ARE YOU COVERED AGAINST A CYBER ATTACK?

If you think the threat of cyber attack isn't relevant to your company, think again. The latest government statistics reveal that almost 700,000 organisations have experienced a cybercrime – and of those companies attacked, 60% were small to medium sized businesses*.

Even the most robust of IT controls won't ensure you're 100% immune from being hacked. That's why a cyber insurance policy is crucial. The experienced professionals at Edgewise will take the time to understand your specific risks in cyberspace.

We'll then ensure your policy covers these risks – from direct business losses, to any legal liability you may have to your customers or other third parties.

*Australian Government stay safe online infographic

DON'T LET HACKERS DESTROY THE COMPANY YOU HAVE WORKED SO HARD TO BUILD

PROTECT YOUR PROFITS FROM CYBER EXTORTION

Protect your profits from the costs of cyber extortion, including ransom payments and fines if a Privacy Act breach occurs.

BENEFIT FROM CUTTING-EDGE COVER

We only work with insurance companies who are experts in cyber insurance – so you can be confident that you're receiving state-of-the-art cover.

ENSURE YOUR COVER KEEPS UP WITH CYBERSPACE

Hackers are constantly coming up with new ways to break into systems. That's why we review your cover regularly – ensuring you're protected against any new and emerging threats.

EXPERIENCE AN EMPATHETIC CLAIMS PROCESS

We hope you'll never experience a cyber attack – but if you do, we'll support you through the claims process and help minimise any disruption to your business.

edgewise insurance brokers

TAKE CARE OF YOUR REVENUE, OPERATIONS AND DATA – AND YOUR REPUTATION

At Edgewise, we understand that every business is different. That's why we tailor your cover to protect you against your company's specific cyber-risks. Depending on your situation, your policy could cover you against:

CYBER EXTORTION
Which could include costs like paying extortion demands, hiring negotiation experts and safeguarding your company from a future attack.

BUSINESS INTERRUPTION LOSS
If your business is unable to operate due to a cyber attack.

REPLACEMENT OF ELECTRONIC DATA
If you need to replace vital records and other business data.

ELECTRONIC MEDIA LIABILITY
Which could cover you against the risk of copyright infringement, defamation claims and misuse of some intellectual property online.

SECURITY AND PRIVACY LIABILITY
which covers damage to your reputation, if third-party data in your system ishacked.

REGULATORY BREACH LIABILITY
If you need to pay fines or pay legal fees due to a government regulator investigation.

COSTS OF NOTIFICATION AND MONITORING EXPENSES
If you have to inform your customers of a security breach and monitor their credit cards to protect them from further attacks.

CRISIS MANAGEMENT EXPENSES
For the cost of managing a crisis caused by a cyber attack.

RECENT REAL-LIFE CASE STUDIES: THE TRUE COST OF BUSINESS CYBER CRIME

A SOLICITOR'S FIRM

Hackers managed to access a large law firm's network, claiming to have access to sensitive client information. The hackers demanded a $10 million ransom payment or they would put the stolen information online.
The law firm, which employed 55 people and had a turnover of $20 million, had to pay out $2 million for forensic investigation, extortion-related negotiations, a ransom payment, notifications, credit and identity monitoring, restoration services and independent lawyers' fees. The firm also sustained $600,000 in lost business income and expenses associated with the system shutdown.

A THIRD-PARTY ADMINISTRATOR

An administrator with 50 employees and a turnover of $65 million was hacked just before a major holiday weekend. The hackers stole the names and credit card information of 25,000 customers and the employee data of the 250 staff members. They also placed a virus into the administrator's IT network, halting its business for 72 hours.
The administrator's clients were unable to access the network and sustained virus-related impacts to their own systems – so they sued. The administrator had to pay $250,000 for forensic investigations, notification and monitoring measures, system restoration and legal advice, and $300,000 in defence costs. The loss to the business and system shutdown cost them $2 million, and they paid $5 million in damages to clients.

A HOTEL

A large hotel with an annual turnover of $250 million was hacked by a former hotel executive.
The ex-staff member gained unauthorised access to the hotel's confidential database of the payment card information of 75,000 customers – plus the personal information of the hotel's 2,500 employees, and sold this information to an organised crime network. The hotel was fined $2.5 million, and spent a further $2.5 million on investigation, credit and identity monitoring and restoration, public relations and defence costs.

PROTECT THE FUTURE OF YOUR BUSINESS BY CONTACTING US TODAY

Get a no-obligation quote today, or get in touch to discuss your cyber cover needs with your Edgewise account manager.

+61 3 9425 1333 email@edgewise.com.au +61 3 9425 1399 edgewise.com.au