Chubb Cyber Enterprise Risk Management

Fact Sheet

CHUBB®

Financial Lines

Chubb Cyber Enterprise
Risk Management

When it comes to a data security breach or privacy loss, it isn't a matter of if it will happen as when it will happen. So when it does happen, you'll need comprehensive protection from an insurer that specialises in handling cyber risks, offers a full suite of integrated insurance solutions to help minimise gaps in coverage, and understands how to tailor coverage to your business.

The Information Age is Changing Business Models and Insurance Needs

The information age allows us to collect more data, store more data and extract information around the globe 24/7. This access to private and sometimes sensitive information can significantly increase a company's vulnerability to cyber security threats - any of which can result in significant out-of-pocket costs that can devastate an organisations bottom line.

Cyber attacks undermine customer, regulatory and employee confidence. They can severely damage the reputation of an organisation which leads to increased customer churn and potential monitoring by regulators.

How prepared is your organisation for:

- Costs for forensic investigations and disaster recovery relating to theft of non-public privacy information or personal records?
- A business interruption event including expenses that result from a security failure or internet virus?
- A cyber extortion threat?
- Costs related to privacy notification, incident response and recovery expenses, public relations costs or credit monitoring?
- A lawsuit stemming from a security failure or alleged technology that results in damages to customers?
- A regulatory proceeding seeking fines or penalties as a result of actual or potential unauthorised access to private information?

The Costs of Data Security Breaches can be Significant

- The estimated annual cost of cyber attacks to the global economy is more than $400 billion.[1]
- Cyber attacks affected 5 million Australians at an estimated cost of $1.06 billion.[2]
- Information theft is the most expensive consequence of a cyber crime (43% of cost) followed by business disruption (33%).[3]
- The average cost of cyber crime to an Australian business is US5.41 million, an increase of 26% from the previous year.[3]

Gaps in Traditional Insurance

The Internet has no boundaries and as business models evolve through the use of new technologies, so must traditional insurance programs and risk management practices. 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 the case and traditional insurance policies may be inadequate to respond to the exposures organisations face today.

Consider these traditional policies:
General Liability policies are typically triggered in response to Bodily Injury (BI) and Property Damage (PD) claims. A cyber attack will not usually involve either BI or PD. General Liability policies typically don't offer cover for any first-party costs.

Property/ISR 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 cover to respond. A cyber attack can cause no physical damage, yet the attack can shut down a business resulting in substantial expense costs and loss of income.

Crime policies typically respond to direct loss from employee theft of tangible property and money or securities. Computer crime extensions usually exclude any third-party liability cover and don't cover the loss of confidential information.

1. Centre for Strategic and International Studies, Net losses: Estimating the global cost of cybercrime– Economic impact of cybercrime II, report, June 2014, McAfee, p. 2. **2.** Symantec, 2013 Norton report: Total cost of cybercrime in Australia amounts to AU$1.06 billion, media release, 16 October 2013
3. Ponemon Institute /Accenture, 2017 Cost of Cyber Crime Study, page 30.

No Company is Immune

Cyber risk is an enterprise wide issue that affects companies large and small. The targets of cyber attacks span a multitude of industries including construction, retailers, restaurants, media companies, manufacturers, banks, asset managers, defence contractors, transport organisations, healthcare organisations, agriculture and professional firms, just to name a few.

Are your clients prepared?

The Solution: Cyber Enterprise Risk Management

Chubb Cyber ERM is more than a policy, it is a risk management solution.

- Cyber Enterprise Risk Management is a comprehensive package designed by cyber risk experts to address the full breadth of risks associated with doing business in today's technology dependent world.
- The policy offers full life cycle support in the event of a network attack or privacy breach.
- The solution includes capabilities for both first party liability and third party liability via several different insuring agreements.
- Policyholders have access to pre event risk mitigation services and post event incident response management, supported by a 24/7/365 call centre, Chubb's expert vendors and award winning claims team.

