Cyber Liability

Cover your cyber risk.

One of the biggest threats facing businesses today is the dramatic rise of cyber extortion and ransomware worldwide and New Zealand has had its fair share of cyber attacks recently. The immediate impact of a cyber attack and its flow on effects can seriously hinder a company's ability to operate. Our cyber policy provides you with the wraparound services that give you peace of mind in the event of cyber attack and the help you need to minimise the likelihood of an attack in the first place.

BENEFITS

24/7 rapid response from IT security experts in NZ

Immediately contain a cyberattack, restrict third party access & secure the perimeter of your IT infrastructure.

Value-add risk management product suite

- Baseline cyber security assessment
- Incidence Response Plan
- Targeted ransomware assessment & ransomware surveillance

Cyber risk management specialists

Tailored Claims Response

Access to our panel of expert risk management partners

- **InPhySec** – IT security, advice and forensics
- **Incident Response Solutions** – Forensic technology
- **Wright Communications** – Crisis communications & PR response
- **Centrix** – Fraud and Identity Reports
- **Cyber CX** - incident response
- **Black Kite** - assessment and identification of cyber vulnerabilities within internet ecosystems

POLICY COVER

Business Interruption
Covers your loss of profits if your IT systems are attacked, the resulting in staff unable to work or customers unable to transact.

Third Party Liability
Hacked personal information to accidentally emailing confidential information, the policy covers any resulting claims

Hacker Theft Cover
This provides cover where funds are stolen as a result of your network being hacked.

Network Extortion, Triage & Breach Consultation
When you notify a claim, we appoint an IT specialist or a law firm, depending on the nature of the breach. Our IT specialists prevent further attack, restore systems and deal with demands.

Costs to Restore
Research, replace, restore or recollect software and any electronic data due to a network attack.

Data Forensic Services
Analysis of 'root-cause' using forensic techniques.

Public Relations Expenses
Cyber breaches hit the press every day. Urgent action may be needed to manage your reputation should this happen to you.

Notification Services and Credit Monitoring
Your customers can be notified if required and their credit history monitored to prevent damage from identity theft.

Mandatory breach reporting
Covers any government or privacy reporting required & media statement preparation where relevant.

Cyber Liability Insurance

Cover your cyber risk.

STATISTICS

Ransomware remains the most prominent malware threat for business

*Source: Datto, 2020

The average ransom fee has increased from $5k to $200k

Due to COVID-19, malicious emails are up 600%

*Source: ABC News, 2021

Experts estimate that a ransomware attack occurs every 11 secs

*Source: Cybercrime Magazine, 2019

Average downtime for a company after a ransomware attack is 21 days

*Source: Coveware, 2021

60% of hacked companies had a loss of revenue after an attack

*Source: Cybereason, 2021, 2020

CYBER RISK MANAGEMENT

PRE-LOSS SERVICES

- Cyber Risk assessment & Security audits
- Endpoint detection
- Shielding services
- Crisis management strategy/ PR response
- Incident response planning / Business continuity planning
- Information security policies & procedures

CLAIMS HANDLING

	Triage and forensic investigation	Data and system restoration	Public relations and notification services	Legal support	Loss assessment
Crisis Containment	Triage – identify problem and commission resources	Prevent any attack or infection from spreading	Initial PR response	Appoint lawyers to ensure confidentiality & privilege	Assess potential for cyber loss
Crisis Management	Forensic investigation to establish extent of breach or loss	Restore system and lost data	Ongoing PR, notification to third parties, set up credit monitoring	Communicate with affected third parties	Investigate business interruption losses
Crisis Resolution		Review security & identify steps to reduce future incidents	Ongoing credit monitoring	Resolve third party claims	Quantify and settle business interruption losses

POST-LOSS SERVICES

A cyber incident may have exposed weaknesses in your cyber security or incident response plan. You might also be vulnerable to further attacks by the same cyber criminals. In the right circumstances, part of our claims response may be to assist with the cost of strengthening your cyber security (such as with shielding) and reviewing your emergency response plan.

TERRITORY

Worldwide Cover

COVERHOLDER

Coverholder at LLOYD'S