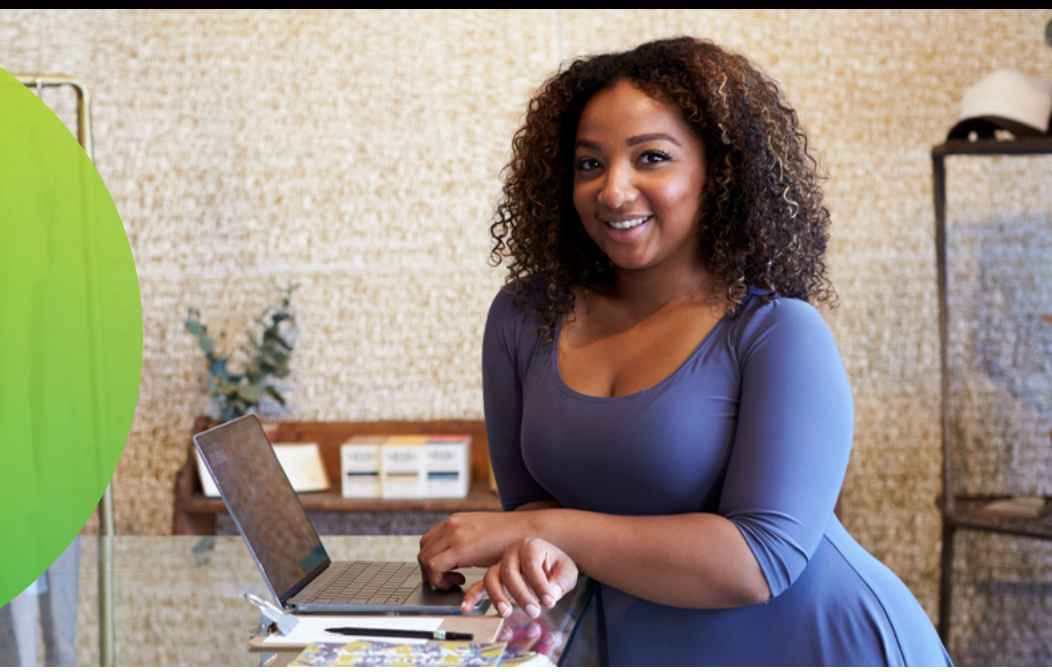
BizCover

NATIONAL NEIS ASSOCIATION INC.

Cyber Liability Insurance *fact sheet*

June 2018



Cyber Liability in a nutshell

If your business is targeted by cyber criminals or suffers a data breach, Cyber Liability insurance will assist in managing incidents from initial notification through to resolution.

The low-down

Cyber Liability Insurance protects your business against the expense and legal costs associated with data breaches which may occur as a result of being hacked, or from the theft or loss of client information.

It provides cover for third party claims (for action taken against your business such as clients suing for breach of privacy, or action taken by the Privacy Commissioner) as well as first party cover to protect against the expenses your business incurs following a cyber attack, such as the costs of repairing and restoring your systems.

Do I really need it?

Almost every business, big and small, handles some form of important data which can be easily compromised. It could be sensitive information on your customers or clients; details about your staff; crucial information about your business such as your budgets, sales data, marketing plans and suppliers details; or credit card and bank account details. If your business stores any of these forms of information electronically, or you have a website, it is at risk of becoming a victim of a cyber attack or data breach.

An attack on your business could cost you more than a large sum of money and an even larger headache. It has the potential to jeopardise your intellectual property, ruin your reputation and put you out of business.

To understand if a Cyber Liability policy would be beneficial to your business, ask yourself the following questions:

- How valuable is your data? Do you store private or commercially sensitive information about your clients, suppliers or your own business?
- How robust is your IT infrastructure? Is it up-to-date with the latest anti-virus protection software?
- Are you and your employees adequately trained on what to be aware of, how to prevent a cyber incident from occurring, and recognising when a data breach has occurred?
- Do you have sufficient resources and an incident response plan to manage a potential cyber breach?

What is typically covered?

First Party Costs
Covers the costs associated with responding to a cyber breach incident, including:

- IT forensic costs
- Data recovery costs
- Cyber extortion costs (including ransom demands from hackers)
- Credit monitoring costs
- Notification and public relations costs
- Legal representation expenses

Third Party Losses
Covers your liability to third parties following a data breach, including:

- Claims for compensation
- Legal and defence costs
- Costs arising from investigations by a government regulator
- Fines and penalties for breaches of the Privacy Act

Business Interruption
Covers lost profits as a direct result of a cyber security breach, including:

- Loss of income and expense reimbursement
- Additional necessary expenses required to continue business as usual

What isn't usually covered?

- Bodily injury and property damage
- Prior known facts or circumstances
- Intentional, criminal or fraudulent acts
- Damage to computer hardware
- Upgrading or replacement of an application, system or network
- Failure or outage of power, utilities, satellites or telecommunication services

Always check the relevant Product Disclosure Statement (PDS) or Policy Wording to view the full list of Inclusions and Exclusions.

Did you know?

- Australia is the 5th most targeted country for cyber attacks globally.
  (Symantec Internet Security Threat Report, April 2016)
- 40% of cyber attacks are directed at SME's.
  (CERT Australia, 2012)
- The average cost of a cyber crime attack to a business is $276,323.
  (Stay Smart Online, Australian Government, 2015)
- Approximately 60% of Australian businesses have experienced at least one ransomware incident in the past 12 months.
  (IDG Communications - Australia, 2017)
- It takes an average of 23 days to resolve a cyber incident.
  (Stay Smart Online, Australian Government, 2015)

Claim Case Study

An employee of an eye surgery clinic opened an email attachment that contained a virus. Once opened, the encrypted virus was spread through their IT system causing them to lose access to their entire network. The Russian based hackers then demanded a ransom payment of $6,000 in BITCOIN.

The clinic had to revert to using paper records to treat their patients and record the details of consultations until their system could be restored. They were also unable to raise invoices during this time.

Fortunately, the clinic had a Cyber Liability policy and their insurer's forensic investigators were able to recover the majority of the clinic's data and restore their invoicing system. The total claim amounted to $90,000 which covered IT expenses, first party damage and lost hours of operation.

BizCover