Cyber insurance

There are no boundaries when it comes to cyber crime.

Fifty six percent of Kiwi businesses experience a Cyber attack once a year[1] and the risk is growing. There are over one hundred ransomware attacks every day in New Zealand[2]. Any business that operates online is vulnerable.

Making sure you've got the right Cyber insurance to get you back up and running after a Cyber attack or breach is critical to your business survival.

Forty five percent of Kiwi companies do not have a Cyber response plan[3]. Yet, in 2015, the estimated cost of Cyber crime in New Zealand was $257 million[4].

Why should a business have cyber insurance?

No matter the size, any business that operates online or has an online presence is vulnerable to Cyber attacks and data breaches.

From viruses and hackers to employee error and system damage, your business is exposed to a range of risks that can stop you trading, impact you financially, affect your customers, and damage your business' reputation.

NZI's Cyber insurance is designed to protect your business against a number of these Cyber exposures. It provides cover for direct costs to your business as well as claims from third parties, and also covers expenses with defending Cyber claims, such as legal costs.

NZI Cyber insurance also provides you with access to a 24/7 emergency helpline and a Cyber Expert team.

When you have a Cyber issue simply call **0800 NZI CYB**. We'll assess your situation and provide you with access to a panel of Cyber experts including IT, legal and forensics experts. This panel will work with your team to proactively manage and resolve the situation, to get you back up and running as fast as possible.

Our Cyber Ultra policy will also provide you with access to a Public Relations expert to help mitigate any reputational damage to your business.

[1] Colmar Brunton Cyber Security NZ SME Landscape 2014

[2] Symantec Internet Security Threat Report, April 2016

[3] PwC – Global Economic Crime Survey 2016

[4] New Zealand's Cyber Security Strategy 2015

NZI offers two Cyber polices. From basic coverage under Cyber Base, to more extensive protection under Cyber Ultra.

NZI Cyber Base policies can provide cover for:

- **Privacy**
  Your liability following loss of personal or commercially confidential information lost, damaged or destroyed data, as well as defence costs.
- **System damage**
  The costs required to restore or replace lost, damaged or destroyed computer records and the costs of retrieving, repairing, restoring or replacing computer systems following a cyber event including for example a hacking attack or virus, malicious damage or operational error.
- **Computer virus, transmission and hacking**
  Your liability to any third party that suffers financial losses from hacker attacks, or viruses that come from or pass through your computer system, as well as defence costs.
- **Multimedia liability**
  Your liability as a result of any invasion or interference with privacy or infringement of copyright, trademarks or trade names arising from your internet or email content, promotional material or digital content downloaded, shared or distributed from your computer system, as well as defence costs.
- **Extortion**
  Payment of ransom or costs associated with negotiating a cyber extortion attempt (please note, payment of cyber extortion costs is subject to local legal requirements and cooperation with appropriate authorities).
- **Privacy breach notification and loss mitigation**
  Costs incurred in respect of a breach of privacy obligations following a cyber event, for example call centre support, credit monitoring, independent audit costs.
- **Privacy fines and investigations**
  Fines or penalties you incur due to a privacy breach as well as defence costs or regulatory investigation defence costs.

In addition to the above, Cyber Ultra can provide cover for:

- **Business interruption**
  Loss of profits suffered if your business is disrupted due to a cyber event.
- **Computer crime**
  Loss due to transferring or paying funds in error as a result of a fraud in connection with either your own or another party's computer system, including a fraud perpetrated by a rogue employee.
- **Brand and personal reputation protection**
  Public relations consultancy costs to protect your brand and reputation including the reputation of any of your directors or officers following a claim or cyber event covered by the policy.
- **Breach of Statutory Duties relating to e-commerce**
  Your liability as a result of a breach of any statutory duty relating to the security or management of information in the course of e-commerce.
- **Social Engineering Fraud**
  Phishing, Phreaking and Fake Invoice losses are an increasing global trend in cyber-crime. Protect your business from these types of fraudulent losses with this additional cover.

Please note this is only a summary of the benefits, they are subject to exclusions and limitations. Please see the full policy wording for full details.