Coverage Highlights

Third-Party Cyber Liability Coverage for:

- Privacy liability arising from the insured's handling of sensitive non-public personal information, confidential third party corporate information, and violations of the Insured's privacy policy.

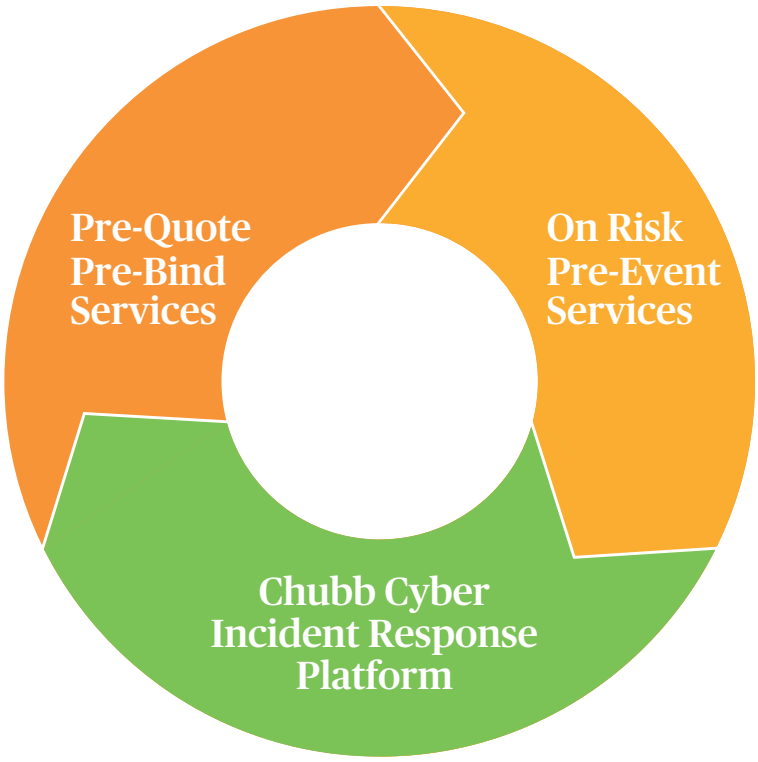
Network Security Liability

- Stemming from the insured's management of their network operations. This could include the impaired access to the Insured's network from an attack, virus attacks (malicious code), the use of the insured's network in a denial of service attack, or the introduction of malicious code.
- Regulatory Fines Payment Card Loss (PCI) and consumers fines result from Privacy or Network Security Liability.

First-Party Expenses

- Incident Response Expenses - including forensic investigation costs, notification expenses and/or regulatory advice. Also, credit monitoring services, identity theft monitoring and fraud services for affected customers are included.
- Business interruption and recovery costs including the cover for acts of criminal hackers, malicious outsiders and distributed denial-of-service (DDoS) attacks. Coverage triggers are extended to human error (fat finger cover) programming errors and power failure of your computer systems.
- Recovery costs to remove malware, reconstruct insured data or costs to mitigate business income loss.
- Cyber extortion expenses, including the cost of hiring crisis negotiators, regulatory IT and PR consultants.
- Data asset loss, includes cover for expenses resulting from entry to, corruption of, or destruction of an Insured's data.

Chubb's Cyber Proposition



Chubb Cyber Incident Response Process

Policyholder calls Chubb Cyber Incident Response Hotline 1800 027 428 or Chubb claims team direct (9am-5pm).

Hotline is available worldwide 24/7/365.

Local Incident Response Manager (IRM) assigned
Incident assessment begins.

Within 5 hours.

Expert vendors Assigned
Based on Chubb's incident triage, our panel of expert vendors are assigned to the incident. i.e.

- Privacy or Data breach
- Rogue employee actions
- Nation state threat

Within 24 hours.

