EBM
Insurance & Risk

Cyber Security

ebm.com.au

The reality of a Cyber security risk

All businesses can be affected

Cyber events can impact any company, regardless of size and industry. Events can be targeted, employee mistakes can be made, or collateral damage losses can be experienced from a wider event.

In 2020, the most common attacks were business email compromise, ransomware and data theft. With the general public more responsive to messages regarding COVID-19, pandemic related scams have also appeared.*

You don't have to be the target to be affected

Cyber-attacks can spread through your suppliers or your outsourced technology providers, leading to significant impact even when you aren't the target.

Responding to legislation

Australian Privacy regulations have increasingly higher standards and penalties. Failure to comply with the Notifiable Data Breaches Scheme can attract fines of up to $420,000 for individuals and up to $2.1 million for organisations. A Cyber Insurance policy is designed to protect your business against the expenses and legal costs associated with data breaches.

Complement to existing IT teams

A Cyber Insurance policy may complement the effectiveness of IT security teams – it supplements their skills and can protect your business from the unknown.

Are you sure you are already covered for cyber risks?

Traditional insurance policies may be inadequate to respond to cyber exposures

A Cyber Insurance policy is specifically designed to address these gaps. Data is one of the most important assets (and is also among the most vulnerable), yet it is generally not covered by standard asset/property insurance policies.

Liability arising from the loss or misuse of sensitive data is only one potential outcome of a cyber event. Business interruption, incident response, and recovery costs make up a significant portion of claims payments, even without liability claims.

Cyber Insurance policies are designed to cover response and recovery expenses (not just data compromise) and generally include:

- Incident response and investigation costs
- Crisis management support via 24-hour incident reporting hotline
- Legal costs in defense and investigation
- Regulatory fines, penalties and defense costs.

*Source: Office of the Australian Information Commission - Notifiable Data Breaches Report: July-December 2020

EBM
Insurance & Risk

Cyber Security

ebm.com.au

Examples of Cyber Insurance policy claims

Unauthorised access to network

A legal firm's network was hacked by an unknown source that gained access to sensitive client information including lists containing personally identifiable information (PII). A forensic technician hired by the legal firm determined that malware had been planted in the network. After the hack, the legal firm received a phone call from the hacker seeking a payment of $10m to not place the stolen client information online.

Impact

With no Cyber Insurance policy in place, the legal firm incurred $2 million in expenses associated with the forensic investigation, extortion-related negotiations, ransom payment, notification, credit and identity monitoring, restoration services and independent counsel fees. It also sustained over $600,000 in lost business income and expenses associated with the system shutdown.

Website rendered inaccessible

During a fundraising campaign, a charity's website was targeted with a denial of service attack, crippling the functionality of the site. This made it impossible for people to make online donations during the final days of the fundraising campaign.

Outcome

In this instance, their Cyber Insurance policy kicked in and the charity received a payment of $1.5m for the lost donations due to the attack, and to rectify the damage to the website.

Employee illegally accessed client and employee data

During a 2-year period, a business that leased a copying machine made copies of proprietary client information and employees' details including driver's license numbers and other personal identifiers. After the lease expired, an intermediary company collected the machine to return to the leasing company. Prior to the return, a rogue employee accessed the machine's data to use for illegal purposes.

Impact

With no Cyber Insurance policy in place, the business incurred $75,000 in expenses from the forensic investigation, notification, identity monitoring, restoration services and independent counsel fees, along with $100,000 in legal fees.

Ransomware attack

A medical practise realised their computer system had been compromised by a ransomware attack, and found they couldn't access any patient medical data on the system for over a week.

Outcome

In this instance, the medical practise's Cyber Insurance policy was triggered, and the insurer sent an IT Forensic Consultant to remediate the system, and confirm the hacker(s) were no longer active. The insurer also appointed a legal firm to process and advise on the potential breach of information by the practise to the authorities. An assessment of the Business Interruption was also provided to the Insured. The practise received $160,000 from their cyber policy cover.

EBM
Insurance & Risk

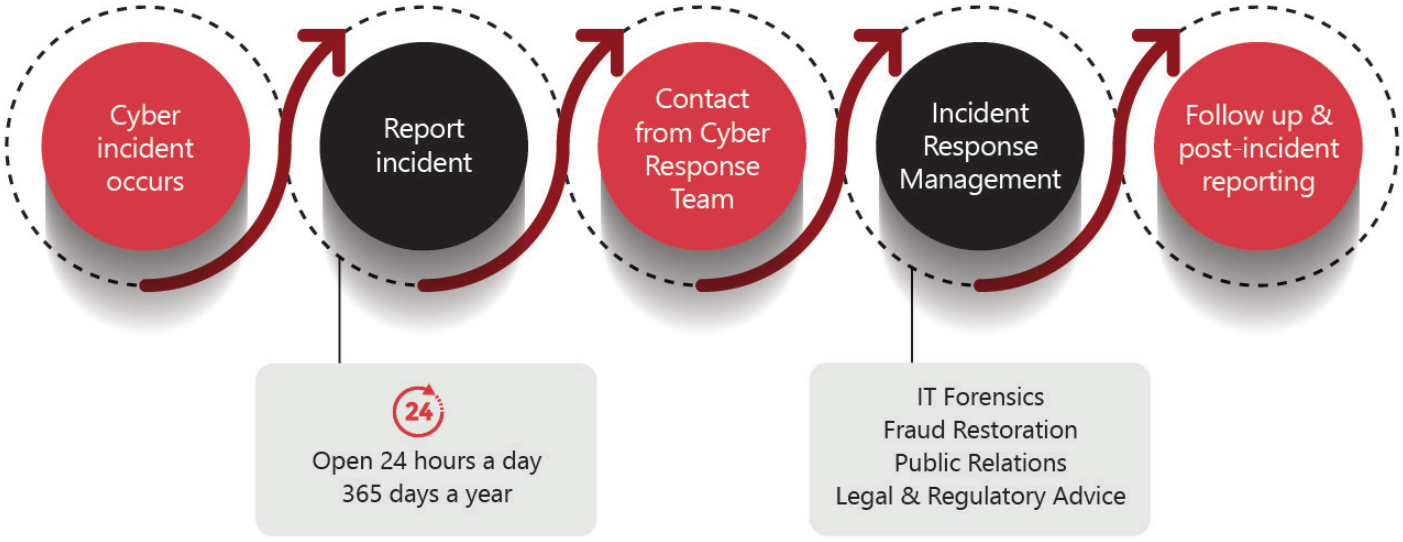
Cyber Security

ebm.com.au

What does a typical Cyber Incident Response Plan look like?

Cyber Incident Response Services can help your business:

- Act quickly to contain the threat and limit potential damage to your business
- Meet the obligations under the Australian Privacy Act
- Limit the consequences of a data breach
- Preserve and maintain public trust.



Contact EBM on **1300 755 112** or visit **ebm.com.au** for more information.

Elkington Bishop Molineaux Insurance Brokers Pty Ltd
AFSLN 246986 | ABN 31 009 179 640
National Insurance Brokers Association | Coverholder at Lloyd's
GBN Worldwide | Asia Australasia Alliance

EBM3-210526