Call your broker | nzicyber.co.nz

Claims examples

Financial advisory practice hit by malware attack.

The business

Cha-Ching NZ (Cha-Ching) is a large financial advisory practice offering advice in personal financial and retirement planning, operating across the country.

The Cyber attack

Cha-Ching's Auckland IT system incorporates a single server and eight laptops for the staff employed at the branch. The laptops are a mixture of the insured's equipment and employees' personal computers. Cha-Ching's company-provided equipment (workstations and servers) runs ESET Endpoint Anti-Virus and Microsoft Essentials, which should provide sufficient protection against the type of intrusion which gave rise to this incident. However, employee-owned equipment has inconsistent levels of security.

How NZI responded

Cha-Ching informed their broker of the cyber breach by email on the day it was discovered. The broker contacted insurers and followed this up with the email notification from the insured. NZI immediately made contact with Cha-Ching when we were told that FYMB, Cha-Ching's IT provider, had rebuilt their files from backup data and that all systems were up and running.

Cunningham Lindsey appointed a forensic IT specialist on behalf of insurers and had them contact FYMB to obtain a detailed technical briefing on the breach. Cunningham Lindsey then contacted Deloitte for assistance. Deloitte contacted FYMB to discuss the breach, determine the point of entry, confirm that the clean-up had been satisfactorily completed, and to establish what steps had been taken to minimise the possibility of future breaches, suggesting improvements where necessary.

Deloitte's review of FYMB's work confirmed that the actions taken by senior staff in triaging and resolving the problem were satisfactory. We established that FYMB had searched for infected files, but found nothing further. It is thought that all other machines that were linked to the network at the time of the intrusion were running with ESET Smart Security. FYMB also checked server logs but found no evidence of further activity, suggesting that the malware was not operating on the server. Anti-virus scans were run on all company-owned machines. Nearly 1,600 infected files, including the Dropbox backup which was auto-synced, and email in question were deleted from the system, and then restored from backup in unencrypted format. Fortunately, the swift action of FYMB saw minimal disruption to the insured's business.

Cost of the claim

The total cost amounted to approximately $13,000.

Online vendor claims after being hacked.

The business

Nuke-it Appliances (Nuke-it) is a vendor of kitchen appliances throughout New Zealand.

The Cyber attack

The client was notified by its web-hosting provider, Hostinator, that its website had been hacked. Hostinator advised the client that they viewed logs and confirmed the website was being used to send spam emails. They suspended the site and instructed the insured to contact a web developer to clean the site.

How NZI responded

Nuke-it immediately called Cunningham Lindsey who in turn contacted Deloitte for assistance. Deloitte investigated and found source of the spam was a fairly common malicious file called "list.php" which contains code required to launch the spam attack. Data logs showed that the attack was launched at 6.40am one morning and lasted around 5 hours. The attack was launched from multiple IP addresses indicating that the attacker was operating through a set of "proxy" servers, to mask their identity. Deloitte advised that the website had been unmanaged in regards to security, patches and updates that meant it was vulnerable to attack. Deloitte immediately redirected the original URL to a sister company in order to minimise disruption and potential loss of business.

Deloitte were able to repair the website and have it back online in the same day they received agreement from Nuke-it to do so and continued to perform spot checking of the website content and logs over the following 7 days. In that period they found only regular scanning and basic credential exploitation attempts (i.e. users unsuccessfully trying to login in to interfaces using default credentials) – all of which is common place for a website on shared hosting. They discovered that someone had already commenced trying to exploit a new critical vulnerability by adding an unauthorised administrator account. Fortunately, because Deloitte identified the critical weakness in the software and subsequent breach of it, they were able to swiftly remedy this and did so free of charge.

When handing full control back to Nuke-it, Deloitte also recommended that they ask their IT vendor to update and maintain the site as new patches are released, and to move the site hosting to a comparably priced but improved hosting provider.

Cost of the claim

The total cost amounted to approximately $16,000.

To find out how much NZI Cyber insurance could cost your business, get an easy online estimate: nzicyber.co.nz/get-an-estimate

NZI is a business division of IAG New Zealand Limited.

Call your broker | nzicyber.co.nz

NZI