Post Incident Activity
- Analysis
- Policy response
- Future remediation
- Lessons learnt
- Risk mitigation

Incident Containment and Recovery.

Initial incident debrief between IRM and policyholder.

Chubb Cyber ERM offers a comprehensive range of pre and post breach services to help your clients navigate the digital age.

Please contact your local Chubb distribution team for more information.

Note: A call to the Hotline does not constitute notification under the policy unless the Insured specifically requests notification to Chubb.

Loss Scenarios

Consider the following loss scenarios based on actual claims and then ask yourself whether you have adequate insurance in place.

Type of Organisation:
Third-Party Administrator

Employees:
500

Annual Turnover:
$65,000,000

Coverage Considerations:
e-Business Interruption, Privacy Notification and Crisis Management, Conduit Wrongful Act, Impaired Access Wrongful Act and Disclosure Wrongful Act.

A clandestine organisation hacked an administrator's network prior to a major holiday weekend and stole personally identifiable information. In addition to obtaining the names and credit card information of 25,000 customers, the organisation stole the employee data of the 250 staff members. A virus was also placed into the administrator's IT network, rendering the firm unable to conduct business for 72 hours. The administrator's clients were unable to access the network for business purposes and sustained virus related impacts to their own systems. The clients sued the administrator for impaired access and conduit related injuries.

The administrator incurred costs of $250,000 for forensic investigations, notification and monitoring measures, system restoration and legal advice. They also sustained more than $2,000,000 in lost business income and extra expense associated with the system shutdown. $300,000 in defence cost where incurred and $5,000,000 in damages where paid to customers who where unable to access the administrator's network.

Type of Organisation:
Hotel

Employees:
2,500

Annual Turnover:
$250,000,000

Coverage Considerations:
Privacy Notification and Crisis Management.

A former hotel executive gained unauthorised access to the hotel's confidential database of names and credit/debit card information of 75,000 customers as well as personal information of 2,500 employees. The information was sold to an organised crime network.

The hotel incurred more than $2,500,000 in expenses associated with the forensic investigation, notifying customers, credit and identify monitoring and restoration, public relations and regularly action defence costs. The hotel was also fined $2,500,000.

Type of Organisation:
Manufacturer

Employees:
50

Annual Turnover:
$10,000,000

Coverage Considerations:
Disclosure Wrongful Act, Privacy Notification and Crisis Management.

A manufacturer leased a copying machine for a 2 year period through a third-party intermediary. During the 2 years the manufacturer made copies of business information, including proprietary client information and its own employee data. After the lease expired the manufacturer returned the machine via the third-party intermediary. Prior to making its way back to the actual leasing company a rogue employee of the third-party intermediary accessed the machine's data and stole and sold the proprietary information.

The manufacturer incurred $75,000 in connection with a forensic investigation, notification, identity monitoring, restoration services and independent counsel fees. It also incurred approximately $100,000 in legal defence costs and $275,000 in indemnity associated with the theft and sale of proprietary client information.

Type of Organisation:
Solicitor

Employees:
55

Annual Turnover:
$20,000,000

Coverage Considerations:
e-Threat, e-Business Interruption, Privacy Notification and Crisis Management.

Hackers obtained access to a law firm's network and claimed to have access to sensitive client information, including a public company's acquisition target, another company's prospective patent technology, the draft prospectus of a venture capital client and a significant number of claimants' personally identifiable information. The firm was contacted by the hacker group seeking $10,000,000 not to place the stolen information on-line.

The law firm incurred $2,000,000 for forensic investigation, extortion related negotiations, a ransom payment, notifications, credit and identity monitoring, restoration services and independent lawyers' fees. The firm also sustained $600,000 in lost business income and expenses associated with the system shutdown.

Risk Minimisation

Businesses have become more reliant on technology to operate but it is still people and our desire to trade that creates the exposures. Yesterday's risks now manifest themselves very differently in today's digitally connected world. At Chubb we understand how to help limit your cyber exposure and insurance costs.

