liability and Incident Response Expenses.

Mitigation

Even with the best security technology and systems, an insured's most vulnerable asset is often its staff. Staff can be duped into surrendering passwords or providing access. Regular phishing training is advised, and having an insurance policy that will provide the relevant expertise is essential.

Physical data record loss

Our insured, a law firm, contacted the Chubb incident response hotline when it came to light an employee of the firm had broken company protocol by taking client records from the office and storing them in their car. The car was subsequently stolen and the client records lost.

Applicable coverage section:

Privacy Liability and Incident Response Expenses.

Mitigation

Have a clear process in place for both digital and physical data storage. Regular data back-up is important to be able to recover quickly. Create an enterprise wide privacy policy that employees are required to acknowledge and adhere to.

Small Businesses - A customisable cyber solution that grows with you

1 Loss Mitigation Services for Small Businesses

To help our SME insureds mitigate common cyber claims trends, Chubb offers a number of services to our policyholders through service providers, where permissible by law.

Password Management Solutions for up to 100 employees of each policyholder.

- Effective password management can help minimize the unauthorized use of stolen credentials.

Employee Training Solutions help your team prepare for phishing threats identify potential cyber threats, protect sensitive data, and escalate issues to the right people when needed.

Vendor Management Solutions help you assess and qualify third and fourth-party vendors before they enter your business ecosystem.

2 Incident Response Services for Small Businesses

Chubb understands that not all events can be avoided. When something does occur, our cyber policies provide an expert panel of incident response service providers for our SME clients.

These specialists are available 24/7/365 and are prepared to guide you in recovering from any cyber event.

- Experts include incident response management, IT forensics, legal resources, public relations, and more.
- Access to the provider network is included as part of the policy.
- Available 24/7/365 via the Cyber Alert® app or toll-free hotline.
- Can provide assistance following any cyber event–they are there to help in any emergency.

3 Small Enterprise Platforms

Chubb's online platforms (available in select countries) have been designed specifically for brokers to quote and bind preferred small business insurance online. By combining intuitive design with a customer-centric experience, brokers can arrange their client's cyber insurance in a matter of minutes before issuing documentation on the spot.

Arrange coverage quickly and easily; includes the same policy benefits as offline:

- Simple question set
- Wide risk appetite for SME businesses
- Same cyber policy language as offline business
- Access to Chubb's Cyber Loss Mitigation Services
- Edit policy dates, limits, commission rates and contact details without the need to contact an underwriter
- Quote and bind risks within a few minutes

Click here for more information on our full suite of cyber services, including cyber security and more.

See here for more information on how Chubb's Incident Response solution operates.

Contact your local Chubb underwriter to find out where we have online cyber insurance capabilities or other simplified SME solutions.

Middle Market - Overview

Middle market enterprises face the same cyber security issues as large enterprises, but with less of a budget to spend, and not as many specialist staff to manage this risk. They often take the same view as many SME clients, believing that only large global businesses have a significant risk. As malicious activity has become more sophisticated, the struggle for middle market businesses to defend themselves is now tougher than it's ever been.

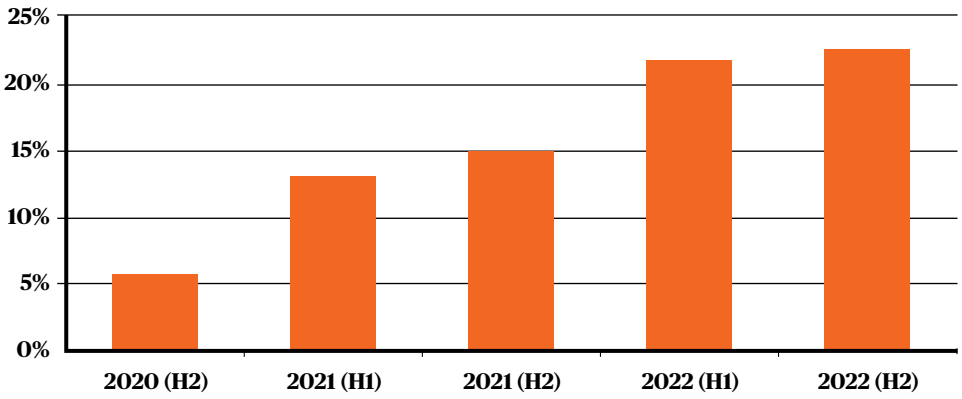
Chubb Cyber Index®

The Chubb Cyber Index® provides users with a means of identifying the leading cyber risks their business may face based on the real-world examples of cyber attacks and data breaches. Users can set parameters and view historical trends based on type of threat, size of a company, and which industry that company operates within.

To find out more, visit the Chubb Cyber Index® at: **https://chubbcyberindex.com**

Chubb Claims Compared to H1 2020 (Percentage Growth)

Middle Market - All Industries



Middle Market - Claims Scenarios

Ransomware

An assisted living facility experienced a “brute force” ransomware attack and had several of its files encrypted. A ransom of approximately €26,000 was initially demanded. After paying a small amount of the ransom demand to obtain a sampling of the decryption tool, the company decided to instead rely on its backups to restore its systems.

Applicable coverage section:

Data and System Recovery, Business Interruption, Incident Response Expenses and Cyber Extortion.

