Proactive →

cfc

Cyber exposure:

Client conversation starters

Before talking about cyber insurance premiums and the coverage available, it's important that clients first recognize some of the basic cyber risks faced by their business as many may not know where their major exposures lie or that insurance exists to cover them.

To help you get the conversation started, we've put together a handful of questions you can ask along with key talking points for each.

Do you send or receive wire transfer payments?

1

- Cybercriminals are increasingly intercepting wire transfers, often by hacking into email accounts, pretending to be someone else, and sending fraudulent instructions.
- These scams are hard to spot because cybercriminals are taking the time to study how their victims send and receive payment requests, and they often come from real email addresses.
- Payments are rarely retrievable as they are siphoned off into other accounts quickly. Banks rarely refund the losses.
- Cyber insurance can refund the often significant financial losses that come from scams like these. In fact, funds transfer fraud makes up about a quarter of CFC's cyber claims globally.

Do you collect or store personally identifiable information (PII) like credit card numbers or health information?

2

- If sensitive information that you are responsible for is lost or stolen, you will most likely have to notify affected individuals of the breach and provide credit monitoring services.
- When it comes to PII, there are a number of rules and regulations about how you collect, use and store that information. If you do not adhere to them, you could face regulatory fines and penalties.
- A malicious third party isn't always to blame. Often times, it's as simple as an employee losing a company laptop.
- Cyber insurance covers the range of costs associated with data breaches, like notifying affected individuals and your responsibilities under different regulations.
- Even if you don't store PII, you probably store other business-critical information on your systems. See Question 3 to find out why this could pose a risk.

Do you store business-critical information on your computer systems, such as client contracts, designs and plans, stock levels and other corporate information?

3

- Even if you don't store a lot of customer records or credit card information, you still likely have important information that you need regular access to, from appointment bookings to intellectual property.
- What's more, if business-critical data becomes unavailable, it can have a serious impact on your ability to operate and ultimately your bottom line. See Question 4 for more information on business interruption.

Proactive →

cfc

How long can your business operate without access to computer systems and the data they hold?

4

- You are probably more dependent on computer systems than you realize.
- Understanding that modern businesses are partly or entirely reliant on technology in order to operate, cybercriminals increasingly see ransomware attacks and targeted extortion attacks as an easy way to make money. They do this by encrypting key data and demanding large sums of money in exchange for the decryption key.
- Most small businesses lack to the technical resources to deal with attacks like these in-house and may not have anyone experienced enough to turn to in the event that their systems are brought down.
- Our incident response team notes that the average downtime is two to three days, but that's with the assistance of technical experts. In worst case scenarios, businesses aren't fully operable for weeks or even months after a cyber event.
- Backups are are frequently targeted and disabled in these attacks, leaving businesses with little recourse when it comes to reinstating their data.
- Cyber insurance not only gives you access to a range of technical experts to help get you back online fast, but it covers the financial losses incurred as a result of your business being interrupted and the costs of re-creating any corrupted data. It can even cover the reputational impact of cancelled contracts and customers choosing to go elsewhere.

Do any of your employees work remotely?

5

- Whether good practice or not, people reuse their passwords across multiple platforms, so if a username/password combination is breached in one cyber attack, hackers most likely have combinations for future attacks.
- With login credentials already to hand, cybercriminals can easily gain access to business email accounts or even log into a company's remote desktop service (RDS).
- In addition, there's always the risk that work devices taken outside of the office can be lost or stolen.
- Cyber insurance can cover the fallout from hackers gaining access to your emails or systems, whether stolen funds, business interruption, or a privacy breach.

Are you confident that you or your employees will never make a mistake?

6

- Humans are the weakest link in the cybersecurity chain. In fact, the vast majority of cyber incidents – for CFC, it's about 75% - involve some kind of human error or oversight.
- This includes everything from being tricked into giving over your username and password, reusing passwords which makes account compromise easier, not following up wire transfer requests with a phone call, or losing devices containing sensitive information.
- Cyber insurance covers the financial losses that can result from these types of events as well as giving you instant access to the right specialists if someone makes a mistake. It also often comes with a range of free risk security tools and employee training.