Simple network hygiene reduces an organisations exposure to cyber risk.

The Australian Signals Directorate suggests organisations that utilise the following 8 strategies can mitigate up to 85% of common cyber attacks.[1]

1. **Application whitelisting** - only allow selected software applications to run on computers. This can prevent all other unapproved software applications, including malware from infiltrating your network.

2. **Patch applications** - patching security vulnerabilities in software applications and keeping them up to date. A regimented patch management process maintains systems integrity. Threat actors use known vulnerabilities to target computers.

3. **Disable untrusted Microsoft Office macros** - Microsoft Office "macros" which can automate tasks should be disabled. These macros are used to automate the download of malware so should be secured or disabled.

4. **User application hardening** - block browser access to various items that are popular ways to deliver malware and infect computers, i.e. Adobe Flash player, web ads and untrusted Java code.

5. **Restrict administrative privileges** - only use administrator privileges for managing systems, installing legitimate software and applying software patches. This access should be restricted to only those that need them.

6. **Patching Operating Systems** - keep your operating systems up to date and fully patched for vulnerabilities. Threat actors will use known vulnerabilities to target an organisations network.

7. **Multi-Factor authentication** - strengthen password controls by using strong authentication with an additional "factor", such as a physical tokens or 'something you have'. Having multiple levels of authentication makes it much harder for adversaries to access your information even if the "password" is breached.

8. **Daily Backup of Important Data** - it may sound obvious but maintaining a regular backup of all data that is stored securely offline will greatly assist with business continuity should an organisation suffer a cyber attack. Don't forget to test the integrity of those back-ups!

In addition to the 8 mitigation strategies above, it is also good practice to prepare your response to a major cyber attack and update business continuity plans.

9. **Have an Incident Response Plan (IRP)** An organisation with a clear, concise and tested IRP will be able take fast action to contain a breach and minimise the financial damage to an organisation. They are more likely to have a better response to legal requirements and potential costly fines.

10. **Appoint a Chief Security Information Office (CISO)** - network and data security is an enterprise wide risk and not a risk that can be managed within the silo of the IT department. A CISO (or equivalent) should be responsible for data protection and have centralised responsibility for data management. The CISO should lead and coordinate an enterprise's response (General Counsel, Risk Management, PR/ Marketing, Executive Management) to a cyber attack. This person should be listed in the IRP.

Why Chubb?

Leadership – We have been committed to protecting organisations with content exposures for over 40 years. Our expertise allowed us to develop “all risk” coverage. What’s more, Chubb offers a full suite of complementary insurance solutions, including directors and officers liability, employment practices liability, and property and casualty coverages.

Protection – The true measure of an insurer is how it responds to and manages claims. We strive to treat each customer the way we would like to be treated if we experienced the same loss - with integrity, empathy, promptness, and fairness - and to reach mutually agreeable outcomes.

Endurance – Chubb’s financial stability and ability to pay claims rate among the best in the insurance industry, as attested by the leading insurance rating services.

About Chubb in Australia

Chubb is the world's largest publicly traded property and casualty insurer. Chubb, via acquisitions by its predecessor companies, has been present in Australia for over 50 years. Its operation in Australia (Chubb Insurance Australia Limited) provides specialised and customised coverages include Marine, Property, Liability, Energy, Professional Indemnity, Directors & Officers, Financial Lines, Utilities as well as Accident & Health, for a broad client base, including many of the country's largest companies.

More information can be found at www.chubb.com/au

Contact Us

Chubb Insurance Australia Limited
ABN: 23 001 642 020 AFSL: 239687

Grosvenor Place
Level 38, 225 George Street
Sydney NSW 2000
O +61 2 9335 3200
F +61 2 9335 3411
www.chubb.com/au

Chubb. Insured.[SM]

Chubb10-105-1117