Is cyber insurance right for my business?

Cyber insurance is finding its way onto the agendas of businesses everywhere, but it's still a relatively misunderstood class of insurance. Because of this, many companies find themselves confused about how cyber insurance actually works and are skeptical about whether it makes sense for their business to purchase a policy.

We hear you. In an effort to answer some of your big questions and put your concerns to rest, here are six big reasons why buying a standalone cyber policy may be a smart decision for your business.

1 You get cybersecurity tools & support, for free

For most small-to-medium sized businesses, having a robust in-house IT security team isn't always possible, or even necessary. But this can leave you without a place to turn in the event that the worst does happen. Would you know what to do if you walked into the office one morning and your systems had been disabled?

Cyber insurance is a highly cost-effective way to gain access to the support you need in order to both prevent and respond to cyber events. Most cyber policies come with a number of proactive risk management tools, such as employee cybersecurity training programs, which help reduce successful phishing attacks, and dark web monitoring, which scans the dark web for signs that data relating to your business has been compromised. Most importantly, when it comes to responding to a cyber event, a good policy will give you access to IT experts, forensic specialists, PR firms, lawyers, and more, and often with a nil deductible.

2 Over half of all cyberattacks are aimed at small-to-medium sized businesses

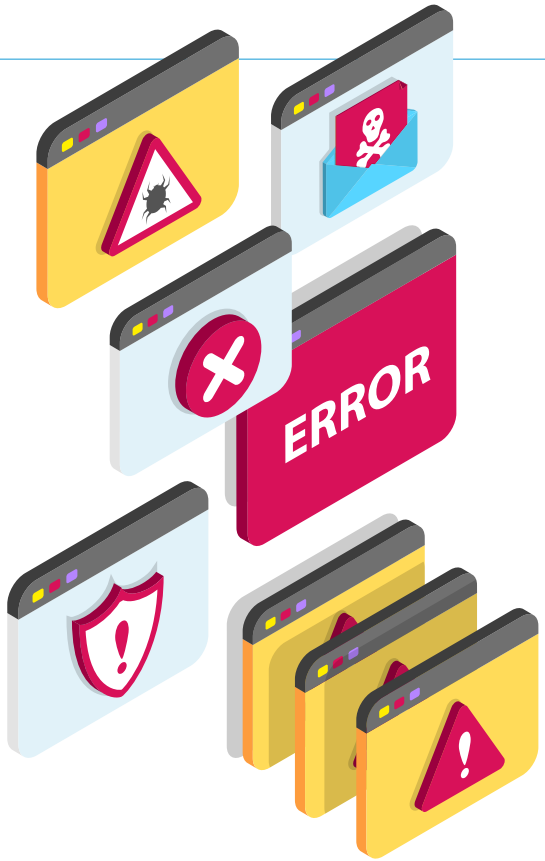
While the headlines focus on major security breaches at major companies, over half* of all cyber attacks are aimed at small businesses. What you don't often hear about is the local law firm that mistakenly transfers $100,000 to a fraudster after being duped by a social engineering scam or the doctor's office unable to use their computer systems for days because of a destructive malware attack. Just because events like these aren't reported in the mainstream media doesn't mean they aren't happening.

Cybercriminals see smaller organizations as low hanging fruit because they often lack the resources necessary to invest in IT security or provide cybersecurity training for their staff, making them an easier target.

3 Your employees will probably click on something they shouldn't

Approximately three quarters of the cyber claims we deal with involve some kind of easily-preventable human error. Theft of funds, ransomware, extortion and non-malicious data breaches usually start with a human error or oversight such as clicking on a phishing link, which then allows cybercriminals to access your systems from the inside.

The fact remains that humans are the weakest link in the cybersecurity chain no matter how hard we try. Cyber insurance is a cost-effective way to not only get access to risk management tools like phishing-focused employee training programs, but also to cover the financial loss if someone makes a mistake.



5 Cyber insurance covers far more than just data privacy

Two of the most common sources of cyber claims we see aren't related to privacy at all – funds transfer fraud is often carried out by criminals using fraudulent emails to divert the transfer of funds from a legitimate account to their own, while ransomware can cripple any organization by freezing or damaging business-critical computer systems. Neither of these types of incidents would be considered a data breach, but both can lead to severe financial damage and are insurable under a cyber policy.

Many businesses think that cyber insurance won't be useful to them because they don't collect sensitive data. However, more than 50% of our cyber claims come from events unrelated to breaches of privacy, and any business that uses technology to operate will have a range of other cyber exposures which a cyber policy can address.

4 You aren't covered under other lines of insurance

Cyber cover in traditional lines of insurance often falls very short of the cover found in a standalone cyber policy. Property policies were designed to cover your bricks and mortar, not your digital assets; crime policies rarely cover social engineering scams - a huge source of financial losses for businesses of all sizes - without onerous terms and conditions; and professional liability policies generally don't cover the first party costs associated with responding to a cyber event.

So, while there may be elements of cyber cover existing within traditional insurance policies, it tends to be only partial cover at best. A good standalone cyber policy, on the other hand, is designed to cover the gaps left by traditional insurance policies, and importantly, comes with access to expert cyber claims handlers who are trained to get your business back on track with minimum disruption and financial impact.

6 Cyber insurance pays more claims than any other type of insurance

CFC has paid more than 1,500 cyber claims in the last 12 months, a number that eclipses previous years and is steadily growing, and the vast majority of these are from small and medium sized business. The industry as a whole is showing similar trends and low declinature rates. In fact, it was recently revealed that 99% of cyber insurance claims were paid in 2018, which means cyber has one of the highest claims acceptance rates across all insurance products.**

Information like this shows that cyber policies are doing what they set out to do, which is provide broad coverage for a range of technology and privacy-related risks affecting modern businesses, all backed up by proactive risk management and expert incident response and claims handling.

Do you have questions about whether cyber insurance is right for your business? Reach out to cyber@cfcunderwriting.com today.

* Verizon Data Breach Investigations Report, 2018 ** Association of British Insurers, 2019