NZI CYBER INSURANCE

CYBER CLAIMS

See how NZI Cyber insurance has helped real Kiwi businesses.

For more information on how NZI Cyber insurance can protect your business and to get an estimate visit nzicyber.co.nz

The following claims examples are based on real claims however some details have been changed and fictitious business names have been used.

CASE STUDY

FINANCIAL ADVISORY PRACTICE HIT BY MALWARE ATTACK

A large financial advisory practice was left unable to operate when a virus compromised thousands of highly important files. The source was deemed to be an infected email accessed by an unsecured laptop. NZI and partners were able to restore the system with minimal impact to the business.

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 cleanup 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

Amounted to approximately

$13,000

CASE STUDY

ONLINE VENDOR CLAIMS AFTER BEING HACKED

An online vendor of high-end restaurant equipment was notified by its hosting provider that the their website had been compromised. NZI and partners were able to mitigate the damage by suspending the site, redirecting traffic to a safe partner site and recommending better practices for the future.

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

To date have amounted to approximately

$16,000