Cyber Event Protection

A Digital Fire

Most businesses purchase fire insurance of some description. Businesses are acutely aware of the impact a fire could have on their operations.

What would you do in the event that your data had been destroyed in a virus attack?

Cyber Event Protection cover provides for a reduction in revenue and the associated costs to manage the impact of a Cyber Event

Protecting Your Business from a Digital Fire

Cyber security is a growing concern for business. Protecting all elements of your IT infrastructure such as hardware, software networks and facilities against a cyber event is a business risk worth mitigating.

It doesn't matter what the size of your business is. Handling customer or transaction data, you run the risk that a data breach could give rise to a material financial cost to your business or significant costs relating to third party claims.

Cyber Event Protection responds to Cyber Events and covers costs, first party risks and third party liability

Losses to your business from a Cyber Event (in your business or a supplier's business)

Loss to third parties because of a Cyber Event in your business

Cyber Event Protection responds to:

Cyber Event

- Point of sale intrusions
- Cyber extortion
- Web app attacks
- Insider and privilege misuse
- Physical theft and loss
- Payment card skimmers
- Crimeware
- Denial of service
- Cyber espionage
- Miscellaneous errors

"Would you know what to do in the event of a cyber attack?"

With Cyber Event Protection you have 24/7 access to cyber experts to help navigate through the complexity and mitigation of a Cyber Event

Example	Claim Scenario	Protection Response
Lost Laptop	A laptop containing lists of customer and personal contact information is left on the bus.	Costs of contacting the customer list and advising them of the situation together with associated costs of appointing a Credit monitoring service.
Client designs destroyed in virus attack	Customer designs are compromised after a work colleague opens an email that lets a virus into the network.	Response team helps you to mitigate the impact of the virus and stop it infiltrating your system any further. Removal of the virus from your system, associated costs of mitigating further loss or damage and the costs of restoring data in your system. Revenue impact on your business as a result of the cyber event.
Patient personal information	IT infrastructure has been accessed and a copy of all of your patient records may have been obtained.	Response team appoints a firm to contact your patients and communicate the situation to them. A Credit Monitoring service is appointed to ensure that your patients' financial records can be watched and any issue can be managed appropriately. The costs of securing your system, contacting your patients and the related Credit Monitoring costs.
Unauthorised sale/use of sensitive information	A Customer alleges that a failure of your IT system has led to financial information being obtained and ultimately leading to their credit rating being impacted. On investigation, an employee has copied these records and passing them on to a criminal gang who have been committing credit fraud.	Appointment of a forensics investigator who assists with securing data and implementing appropriate preventative measures. Credit monitoring facility is established to identify any unusual credit activity. Defence costs and payment of award, fine or penalty.
Extortion attempt	You receive an extortion e-mail. It is clear that if you don't comply with the demands, your business will be impacted.	Response team will determine that this is a genuine threat. The team neutralise the threat to your business and no extortion monies are paid. The costs to protect your operations and neutralising the treat.
One of your suppliers suffers a cyber event	A supplier advises you that they have had a significant cyber event and they cannot use computer systems to manage their customer delivery cycles. You have been unable to find a temporary solution for stock supplies. You suffer a downturn in business.	Impact on business costs paid as your supplier is subject to a Cyber Event as described in the policy.

Cyber Event Protection Summary of Cover

Covers reasonable costs and expenses (upon insurer approval) such as:

Cyber Events

- ☑ Credit and Identity monitoring costs for a period up to 12 months (allows you to be proactive in identifying risks and notifying parties in a timely manner to mitigate damages
- ☑ Customer notification costs incurred in notifying parties whose data or information has been wrongfully accessed or lost
- ☑ Cyber Extortion Costs where a third party is seeking to obtain financial gain through extortion
- ☑ Data Restoration Costs in restoring or replacing data or programs that have been lost, destroyed, damaged and the cost to mitigate or prevent further damage (including licences costs but excluding redesign, replication or reconstitution of proprietary information, facts, concepts or designs)
- ☑ Data securing costs to avoid ongoing impact on your business
- ☑ External Management costs; public relations manager
- ☑ Virus Extraction Costs (costs incurred to remove a virus)

Cyber Event Response Costs

- ☑ Impact on Business Costs (loss of revenue and increased costs incurred to avoid a reduction in revenue

Can YOUR business afford to be without this protection?
Call your local Cowden office TODAY and protect yourself from Cyber Events

Cowden Limited - Ph: (08) 9322 4822

Cowden (SA) Pty Ltd - Ph: (08) 8300 0888

Cowden (VIC) Pty Ltd - Ph: (03) 9686 6500

Cowden (NSW) Pty Ltd - Ph: (02) 9966 4400