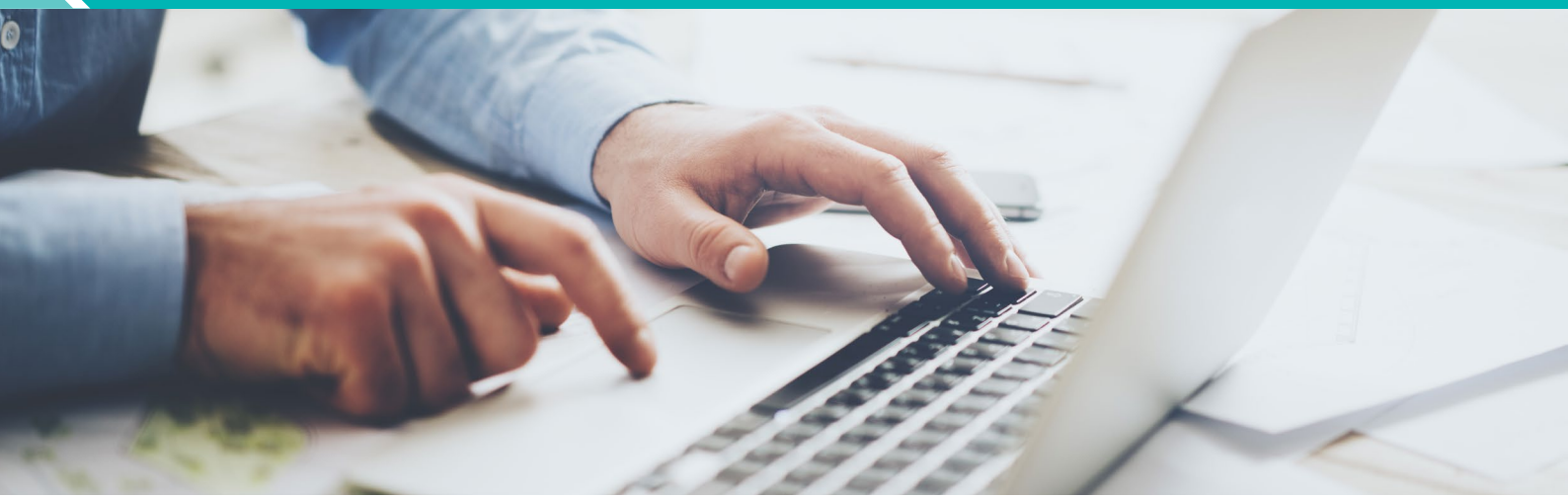

The realities of insuring against cyber crime

Think your business is too small or that your data and information isn't important enough to be targeted by hackers? Think again.

Much of our communication, be it personal or businesses-related, has increasingly moved online in the last two decades, and continues to do so, especially in these recent times of COVID-19 with nearly everyone doing business exclusively online. Every day, thousands of pieces of information are transmitted via email, text, Messenger, WhatsApp, LinkedIn, social media and so on.

Yet while we've launched with a vengeance into the online world, whether by choice or of COVID-necessity, how many of us have kept pace with adequate cyber protections and insurances? Every day, we see individuals and businesses being targeted by cyber criminals. And it's not just the big end of town in the crosshairs — plenty of smaller practices fall victim to cyber crime.

Cyber insurance can be regarded as business-critical insurance because statistics show that the likelihood of a claim occurring within a cyber insurance policy is now as high, if not higher, than making a claim against your business insurance or PI insurance.

Yet not all insurance policies are the same, and so businesses need to understand exactly what they are and are not covered for. At a minimum, a cyber policy should provide a 24/7 breach response service (including IT forensic services), breach response management, credit monitoring, public relations crisis management, civil and regulatory defence costs and penalties, cyber extortion costs, business interruption cover and cyber terrorism.

Proactive IT management and response plan

In addition to cyber insurance, a proactive IT management and a data breach response plan, supported by your IT, are critical elements to future-proof a business. The idea is that a data breach response plan should be no different to having a fire evacuation plan; it needs to be tested and rehearsed regularly.

Often recommend are three pillars of secure information management to identify and address risks within the IT infrastructure to reduce the likelihood of a cyber-attack. In what could be dubbed the "CIA of data management", these are:

- confidentiality
- integrity, and
- availability.

This three pillar approach ensures all data remains available and accessible (availability) to only authorised users (confidentiality) and remains intact and unchanged by unauthorised access or processes (integrity).

What does proactive IT management look like?

It's easy to tell a business to ensure its service providers are proactively managing IT systems, network and company data, with a focus on prevention. But what does this mean practically?

One could label this as an "always eyes on" holistic approach. This would include comprehensive monitoring, maintenance, support and management of organisational systems to help identify issues or concerns before they become a problem.

A set of overarching guidelines and business security principles should be established, and then the business should work through a practical approach that covers these key areas:

- password management and security
- network and data access management and security
- physical security
- information exchange policies and security (eg secure, encrypted, audited email)
- backup and disaster recovery
- education and awareness for internal staff
- cyber insurance coverage and policy wording
- policies and procedures (eg incident and data breach response plan)
- legal response and management plan, and
- responding to the psychological impacts following a data breach.

A big risk

A successful attack can cause lasting and irreparable damage to your business. It can result in business downtime, legal and financial liability, as well as damage to your reputation, brand and the trust you have with clients. The biggest risk your business can take is to do nothing.