Mitigation

Investing in security technology, whilst essential to help prevent unauthorised access, is not foolproof. Attackers are constantly evolving their attack methods, and any business has to review their security and procedures regularly to keep pace with the threat.

Employee Error

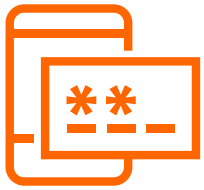
An employee at a hardware retailer ignored internal policies and procedures and opened a seemingly innocuous file attached to an email. The next day the hardware store’s stock order and cash registers started to malfunction and business trade was impaired as a result of the network failing.

Applicable coverage section:

Data and System Recovery, Network Security Liability, Business Interruption and Incident Response Expenses.

Mitigation

Regular training to ensure staff are aware of what to look for in suspicious email attachments, and what process to follow should they have suspicions. In addition, immediate access to an incident manager and a network of responders will enable a swift response.



Data Breach

A hotelier’s network was hacked, leaving potentially all records belonging to both employees and customers compromised, including payment card information from customers.

Applicable coverage section:

Incident Response Expenses, Data and System Recovery, and Privacy and Network Security.

Mitigation

Detection awareness security is a useful tool for combating a hacker. This allows any suspicious activity to be picked up quickly. Encryption of data is also paramount to ensure breached data cannot be easily removed and used.

Middle Market - Claims Scenarios

Cryptomining

A manufacturing company experienced a ransomware attack that resulted in the encryption of several of their files. After the Insured contacted Chubb through the 24/7 incident response hotline, we offered a consultation with an incident response manager and forensic experts from our cyber panel. As a result of these discussions, the Insured chose not to pay the ransom. However, once the forensic firm began working on remediating the ransomware attack, they discovered that the Insured was also the victim of Cryptojacking. The attackers had installed software in the Insured's system that was mining Bitcoin. Cryptojacking occurs when an unsuspecting party's computer system is being used for cryptocurrency mining without their knowledge.

Applicable coverage section:

Incident Response Expenses, Business Interruption, Data and System Recovery and Privacy and Network Security.

Mitigation

Regularly reviewing IT security is important for a manufacturer to ensure production isn't affected by an attack. They need to consider a disaster recovery plan, and business continuity plan should they be caught up in an attack to allow them to minimise the disruption. Unauthorised access is not foolproof. Attackers are constantly evolving their attack methods, and all businesses must review their security and procedures regularly to keep pace with the threats.

Data Theft Results in Extortion, Business Interruption and Extra Expense

An unknown organisation hacked a law firm's network and may have gained access to sensitive client information, including a public company's acquisition target, and a significant number of class-action lists containing plaintiffs' Personally Identifiable Information (PII).

A forensic technician hired by the law firm determined that malware was sent in an email which evaded email filtering controls, and also tricked a user into clicking a malicious link in order to execute itself within the organization's network.

Applicable coverage section:

Cyber Extortion, Privacy and Network Security, Business Interruption and Incident Response Expenses.

Mitigation

Training of staff to attempt to prevent opening malicious email is important. In addition having IT security in place to catch malware should it slip through the net should be implemented.

Middle Market - A customisable cyber solution to fit your business

1 Loss Mitigation Services for Middle Market

To help our Middle Market insureds mitigate common cyber claims trends, Chubb offers a number of services to our policyholders.

Password Management Solutions included in the policy for up to 100 employees of each policyholder.

- Effective password management can help minimise the unauthorised use of stolen credentials.

Phishing Training Simulations are available to policyholders.

- Phishing is one of the fastest growing causes for cyber losses, and simple training for employees can be an effective tool to minimise a phishing attack penetrating Middle Market companies.

2 Penetration Testing & Attack Surface Management

Get preferred pricing and connect with security experts to evaluate your internal and external systems for cyber exposures from an attacker's point of view. Improve your visibility, inventory, and understanding of your online assets and exposures

- Attack surface management: Scanning on publicly available, internet-facing IP addresses and domain names that are operated by a policyholder or by service providers.
- Internal Network Pen. Test: up to 25 active systems
- External Network Pen. Test: up to 10 active systems

Custom Scope

- Mobile App, Web App, and Cloud Penetrating Testing

3 Incident Response Services for Middle Market

Responding quickly and effectively to a cyber event is key to minimising impact and losses - for when something does occur, our cyber policies provide access to an expert panel of incident response service providers for our Middle Market clients. These specialists are available 24/7/365 and are prepared to help your business recover from any cyber event.

- Experts include incident response management, IT forensics, legal resource, public relations experts, and cyber extortion negotiators.
- Flexible to use our panel of providers or any vendors that you have already contracted with as part of a cyber incident response plan.
- Available 24/7/365 via the Cyber Alert® app.

Click here for more information on our full suite of cyber services, including cyber security and more.

See here for more information on how Chubb's Incident Response solution operates.

Middle Market - A bespoke cyber solution

3 Risk Engineering Services

How each client operates and the technology they use can be different in every circumstance. Our Cyber Risk Engineers help clients identify and understand their technological vulnerabilities and assist them in preventing a future cyber event even before a policy incepts.

