← Reactive

Cyber exposure:

Client objection handling

By now, you may have spoken to your clients about their cyber exposures and perhaps even presented a quote for coverage. But they still aren't convinced.

To help you explain their cyber exposure and the value of cyber insurance as a form of protection, we've put together some of the most common client objections along with key talking points to help you respond in handling each.

"We don't need cyber insurance. We invest in IT security..."

1

- Similar to when a business installs security cameras and sprinklers systems, they still purchase property insurance in case those precautionary measures fail. Cyber insurance works the same. **IT security is a great precautionary measure, but hackers can still gain access and cause damage regardless.**
- **Cyber threats continually evolve to bypass the latest security measures**, even large corporates who spend vast amounts on cybersecurity still routinely get hit.
- Theft of funds, ransomware, extortion and non-malicious data breaches **usually start with a human error** or an oversight like losing a laptop or clicking on a phishing link, which then allows cybercriminals to access your systems.
- Ultimately the cyber landscape is everchanging and **no matter how much a company invests in IT security, they will never be 100% secure.** Cyber insurance is there to add another layer of protection and respond in the event that the worst happens.

"We outsource all of our IT, so we don't have an exposure..."

2

- Unfortunately, **using a third party for IT doesn't eliminate your exposure.**
- If you outsource your data storage to a third party and that third party is breached, you will still likely be **responsible for notifying affected individuals** and dealing with subsequent regulatory actions.
- What's more, many businesses rely on third parties for business-critical operations, and should those providers experience a system failure, **it could have a catastrophic effect on your ability to trade**, resulting in a business interruption loss.
- Most third-party technology service providers have **standard terms of service that limit their liability** in the event that a breach or system outage causes financial harm to one of their clients.

"We don't collect any sensitive data, so we don't need cyber insurance..."

3

- **You don't need to be collecting sensitive data to have cyber exposure.** In fact, any business that relies on a computer system to operate, whether for business critical activities or simply electronic banking has a very real cyber exposure.
- Two of the most common and costly sources of cyber claims are **ransomware and funds transfer fraud**
- Funds transfer fraud is often carried out by criminals using fraudulent emails to **divert legitimate fund transfers to their own accounts,** whilst ransomware can cripple any organisation by encrypting or damaging business-critical computer systems.
- **Neither of these types of incidents needs to involve a data breach, but both can lead to severe financial losses which are insurable under a cyber policy.**

← Reactive

Cyber attacks only affect big business. We're too small to be a target...

4

- Cyber attacks impacting large companies tend to make the news, but just because cyber attacks on small businesses are less newsworthy doesn't mean they aren't happening. In fact, **the majority of cyber attacks are aimed at small businesses.**
- Cyber criminals see smaller organizations as low-hanging fruit because they often lack the resources necessary to invest in IT security or provide cyber security training. **Ultimately, cyber criminals will target the most vulnerable companies, not just the most valuable.**
- Cyber insurance is a great solution for smaller organizations because not only does it provide financial protection against the growing number of cyber attacks on these businesses, it also **provides access to a whole range of technical and legal experts** who are effectively on retainer to the policyholder through their purchasing of a cyber policy, which many small businesses might not otherwise be able to afford.

Cyber is already covered by other lines of insurance...

5

- Cyber cover in traditional lines of insurance often **falls very short of the cover found in a standalone cyber policy**. While there may be elements of cyber cover existing within traditional insurance policies, it tends to be only partial cover at best.
- 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.
- A standalone cyber policy 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.

Cyber insurance is too expensive...

6

- Although cyber insurance policies have become more expensive in recent years, this is **primarily a response to the increased severity of cyber claims.**
- The size of ransom demands in particular has grown exponentially, with demands increasing from the low hundreds just a few years ago to the hundreds of thousands or even millions today.
- Given the significant financial losses organizations can be faced with, whether in the form of **ransom payments, system damage and business interruption costs, or stolen funds,** cyber insurance is well worth the extra spend.
- Cyber insurance also gives you instant access to a wide range of technical specialists who are experts at helping businesses quickly recover from cyber events. **At CFC our cyber threat analysis team is also working behind the scenes around the clock to monitor, detect and prevent cyber attacks from happening in the first place.**