Cyber Insurance

Protecting your business from a “Digital Fire”

Would you leave your business premises uninsured? We hope not!
Imagine opening a plausible looking email only to find all of your computer systems locked by a cryptolocker demanding $1 million to “unlock” your files. What if your customer’s private information was also being held to ransom?

This is what we refer to as a “digital fire” which in our experience can cause just as much financial loss to your business, if not more than an actual fire at your premises.

Cyber attacks occur to all types of businesses, and at any time.

Are you aware of recent changes to legislation which may oblige you to report data breaches?
It is known as the Notifiable Data Breaches (NDB) Scheme and applies to any business with an annual turnover of more than $3 million and any business who handles personal information. Fines and penalties apply for failure to notify and a Cyber policy insures this exposure.
https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

Fortunately these fines and penalties can be covered by cyber insurance as well as the following;

Cyber Events - Crimeware, cyber espionage, cyber extortion, denial of service, hacking, insider and privilege misuse, miscellaneous errors, payment card skimming, physical theft and loss, point of sale (POS) intrusion and web app attacks. Further optional covers include cyber theft, tangible property and telephone phreaking; where your telephone system is hacked and routed to expensive overseas calls.

Losses to your business - Business interruption to cover lost income resulting from a cyber event with an option to also cover contingent business interruption; if one of your external suppliers halts operation due to a cyber attack on their systems.

Loses to others – Legal expense, settlements, awards, damages, mandatory notice, multimedia injury (as well as civil fines and penalties already noted).

Response costs – Credit and identity monitoring, customer notifications costs, extortion costs, data restoration costs, data restoration costs, data securing costs, external management costs (including public relations), virus extraction.

Loses to others – Legal expense, settlements, awards, damages, mandatory notice, multimedia injury (as well as civil fines and penalties already noted).

Do I need cyber insurance if everything is in the “cloud”?
Yes, you do. Many believe that since their data is stored and managed by someone else, that it is safe. This is far from the truth. In fact they have just added a level of complexity as they are now relying on a third party provider to take the right steps to keep the data secure. While Cloud providers may provide a higher level of cyber security for data, this does not prevent the human factor.

The Human Factor:
“It won’t happen to me, we have a firewall in place” is a common comment we hear a lot from people, however, buildings are equipped with fire extinguishers and blankets, yet they still burn! You can have all the security protection in the world and all it takes is one employee to open a scam email and your entire IT system is compromised.

With recent events, we are relying on technology more than ever. Protect yourself by having adequate security measures in place, educate your employees of the cyber risk and exposures, and purchase a Cyber Event Protection policy to cover the costs incurred from the Cyber Event and the additional costs to manage your reputation.

Please contact us today to organise a policy to protect your business and your data.

Contact us here

Genesis Insurance Brokers Australia
Phone: 07 5593 7473