Key Benefits

Direct engagement with clients to gain a deep understanding of the risk and exposures

Flexibility for engagements pre-bind or on-risk

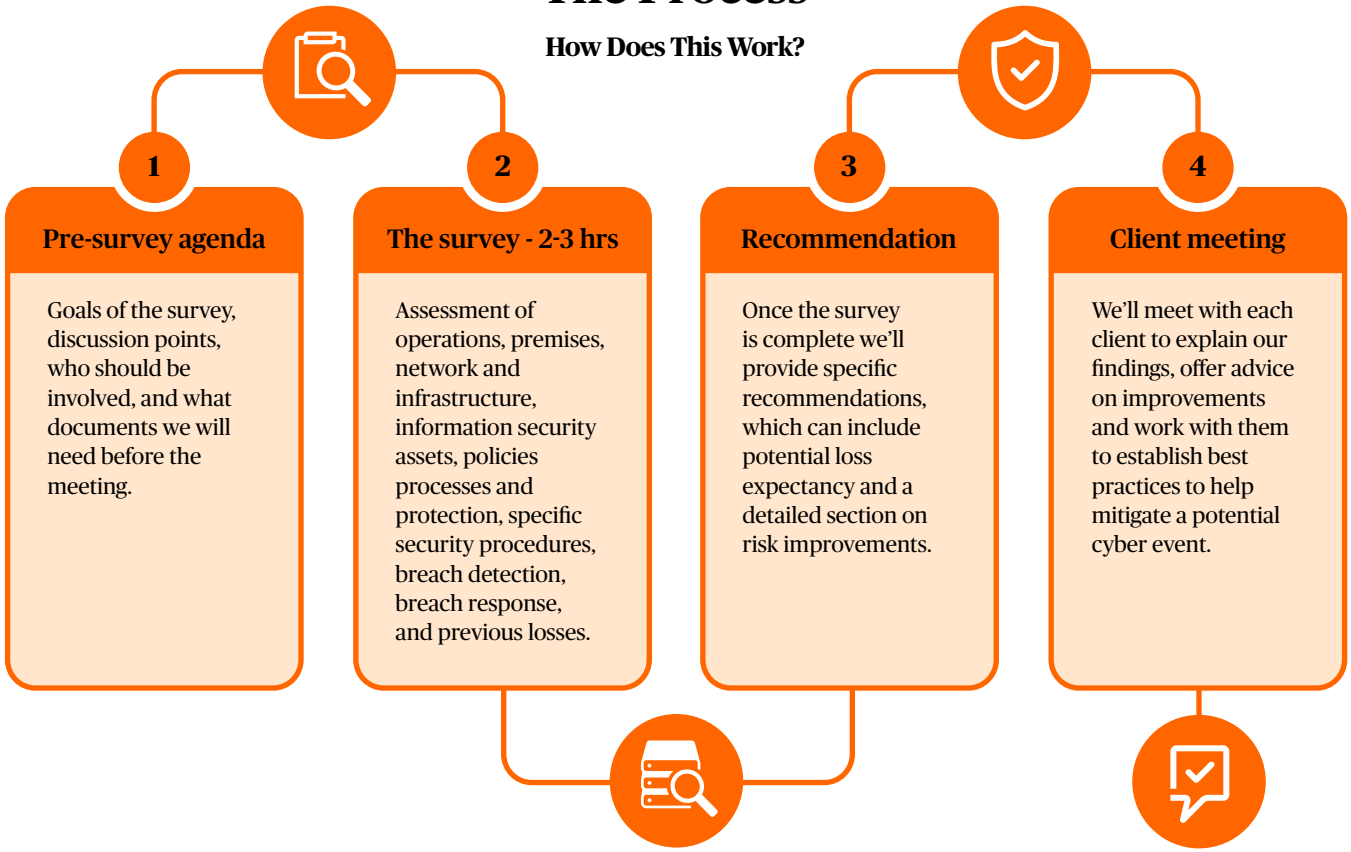
Risk recommendations with guidance on how clients can improve their overall cyber risk management profile

Additional direct technical training is available for clients and brokers

While this service is specifically designed for Middle Market customers, it can be considered for any size company.

The Process

How Does This Work?



