CYBER EXPLAINED

How exposed are you?

Although technology has improved the way that organisations of all types run their day-to-day business, its growth has bred an entirely new set of risks. But while hack attacks, data breaches, and cyber crime might seem like problems that only large corporates face, that is quickly changing. In fact, the majority of attacks today are on small and medium-sized enterprises that lack the infrastructure to prevent such attacks as well as the economic stability to absorb the costs associated with the fallout.

That's why having robust cyber insurance in place is a must. Designed to sit alongside good network security guidelines and practices, our cyber policy provides well-rounded and flexible cover that works for a wide range of businesses and covers you should the worst happen. Talk to your broker today to find out more about what kind and levels of protection are suitable for your company.

Cyber risk in numbers*

Major data breaches at companies like Sony and Target may make the headlines, but it's the attacks on average businesses that reflect the reality of cyber crime. In the last year alone....

60% of all targeted attacks struck small and medium-sized organisations.

23% was the percentage increase in data breaches on the previous year.

1 in 244 emails contained malware.

17% of all Android apps were actually disguised malware.

113% was the percentage increase of ransomware attacks, one of the fastest growing crimes globally, on the previous year.

* Numbers acquired from the 2015 Symantec Internet Security Threat Report

Cyber claims examples

A company accountant of a Sydney manufacturing firm received an email from her boss asking her to transfer $120,000 to a supplier abroad. Because this was a common type of request, she processed the payment before realising that the tone of the email wasn't right and the domain name was a single letter off. Upon further investigation, it was found that cyber thieves had infiltrated their systems and grew knowledgeable enough about company dealings to send a convincing phishing email that lost the company thousands. Our policy would cover the costs associated with phishing scams under the cyber crime clause of the policy.

A director of a medium-sized healthcare firm in Brisbane received an email one day from an unknown individual who claimed that he had breached the company's systems and was holding confidential patient data which he would release to the public unless the company paid 25 bitcoin (approximately $7,500). Our claims team would first help identify that this was a credible threat and then work closely with the company to determine if paying the ransom would be the best course. Ransom payments in this type of instance would be covered under the cyber threats and extortion section of our policy.

A furniture store based in Melbourne was the victim of a significant data breach after malware had been unknowingly installed on some of its in-store payment systems. Evading anti-virus software and present on the system for many months, this resulted in the loss of nearly 20,000 customer credit card details. The company faced a large bill after it had to launch a forensic investigation and pay for PCI-related fines and card brand assessments. Our policy would cover these under the privacy liability clause.

A unencrypted laptop belonging to an employee of a charity was left on public transportation. It contained the personal details of nearly 5,000 donors. Conscious of the need to protect its brand and reputation, the charity decided to voluntarily notify those affected. Our cyber policy includes voluntary notification for privacy breaches such as this, as well as notification required by law.

A small accountancy firm found their entire network riddled with malware after a temporary worker accidentally clicked on an infected link. In order to fix the problem, they had to hire a specialist team of IT forensic consultants that had to rebuild their system and restore data at cost of $45,000. Our policy would cover the external costs associated with restoring, repairing and rebuilding systems after hack attacks, viruses and employee errors under the system damage section of the cyber & privacy clause.