CYBER ATTACK

It's just a matter of time

Mandatory Notification of Data Breaches

With the introduction of new legislation on 22 February 2018 organisations now face greater scrutiny than ever before, especially with more businesses using the "Cloud" to conduct transactions. Failure to comply can result in penalties up to $360,000 for individuals and $1.8 million for organisations.

Amended Privacy legislation and increased publicity around cyber attacks, brings a heightened awareness of privacy and cyber exposures. The numbers are alarming with more than 20% of Australian businesses experiencing cyber crime and 40% of all attacks directed at SME's.

Cyber Liability and Privacy Protection

The risks to an organisation from handling personally sensitive information continues to grow. The recently introduced legislation provides more protection to individuals and imposes stringent reporting regimes and remedies that must be complied with.

Cyber insurance protects your business against the expenses and legal costs associated with data breaches, which may occur after being hacked or from theft of client information. The treatment of sensitive and personal information should be at the forefront of every business operator, as a data breach may not only cause reputational risk but dramatically impact your income and so much more.

What does a Cyber insurance policy cover?

A typical Cyber insurance policy is designed to provide protection when there is a breach of your IT systems resulting in loss of your, or someone else's information, and offers coverage for a range of first-party and third-party losses.

First-party coverage generally includes:

- IT System restoration and remediation
- Business Interruption
- Forensic investigation and data recovery
- Extortion
- Crisis management and PR

Third-party coverage generally includes:

- Regulatory defence expenses
- Litigation expenses
- Notification costs
- Monitoring
- Communications and media liability

Whilst prevention is key, without a Cyber insurance policy, you may not have the resources to manage a data breach. Cyber insurance includes protection across the following areas:

• Privacy Liability	A failure to maintain confidentiality of data
• Network Security Liability	The unauthorised use of your networks
• Media Liability	Your online media liability
• Cyber Extortion	Network or data extortion / blackmail
• Data Asset Loss	Data loss and restoration including decontamination and recovery
• Business Interruption	Due network security failure or attack

EBM

1300 INSURE (1300 467 873) | F: 1300 365 822 | ebm@ebm.com.au | www.ebm.com.au
New South Wales | Victoria | Queensland | Western Australia | South Australia
Coverholder at Lloyd's | GBN Worldwide | Asia Australasia Alliance | National Insurance Brokers Association
Elkington Bishop Molineaux Insurance Brokers Pty Ltd | AFSLN 246986 | ABN 31 009 179 640 | Est 1975

"Cyber crime is the greatest threat to every company in the world."
Ginni Rommety, CEO IBM

What would you do if you experienced a Cyber Attack? Is your IT provider experienced to respond quickly?

Some additional benefits of cover under a separate Cyber insurance policy:

- Incident response and investigation costs
- Crisis management support via incident reporting hotline (open 24 hours, 365 days of the year) and local vendors
- Legal costs in defence and investigation
- Regulatory fines, penalties and defence costs

Cyber Liability Claims Examples

Any company	Stolen or lost laptops, lost paper files and USB network security breaches represent a significant concern. • At least 31% of laptops store sensitive information in unencrypted format. • Only 7% use some form of anti-theft feature.	Average cost of a stolen/lost laptop is $49,000. Rising up to $115,000 if recovery is delayed. Hardware cost is insignificant compared to other factors including recovery of sensitive information, detection and escalation costs, intellectual property loss, productivity impact, business interruption and legal/regulatory costs. Research suggests 85% of customers are likely to take their business elsewhere and 47% would take legal action.
Travel agency with four locations, $10M turnover and 30 staff	The Insured experienced three separate data breaches over a three-year period in which hackers gained access to the Company's computer system. Over 250,000 individuals' credit card information and passport details were compromised.	$1,750,000 was paid for the forensic and legal costs in defending the investigation brought by the regulator and the cost of notifying the affected individuals including providing credit monitoring services.
Not for Profit	The Insured was targeted with a denial of service attack (floods a targeted system with incoming web traffic until it is virtually crippled) in the last few days of a fundraising campaign. People were unable to make donations for a day while the website was being fixed.	$1,500,000 paid for the lost donations and rectifying the damage to the Insured's website.
Online retailer with turnover of $5M and 15 staff	Hackers defaced the Insured's website inserting links to a competing retailer, as well as gaining access to personal information of their customers.	$800,000 was paid for loss of income, cost to repair the website as a result of the hack, defence costs for regulatory actions by the Privacy Commissioner, and costs of notifying the affected individuals including providing credit monitoring services.
Healthcare network	A part-time employee of a healthcare provider stole a computer that still contained prescription records including names, address and medication lists.	$1,200,000 paid for the forensic and legal costs in defending the investigation brought by the regulator and the cost of notifying the affected individuals.
Medical Clinic	The loss of a physician's unencrypted, password free mobile phone in a taxi resulted in the exposure of patient names, date of birth, social security numbers, diagnosis information and test results.	$700,000 paid for the cost of notifying the affected individuals and defending the investigation brought by the regulator.

Protection for your business against Cyber Attack starts with prevention. Your EBM broker can provide a Cyber Security Checklist to offer some guidance in this area, together with insurance options designed to protect against various cyber exposures including crisis response.

Call us on 1300 INSURE (1300 467 873) to speak to an EBM broker.
Visit www.ebm.com.au/cyber-liability/ to find out more and to download our Cyber Security Checklist.

EBGEA4089-190607