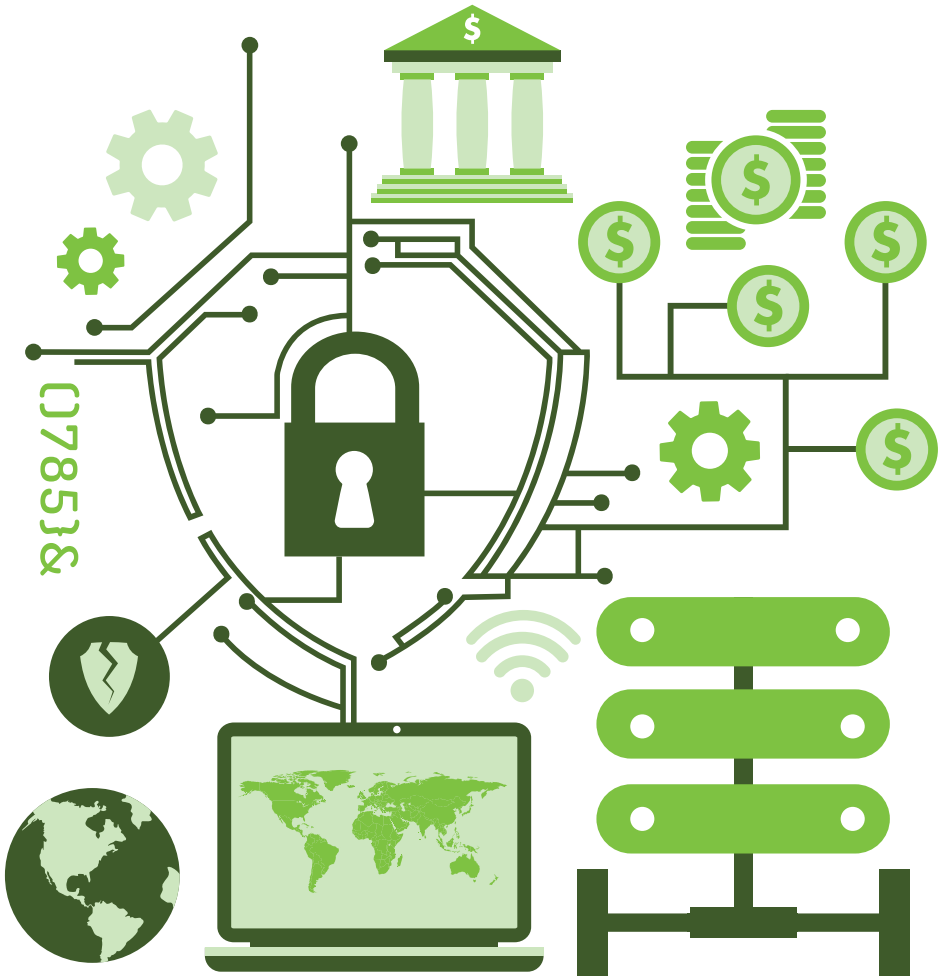
Large Businesses - Overview

As the number of highly publicised cyber attacks on large and multinational companies has increased in recent years, the demand for cyber insurance has escalated rapidly. The growing demand has been fuelled by intensified pressure on boards to demonstrate an accurate assessment of cyber risk, increased regulatory oversight, and an expanded need for information sharing amongst colleagues and partners. Boards and risk managers recognise that cyber insurance should be more than just risk transfer. Chubb's offering for Large Businesses provides a global-yet-flexible incident response solution, extensive multinational programme options, captive fronting abilities, and meaningful capacity through our Global Cyber Facility.

Incident Response Services for Large Businesses

Cyber incident response plans are often established and frequently tested by larger organisations – Chubb's cyber incident response services are intended to supplement what is already in place. Our team of cyber incident response coaches are prepared to work with an insured's preferred specialist vendors, even if they are not part of the Chubb panel.

- Policy includes the use of vendors with whom our customers have already contracted as part of a cyber incident response plan.
- Our global network of local incident response teams are designed to meet the needs of multinational risks.
- Chubb's Cyber Alert® app, designed for a risk manager or IT manager, connects to our incident response and claims team to streamline expert assistance and policy response.



See here for more information on how Chubb's Incident Response solution operates.

Global Incident Response Panel

Large Businesses

1 Multinational Programmes

The global nature of cyber risk requires companies to understand how their policies can respond to an international event, and what restrictions might apply. Structuring an efficient, cost-effective multinational insurance programme requires a close understanding of the evolving cyber regulatory environment.

Some specific questions when considering a multinational insurance programme:

- Where are the entities located? Restrictions may differ between countries.
- Do countries allow a non-admitted insurer to pay losses directly to the local entity? What are the specific country restrictions?
- Does the client want to protect insureds locally? Benefits from a local policy include: local claims payments, local policy language, and local claims handling.

Chubb's multinational cyber capabilities:

Chubb can offer multinational cyber programmes locally and cover more than 94 countries around the world, serviced by Chubb's fully staffed global services team with the expertise and specialists prepared to assist with multinational insurance needs.

2 Global Cyber Facility

A broad cyber risk management solution for Large Businesses.

Whom does this apply to?

- Organisations with more than $1B in annual revenue.
- All industry classes, including retailers, financial institutions, and manufacturers.

Components to the offering:

- Pre-event loss control services from globally recognized cyber defence organisations to address cyber deficiencies identified during risk assessment.
- Risk transfer policy.
- Post-event incident response and claims management.

Key policy coverage:

- **Primary limits available up to $30m of Chubb capital** accretive to the market to support large towers.
- **DIC/DIL endorsements available to fill gaps** between an organisation's cyber, casualty, and property policies.
- Flexible policy form available.

What is the process?

- Proactively begin sales process three months prior to market tender.
- Proprietary Chubb assessment to analyse an organization's risk profile.
- Direct engagement between client and Chubb underwriting.

Large Businesses

3 Captives

Managing cyber risk within a captive is becoming increasingly relevant for multinational companies that find a combination of risk transfer and risk retention meaningful. Captives are becoming a common solution to maintain adequate but manageable premiums, or to carve out local policy deductibles into a consolidated structure.

A captive can also provide more comprehensive coverage than what is available in the commercial insurance market for the parent company. This allows a company to gain an understanding of its exposures and to capture loss information so that an insurer or reinsurer will then be able to take on the risk at an appropriate limit and premium.

Why

- Optimise risk transfer
- Provide diversification
- Act as incubator
- Access to add-on services

How

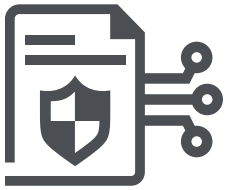
- Various structures possible
- Small primary/large deductible layers
- Quota share of large programs
- Peril specific

Challenges

- Uncertainty/ understanding exposure
- Pricing of retention layer
- Aggregation with other lines

Key Selling Points

Not all of your clients will understand the importance of a cyber insurance policy, or all of the benefits that one can provide. We've put together a few key selling points to help you explain some of these benefits to your clients.



