cyber liability INSURANCE explained

What is a cyber liability insurance?

In simple terms, Cyber Liability insurance, also known as Data Breach insurance, helps your business to cover the costs associated with a cyber-attack or data breach incident on your computer systems - including the loss of your own profits and claims from third parties, like your customers.

Who should consider it?

Any business with or without an online presence is at increasing risk of a cyber-attack. Data is valuable and cyber related crime is increasing exponentailly year on year.

Geographic location is no barrier for a hacker and small businesses are considered easy targets. It is now thought that an Autralian buisness suffers some form of cyber crime related attack every 8 minutes.

With the average cyber incident costing $280,000 in customer notification costs, extortion costs and ransoms, potentially being sued by customers or employees for the loss of personal information - not to mention colossal fines; a Cyber Laibility insurance policy is worthy of consideration. A $280,000 loss to a small business could be catastrophic.

What risks can this type of policy cover?

Insurer's policies do vary, but basically a good quality Cyber Liability policy should cover:

- lost revenue because of a security breach or cyber incident,
- ransom costs,
- the IT cost to recover, 'unlock' or rebuild your data,
- defence costs for legal claims,
- government regulator investigation costs and fines,
- crisis management costs,
- forensic investigation costs,
- hefty customer notification and imposed monitoring costs if the breach was significant or'reportable', and
- civil action costs from third parties affected by a breach of your systems.

What is cyber crime?

Cyber crime is defined as any crimial acivtiy that is carried out via a computer or the internet. The most common types of cycber crime experienced by Australian businesses include:

- email scams and email compromise,
- socal engineering,
- theft of money via fraud,
- theft of financiall or sensivite data including identiy theft, and
- cyber extorion

What is a data breach?

A data breach occurs when personal information is accessed and disclosed without authorisation or is lost.

Examples include:

- a mobile phone that holds an individual's personal information is stolen,
- an individual's personal information is sent to the wrong person, or
- the hacking of a database containing personal information.

A business has 30 days from the time it becomes aware of a data breach to investigate whether the incident is an eligible data breach and report the breach if required to the OAIC. (Office of the Australian Information Commissioner). Failure to act could see fines and penalties be applied by the OAIC. At $360,000 for individuals and $1.8 million for companies it can be an expensive exercise.

A Cyber Liability Policy has a forensic assessment component designed to investigate a breach for you, so you know where you stand enabling you to act on your obligations.

cyber liability INSURANCE explained

Common misconceptions about this risk

No.1 **Businesses that don't have a website are not at risk.**
Not true. Your business may not have a presence online in the form of a website, but it is likely that you use a computer or mobile device and an internet to transact banking and manage invoicing - both of which involves sending and receiving important sensitive information.

It is worth noting that emails are also cited as one of the most common ways in which a system breach or cyber-attack can occur.

No 2 **My data is safe in the Cloud - I'll just reinstall it if I'm hacked.**
Ok,that might work, but your business is legally responsible for the information that it stores in the 'cloud'. A breach (illegal access) of this information could result in a business incurring significant imposed notification costs, remediation and investigation costs and in some cases, civil litigation costs or fines if the breached or stolen information is considered sensitive.

It is also worth noting that many hackers have been poking around in targeted systems for a significant period of time before they actually do anything to comparmise a system. It is unlikley a previous backup of your data is clean. Wiping and reloading is not always a guaranatee of having rid youself of the problem.

No 3 **We don't hold any sensitive information.**
That's very unlikely. Your business probably holds information that is sensitive regardless of your business activities.

Bank account information of suppliers, customers and employees, employee dates of birth and tax file numbers or work cover claim details, ethnic or religious origins, tracked GPS locations via vehicle monitoring software and individuals' facial photos like those on a Drivers Licence are all examples of sensitive information and fetch a tidy sum when sold of the dark web for crimial purposes. An idenity can be stolen or misused with surprising little information.

No 4 **We can't get hacked.**
Not true. No system is 100% safe or protected. If the likes of CommBank, Facebook, Sony and more recently Optus, Telstra, and Medibank Private with endless cyber security budgets and resources can be hacked it is fair to say that the average small business is vulnerable too.

Hackers see small business as attractive easy targets with lots of valuable data. Cyber security beaches don't always involve a hack of your systems. An unsecured device, like a phone or tablet that is misplaced or stolen can leave your systems extremely vulnerable.

Getting a quote

Getting a quote is quick and easy. Visit our website, www.reefib.com.au and navigate to the Business Insurance page to complete a quick online quote request or call us for a chat on 0473 007 606. Typically, we only need a few details about you, your I.T. systems and your business to provide a quote.

Reef Insurance Brokers
Po Box 750 Bungalow Q 4870
Po Box 962 Ravenshoe Q 4888
Ph: 0473 007 606
Email: hello@reefib.com.au