Proactive →

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 payments electronically?

1

- **Cybercriminals are increasingly intercepting electronic fund 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 subject to unauthorised access or disclosure, you will most likely **have to notify affected individuals** of the breach and provide credit monitoring services.
- When it comes to PII, there are usually **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** or sending an email containing sensitive information to the wrong person.
- **Cyber insurance covers a range of costs associated with responding to data breaches**, including legal advice, notifying affected individuals and any regulatory fines and penalties that may be incurred.

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 PII like customer records or credit card information, **you'll 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 serious impact on your ability to operate effectively, ultimately impacting your bottom line. **See Question 4 for more information** on business interruption.

Proactive →

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 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 system downtime can vary, but in worst case scenarios, **businesses can be inoperational for weeks or even months after a cyber event**
- **Backups 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

- Many ransomware attacks stem from cybercriminals exploiting remote access solutions, whether by conducting brute force attacks **which crack simple passwords or by using stolen login credentials.**
- Similarly, funds transfer fraud scams often rely on **cyber criminals gaining remote access to employee accounts** to perpetrate their scams.
- Employees may also be **more susceptible to phishing scams whilst working from home**, especially when they have no one in the immediate vicinity to sense check suspicious emails.
- In addition, there's always the risk that **work devices taken outside of the office can be lost or stolen,** which may result in a data breach.
- **Cyber insurance can protect against the financial losses** which may be the unintended consequence of remote working, whether that be in the form of ransomware, funds transfer fraud or a data breach.

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

6

- Having good cyber security controls in place can make an organisation less vulnerable to attack, but it can never make them 100% secure. Indeed, **humans are often the weakest link in the cyber security chain.**
- This includes everything from employees clicking on a malicious link or attachment in a phishing email, handing over their username and passwords to fraudsters, using weak passwords, **not following up new funds transfer requests with a phone call,** or losing devices containing sensitive information.
- **Cyber insurance covers the financial losses** that can result from these common errors, as well as giving you access to technical experts if someone makes a mistake. It also usually comes with a range of **free risk management tools**, including phishing tools to help employees better spot suspicious emails.