cfc

cfcunderwriting.com

Top five reasons to buy cyber

Making the case for cyber insurance, a relatively new type of cover, can be tough for brokers even if it's clear that nearly all companies would benefit from it. So to help brokers make the argument for cyber insurance more easily, we've put together the top five reasons to buy cyber.

5. Cybercrime is the fastest growing crime in the world, but standard property or crime insurance policies can be restrictive in the cover they offer.

The widespread use of technology and the internet now means that your business is exposed to the world's criminals and is vulnerable to attack at any time of the day or night. For example, social engineering scams are becoming a pandemic in the business world, leading to significant losses for companies of all types. Cyber insurance is at the forefront of protecting against this new wave of crime, providing cover for a wide range of electronic perils, from wire transfer fraud to ransomware.

4. Technology systems are critical to operating your day-to-day business but their downtime is not covered by standard business interruption insurance.

Almost all businesses rely on computer systems and other technology to conduct their core business, from electronic point of sales software to back office work flow management systems. In the event that these systems are brought down, a traditional business interruption policy would likely not respond. Cyber insurance can provide cover for loss of income and extra expense associated with a cyber event.

3. Data is one of your most important assets yet it is not covered by standard property policies.

Most businesses would agree that data or information is one of their most important assets and worth many times more than the physical equipment that it is stored upon. Yet most business owners do not realize that a standard property policy would not respond in the event that this data is damaged or destroyed. A cyber policy can provide comprehensive cover for data restoration and even re-creation in the event of a loss.

2. Complying with breach notification laws costs time and money.

Breach notification laws are now commonplace across many territories, and among other things, generally require businesses that lose sensitive personal data to provide written notification to those individuals that were potentially affected or risk hefty fines and penalties. Australia's Notifiable Data Breaches Act, Canada's Digital Privacy Act, Europe's General Data Protection Regulation, and several US state laws make it a legal obligation to notify, and there is also a growing trend towards voluntary notification in order to protect your brand and reputation. Cyber policies can provide cover for the costs associated with providing a breach notice even if it's not legally required, and can also cover the associated regulatory fines and penalties.

1. A good cyber policy provides access to a wide range of incident response services.

Responding to a cyber incident requires a range of specialists – from IT forensics firms to specialist PR agencies – that help deal with both the immediate aftermath as well as the longer term consequences of a cyber event. Small and medium sized businesses, in particular, are facing an uphill battle; not only are they increasingly being targeted by cybercriminals but they are also unlikely to have the range of required incident response specialists in-house. The good news is that cyber insurance can provide easy access to these services, helping companies more easily negotiate the changing face of crime.