Affirmative protection

Traditional insurance policies may be inadequate to respond to cyber exposures. A cyber policy is specifically designed to address these gaps and give you affirmative protection against exposure that can be difficult to grasp.

You don't have to be the target to be affected

Cyber attacks can spread through your suppliers or your outsourced technology providers, leading to significant impact even when you aren't the target. Chubb has seen significant collateral damage from cyber incidents originating at separate companies. What if your data storage provider is the target of a cyber attack, and your data is compromised in the process?

Insurance covers response and recovery expenses, not just liability resulting from data compromise

Liability arising from the loss or misuse of sensitive data is only one potential outcome of a cyber incident. Business interruption, incident response, and digital data recovery costs make up a significant portion of Chubb's claims payments, even without liability claims.

Complement to existing IT teams

Cyber insurance does not undermine the effectiveness of IT security teams - it supplements their skills and protects a business from the unknown.

Key Selling Points

Multinational threats

Cyber losses are not only sustained locally. Chubb helps companies recover from cyber incidents taking place around the world, including data breaches, ransomware attacks, and other incidents.

All businesses can be affected

Cyber incidents can impact any company, regardless of size and industry. Threats can be targeted, employee mistakes can be made, or collateral damage losses can be experienced from a wider cyber incident. Chubb has flexible solutions depending on your needs, maturity level, and size of business.

Responding to evolving regulation

New privacy regulations have increasingly higher standards and penalties - and cyber insurance can help you through these changes. Chubb's policy language contemplates new and evolving privacy regulations.

Adapting to emerging cyber risks

Chubb delivers emerging cyber claims trends on a quarterly basis, keeping you aware of new risks as we see them. The Chubb Cyber Index® also gives you up-to-date information on both recent and historical trends.

Cyber Services

Bridging the gap between cyber insurance and cyber security expertise

Purchasing cyber insurance from Chubb is a great first step an organisation can take to help recover from the financial and reputational losses when data breaches and system outages occur, but protection doesn't end there. Chubb's policyholders have access to essential mitigation tools and advisory resources to help reduce exposures 365 days a year.

Help your clients put the power of our solutions and advisory services to work today. To get the latest information on our services or to schedule an orientation call with a Chubb Cyber Risk Advisor, visit https://go.oncehub.com/ChubbCybersecurityServices or email us at cyber@chubb.com

To register for services and to find out more information, please visit the Chubb Cyber Services website:

www.chubb.com/cyber-services

Cyber Services

1. Cyber Incident Response Solutions

Deploy tools and assessments that can help identify and address cyber security risks before an incident occurs.

Incident Response Mobile App | Breach Response Plan Builder | Virtual Cyber Incident Response Tabletop Exercise

2. Cyber Vulnerability Management Solutions

Stay on top of software and network vulnerabilities that could impact the bottom line.

Chubb Cyber Vulnerability Alert System | External Vulnerability Monitoring | Penetration Testing and Attack Surface Management | Vulnerability Management Platform Library

3. Endpoint Cyber Security Solutions

Access solutions to help stop malicious activity from entering and spreading through a network.

Endpoint Security and Response | Extended Detection and Response

4. User Security and Education Solutions

Create and maintain a workforce to serve as a first line of defense.

Multifactor Authentication (MFA) Assessment and Implementation Solutions | Secure Password Manager | Phishing Email Simulator | Security Awareness Training | Cyber Risk Resource

www.chubb.com/uk-en/business/cyber-services-registration.aspx

Get More Info

Get more info, contact our Cyber Risk Advisory Team
cyber@chubb.com

*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.

Discounted cyber services offered by third party vendors:
External Vulnerability Monitoring, Secure Password Manager, Personal Cyber Risk Dashboard The cyber services set forth above are 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.

Stay Ahead: Be Informed, Act Swiftly Against Vulnerabilities

In today's constantly evolving digital landscape, businesses of all sizes find themselves under the constant threat of cybersecurity breaches. According to Cybersecurity Infrastructure Security Agency (CISA), 50% of known exploited vulnerabilities (KEVs) are exploited within two days of being identified and 75% are exploited in less than a month. It is imperative to have a vulnerability management program in place to act fast and remediate before malicious activity enters and spreads throughout an organization's network.

Vulnerability Outreach Programme

With our Vulnerability Management Outreach, our Cyber Intelligence Team routinely monitors, scans, and identifies vulnerabilities and new critical threats to help safeguard our policyholders. Policyholders who register to receive alerts are informed by:

Outreach Program - a proactive notification to cyber policyholders if identified known critical vulnerabilities are detected to be in their environment and have a high probability of exploitation.

- An initial communication via email, which details the exposure and actions required to remediate.
- Follow-ups, which are then conducted via email and phone calls.

Breaking Alerts - are sent to cyber policyholders when new vulnerabilities with a high probability of exploitation are discovered and may impact their environment.

- A communication via email, with information on the new threat is generally sent within 24 hours of discovery.

