Shielding your practice against cyber-attacks

Cybercrime is on the rise in South Africa, costing members of the public R2.2 billion a year. Increasingly, healthcare providers are being attacked due to their rich databases containing patients' health and banking information. To mitigate this, private practices are now turning to cyber liability to protect themselves from data breaches and ransomware.

Issued on behalf of Indwe Risk Services (Authorised FSP 3425) and MC de Villiers Brokers (Authorised FSP 7241)

Last year South Africa experienced a surge in cyber-attacks. Credit bureau Experian grabbed headlines with its massive data breach which exposed the personal details of 24 million South Africans. Other big organisations to be targeted by hackers have included a hospital group, a bank and a metropolitan municipality.

Taking advantage of COVID

What happened to Life Healthcare isn't isolated. Hackers are taking advantage of the COVID-19 situation to extract people's personal information for their own malicious purposes, and the latest international trends in cybercrime are now reaching our continent.

As hackers accelerate their attack, healthcare practices will need to improve their data security, especially now that so many employees are working from home. They will also need to rethink their cyber liability, is the advice of industry experts.

Cyber liability and POPI

The need to invest in cyber liability is made more urgent by the Protection of Personal Information Act (POPIA), which will be enacted from 1 July 2021. This law will bring SA up to date with other privacy legislation, such as Europe's General Data Protection Regulation (GDPR).

Both POPIA and GDPR emphasise the need to protect personal client data from loss, damage or unlawful access. The onus is on healthcare practices to implement reasonable technical and organisational measures to ensure the protection of their patients' details. This involves identifying all internal and external risks, establishing the necessary safeguards and frequently updating them as new risks emerge.

Smaller isn't necessarily safer

Just because a practice is smaller doesn't mean it won't be targeted for hacking. It is true that the larger the practice, the greater the risk and the more a cyber liability policy will cost. But smaller practices are often more vulnerable because they're mainly focused on treating patients, not ensuring they have the latest security measures in place.

Cyber criminals love targeting healthcare organisations because their databases contain patient names, birth dates, addresses, ID numbers, banking details and medical aid information. Often smaller practices don't encrypt their patients' information, so even if a laptop is stolen, it's a potential data breach. Other practices are under the false impression that data storage is the responsibility of their electronic health record (EHR) systems provider, so they're not liable if anything goes missing or gets hacked. This is simply not true.

Beware of back-door access to information

The more data is exchanged between practices, medical aids, hospitals and labs, the more vulnerable it becomes to cyber-attacks. Practices need to realise that even if they are not directly targeted, they can still be liable for data lost by a vendor or third party.

Doctors should aim to work together with third parties like labs and hospitals to keep their patients' data secure. It's a shared responsibility; you each have a duty to keep it safe.

Get the best cover you can afford

While cyber liability is covered by most malpractice insurance policies, its usually limited and contains exceptions. It is therefore a good idea to go for a comprehensive cyber liability policy that covers hiring IT experts to fix any data breach, paying a ransom to free hijacked data, compensation for loss of income from downtime or patients leaving the practice, hiring a PR firm to handle bad publicity and hiring attorneys to deal with lawsuits filed by patients, as well as any damages awarded.

The cost of your policy would depend on the size of your business, with an entry-level figure being around R2 000. Cyber insurance may seem like an unnecessary extra expense, especially as doctors already pay such high indemnity fees, but not having it isn't worth the risk. The last thing you want to have to think about when you've been hit by a cyber-attack is how you're going to afford to pay for it to be fixed.