



An introduction to Cyber Liability Insurance Cover

Are you a small business owner?

If your company retains or stores sensitive personal data, your company could be financially ruined if that data is compromised. Consider for example 80% of your company's sales are via credit card and hackers gained access to your company's computer system. Privacy is breached, \$1,750,000 is incurred for the forensic and legal costs in defending the investigation brought by the regulator and costs associated with notifying the affected individuals including providing credit monitoring services.

You might think that's a worst case scenario, but what if the hackers held you ransom with all your company's data in exchange of a large cash payment. Could you afford to pay these costs? Also, don't forget the loss of business while your website is down, dealing with this situation.

Data breaches are now a fact of life, but how can you better manage the risks related to a data breach and reduce the significant cost that can result from them? One options is to buy insurance, Cyber Liability Insurance.

Cyber Liability Insurance Cover can include:

Privacy Protection - Protection for third party liability in the event of a data breach, including civil penalties and compensatory awards levied by regulators)

- Includes cover for breaches caused by others acting on behalf of the Insured (including subcontractors)
- Includes cover for electronic and non-electronic incidents such at phishing or social engineering

Breach Costs – payment for the costs associated with responding to a breach of personal information, by the Insured or anyone acting on behalf of the Insured (including subcontractors)

- Forensic investigations (including PCI forensic report)
- Notification costs (individuals and regulators)
- Credit monitoring services
- Call centre costs
- PR costs

Cyber Business Interruption - Compensation for lost or reduced revenue.

Cyber Liability – Liability cover as a result of content in email, on the intranet, extranet or website. Including alternations and additions made by a hacker.

Hacker Damage – Reimbursement for costs to repair, replace or restore systems and data as a result of a hack. Hacker includes an employee of the Insured.

Cyber Extortion – Payment of ransom demands, and specialist consultant fees, where a hacker holds, or threatens to hold your website, extranet, intranet, network, programs or data to ransom.

Should I be concerned?

More than 20% of Australian businesses experienced cyber crime in 2012 and 40% of all attacks were directed at SME's.

SME's should also be aware new Privacy legislation was introduced effective March 2014, with penalties of \$340,000 for individuals & \$1.7 million for companies, for breaching the legislation.

Cyber Liability on a large scale – The Sony example

An example of a Cyber security breach on a large scale and the story that received the most media attention was Sony's Playstation Network (PSN) which was hacked in April 2011. This caused their network to be offline for several weeks. Account names, birth dates, email addresses and credit card numbers had been compromised.

The regulator had fined Sony US\$425,397 labeling it as a "serious breach of the Data Protection Act" due to the account information leak, and said it "could have been prevented."

Following the security breach, 65 class action complaints were filed and later became a Consolidated Class Action Complaint (CAC) in the United States. In addition to a \$15,000,000 settlement, Sony provided a "welcome back package" with free games for PSN users.

What have we learnt from Sony?

The Sony incident will go down in history as one of the gaming world's biggest fiascoes, so what can you as a business learn from Sony's story?

- Even large corporations are vulnerable.

Sony was a pioneer in technology, but it proved just as vulnerable to attacks as your average company.

- Minimise information that is shared.

Too many companies, Sony included, ask for information they don't really need. Optional fields are best left blank.

- Sometimes it's out of your hands.

Sony's breach proves that even the most vigilant users can be harmed through no fault of their own.

- There's no comfort zone.

It's when you fall into a sense of security ("it won't happen to me") then you're most vulnerable to data theft.

- Cloud computing, the future.

After the Sony fiasco, will users still be comfortable putting so much of their professional and personal information online?

- Your antivirus isn't enough.

Bolster your online arsenal with web-security software. These programs encrypt all communication from your computer, so that anything that's stolen will be useless to the thief.

- Threats to your financial identity exist where you least expect it.

Playing a game of Portal 2 may be the last place you'd expect criminals to lurk, with banking and government sites carrying much more sensitive information. But as it turns out, hackers don't discriminate.



How do I apply for cover?

Complete a few simple questions via the below link and we will provide a quotation within 24 hours.

<https://mibrokers.wufoo.com/forms/mib-cyber-liability-quote-form/>