Additional Cyber Vulnerability Management Solutions

In addition to our Vulnerability Management Outreach, all Chubb Cyber policyholders are eligible to register for the following complimentary cyber services:

- **External Vulnerability Monitoring** - In partnership with BitSight, and Security Scorecard, policyholders can monitor cyber risk as a daily measurement of their security performance via a platform that uses key metrics to highlight both strengths and potential weaknesses, providing visibility into the security of their organization.

Cyber policyholders can also take advantage of the following vulnerability management solutions at preferred pricing:

- **Penetration Testing and Attack Surface Management**- Connect with offensive security experts to evaluate policyholders' internal and/or external systems for cyber exposures from an attacker's point of view. This can improve visibility, inventory and understanding of online assets and exposures. Provided by NetSPI.
- **Vulnerability Management Platform** - Access software to help policyholders discover vulnerabilities across their IT environment so that they can prioritize and remediate them to improve their security posture. Provided by Tanium.

To register for Chubb's Vulnerability Management Outreach programme and to get more information on Chubb Cyber Services, please visit here.

Incident Response Services - Overview

While Chubb's Cyber Loss Mitigation Services can help decrease the chances of a cyber event, the reality is that no level of protection is perfect against cyber threats. Chubb's cyber policies include our network of Incident Response specialists that are available 24/7/365 and prepared to help our insureds recover from any cyber event.

Highlights

Chubb helps companies recover from multiple cyber incidents every day around the globe.

When insureds notify a cyber incident through the Chubb Cyber Incident Response Centre, they will receive **immediate assistance** from a cyber reporting specialist to collect important details to get the right experts together. 90% of these insureds will receive a call back from an expert cyber incident response manager within 15 minutes.

Flexible providers - we realise that some companies would like to use providers that are not part of our network. Chubb offers flexibility for insureds to use specialists of their choosing in many territories, and these can be seamlessly included in our incident response network.

See how our incident response process works here:

Next

See our preferred cyber incident response vendors around the world here:

Next

Incident Response Services - How it Works

This guide details how to access the Chubb Cyber Incident Response Team, how to report a claim, and what to expect from our Incident Response Platform.

1 Client suffers a cyber event

The Chubb Incident Response Platform is available 24/7/365. It provides access to the Chubb Cyber Incident Response Centre and our Cyber Incident Response Team and offers a holistic approach to managing cyber events.

2 Client reports the cyber event using any of the following methods:

Chubb Cyber Alert® mobile application

Find in the Apple Store and the Google Play Store

Download on the App Store | ANDROID APP ON Google play

Access our platform: **www.chubbcyberalert.com**

Telephone Hotline

Find your local number below:

Local Toll Free Numbers

Argentina	**800 666 1967**
Australia	**1 800 027428**
Austria	**0800 005 376**
Belgium	**800 49 405**
Brazil	**0800 095 7346**
Canada	**1 866 561 8612**
Chile	**1 230 020 1212**
China	**400 120 5310**
Colombia	**01 800 518 2642**
Czech Republic	**800 142 853**
Denmark	**80 250 571**
Finland	**0 800 1 12382**
France	**08 05 10 12 80**
Germany	**0800 589 3743**
Hong Kong	**800 900 659**
Indonesia	**001 803 011 2974**
Ireland	**1 80 093 7331**
Israel	**1 80 921 3812**
Italy	**80 019 4721**
Japan	**00531 1 21575**
Korea South	**00798 14 800 6017**
Malaysia	**1 800 8 12541**
Mexico	**001 855 250 4580**
Netherlands	**0800 020 3267**
New Zealand	**0800 441402**
Norway	**800 12554**
Panama	**001 800 507 3360**
Peru	**0800 56006**
Poland	**00 800 121 4960**
Portugal	**800 8 14130**
Singapore	**800 120 6727**
South Africa	**080 09 82340**
Spain	**800 810 089**
Sweden	**020 088 3181**
Switzerland	**080 016 6223**
Taiwan	**00801 13 6828**
Turkey	**0811 213 0171 (landline)**
Turkey	**0812 213 0043 (mobile)**
U. Kingdom	**0800 279 7004**
USA	**1 844 740 9227**
Vietnam	**1203 2353 (VNPT)**
Vietnam	**1228 0688 (Viettel)**

Catch all- any other country can access **+1 844 740 9227 (not toll free)**

Incident Response Services - How it Works

3 Contact from Chubb's Incident Response Centre

Within 1 minute of reporting an event, the client will be connected to a consultant to collect:

- Insured name
- Location of policy
- Contact details
- Location of event

Information will be sent to local incident response management and can be sent to Chubb's claims department. Keeping Chubb informed will provide for the most efficient policy response.

4 Incident Response Management

Within 1 hour of reporting, the client will receive a phone call from a local Incident Response Manager where the event is occurring. Next steps include:

- Conduct initial investigation
- Develop response plan of action to contain event
- Appoint specialists to help with advice and recovery:

IT Forensics | Legal Counsel | Public Relations | Regulatory Compliance | Identity Protection | Credit Monitoring | Forensic Accountancy

5 Recovery

With an expert panel of vendors working to contain the event, the Cyber Incident Response Team will support you in the recovery of your business activities.

6 Follow-up

Chubb's specialist vendors will then discuss the provision of additional services to assist you with your analysis of the event to include future remediation, a review of lessons learned and risk mitigation advice.

Coverage – Cyber Enterprise Risk Management

The Coverage

First Party

- **Incident Response** - from an actual or suspected cyber incident
- **Business Interruption** - loss of net profit and continuing operating expenses
- **Data and System Recovery** - increased cost of work, data recovery costs, additional business interruption mitigation
- **Network Extortion** - extortion payments and negotiation

Third Party

- **Cyber, Privacy and Network Security Liability** - liability following data breach or failure of network security:
  - **Payment Card Loss** contractual liabilities owed to payment card industry firms as a result of a cyber incident
  - **Consumer redress fund**
  - **Regulatory fines** and penalties (where legally insurable)
- **Media liability** - liability following defamation or infringement online

The Highlights

- **Contingent business interruption** for outsourced technology providers
- **System failure** includes - human error, programming error, power failure
- **Standard extensions:**
  - **Emergency incident response** expenses within 48 hours for SME and Middle Market insureds
  - **Betterment costs** - improvement of software and applications
  - **Cyber crime** - direct financial loss following cyber theft
  - **Reward expenses**
  - **Telecommunications fraud**
- **Pay on behalf** for incident response expenses
- **Flexible incident response providers**
- **Rogue employee**
- **Voluntary notification**
- **Voluntary Shutdown**
- **Reputational Harm***
- **Hardware/Bricking***
- Industry's first introduction of widespread cyber events coverage

* by endorsement

Endorsements

Chubb addresses growing cyber risks with a flexible and sustainable approach. Policyholders may tailor cyber insurance coverage levels for Widespread Events, Ransomware Encounters, and Neglected Software Vulnerabilities.

1 Widespread Events

The world is becoming more digitised and interconnected every year. Widely used software programmes, communication platforms, and technology platforms are leveraged and often relied upon by thousands or millions of companies. A single attack upon and/or failure of one of these widely used platforms or technologies could create an aggregation risk that exceeds the insurance industry's capacity to insure. In order to provide policyholders with coverage clarity and market stability, Chubb provides affirmative and specific limits, retentions, and coinsurance for such Widespread Events.

Types of Widespread Event perils covered include:

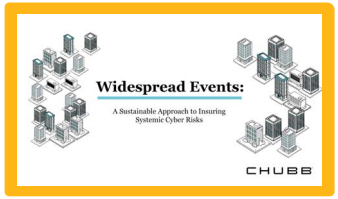
- **Widespread Software Supply Chain Exploits**
  These are attacks that allow bad actors to enter systems through trusted, certified software and are effectively a Trojan horse to a system.
- **Widespread Severe Zero-Day Exploits**
  These are attacks arising from certain software vulnerabilities that are known by cyber criminals but not yet known by anyone else – vulnerabilities that can be easily exploited, are severe, and often lack protection.
- **Widespread Severe Known Vulnerability Exploits**
  These are attacks arising from severe known software vulnerabilities that are not patched. The vulnerabilities are considered severe because they are easy to exploit, can be deployed remotely with limited access privileges, and can result in significant adverse impact.[1]
- **All Other Widespread Events**
  Certain types of cyber attacks can be carried out concurrently or automatically against a wide number of victims, ultimately causing a catastrophic cyber event. The Internet and some telecommunications services have risen to the level of critical societal infrastructure, and some large cloud computing firms are so widely used that an outage could impact the operations of thousands or even millions of companies.

Real-World examples of Widespread Event perils:

- Widespread Software Supply Chain Exploit: Solorigate (2020), NotPetya (2017)
- Widespread Zero-Day Exploit: Hafnium (2021)
- Widespread Severe Known Vulnerability Exploit: MSSP Attack (2021)
- Other Widespread Event: Virginia Cloud Outage (2020)

Chubb's 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, with no return of expenses incurred prior to that determination.
- Policyholders can opt out of sharing certain types of investigatory data when it is mutually agreed that an incident is a Widespread Event.
- All cyber incidents are categorised as either Limited Impact Events (e.g., a local event with "business as usual" loss rules) or Widespread Events (e.g., a systematic event with structural loss adjustment differences such as limit, retention, and coinsurance), enabling policyholders to purchase the coverage that best meets the needs of their organisation.



Widespread Events

[1]NIST Security Vulnerability Trends in 2020: An Analysis (2021). Accessed at https://www.redscan.com/media/Redscan_NIST-Vulnerability-Analysis-2020_v1.0.pdf.

Other coverage sections

2 Ransomware

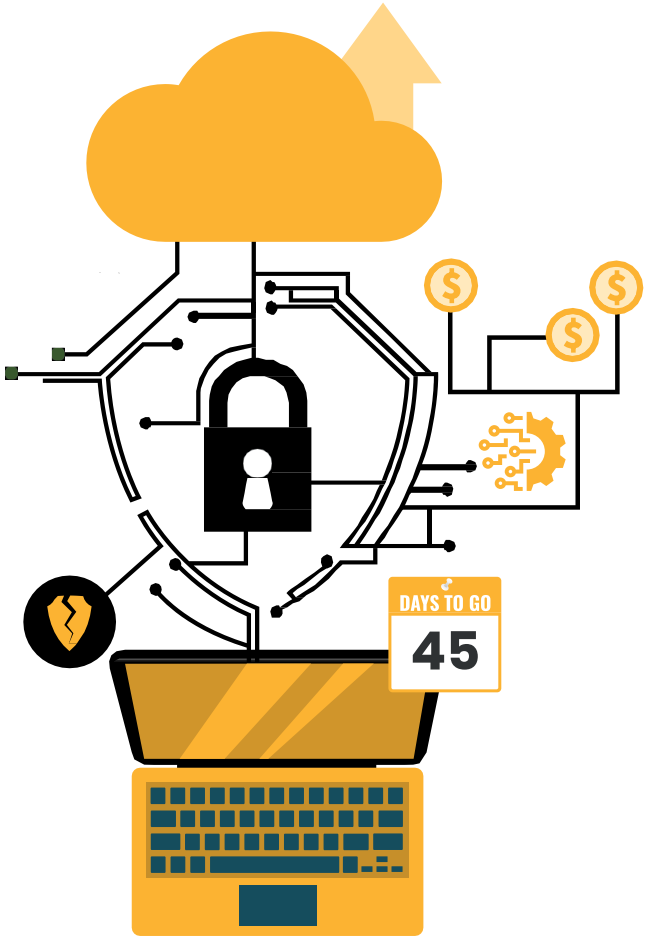
Ransomware attacks have grown dramatically in both frequency and severity. The loss implications to policyholders are far broader than just the value of the ransom amount. Whether the ransom is paid or not, policyholders often incur legal costs, forensic investigatory expenses, business interruption loss, digital data recovery costs, and, potentially, liability and legal defense costs.

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 Vulnerabilities

Keeping software up to date is an important aspect of good cyber risk hygiene. Many losses can be prevented by patching vulnerable software before cyber criminals have an opportunity to exploit it, but some organisations may not patch software right away. Sometimes there are legitimate reasons why 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 within the first day or week after they become available. For that reason, Chubb provides policyholders with a minimum 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 section 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 45-, 90-, 180-, and 365-day points.



Appetite

To help you better service your clients, we have created the following summary of our appetite. This is not an exhaustive list, but provides general guidance. For unique risks or industries not listed below, contact our underwriting team to discuss your requirements.

Preferred

- Advertising*
- Agriculture
- Architects & Engineers
- Art Galleries & Museums
- Automotive Dealers & Service Stations
- Chemicals and Allied Products
- Communications*
- Construction
- Food Production / Manufacturing
- General Contractors
- Management Consultants
- Marketing Consultants
- Non-Profit
- Performing Arts & Theatre*
- Printing and Publishing*
- Products Manufacturing
- Real Estate
- Technical Consultants
- Trade Associations
- TV/Radio/Movie Production*
- Wholesalers

Accepted

- Accountants
- Allied Health Providers
- Asset Managers
- Computer Hardware / Software
- Depository Institutions
- Doctor's/Dentist's Offices
- Employment Agency /Personnel Agency
- Engineering and Management / Services Manufacturing
- Financial Institutions - Not Otherwise Listed
- Industrial Manufacturing
- Investment / Fund Managers
- Law Firms - Corporate Based
- Mortgage Brokers
- Personal Services
- Professional Services - Not Otherwise Listed
- Restaurants / Hospitality
- Retail
- Transportation Services - Not Otherwise Listed

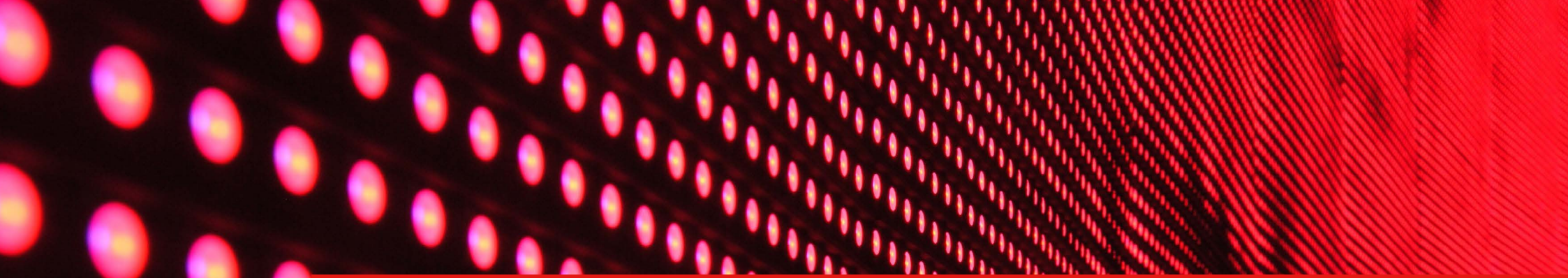
Selective

- Assisted Living Facilities
- Billing Services
- Broadcasting*
- Call Centers
- Collection Agencies
- Colleges and Universities
- Commodities Traders
- Currency Exchanges
- Government
- Hospitals
- Insurance - Non-Personal Lines
- Notaries
- Nursing / Retirement Home
- Public Authority / Special District
- Retail Savings Bank
- Securities and Commodities Brokers
- Small Schools / School Board Pre-K to 12
- Telecommunications
- Telemarketing Services*
- Title Agents

No Appetite

- Adult Content
- Airline
- Cryptocurrency Exchanges
- Initial Coin Offerings
- Data Aggregators
- Online Exchanges
- Social Networking Site / Application
- Trading Platforms

*Not including media E&O coverages



CHUBB®

For more information

To learn more about our cyber offering, please contact our underwriters or visit **www.chubb.com/cyber**

Return to start