Protecting patient information: Why anti-virus software (on its own) won't cut it in 2020

Legislative requirements under the Federal Government's Notifiable Breaches scheme came into effect from 22 February 2018. The scheme outlines standards of accountability and transparency to protect individuals' personal information. As a practice, you have access to patient records and private information, and this information must be protected. Cybersecurity is important for both individuals and businesses to protect the confidentiality, integrity and availability of information.

It is often said that if a burglar is determined to rob your house then the best you can do is make it difficult for them. We are all aware what to do to secure our home and most of us are also aware how to secure our online privacy (i.e. using anti-virus software, passwords and backups). Our human failings mean that sometimes we forget to lock doors or upgrade our anti-virus software on all devices. We all believe that the worst will never happen to us – but after a cyber-attack, you will have continuous threat monitoring to reduce the risk of impact to your dental practice.

Three main risks of the most common cyber-attacks

1. Denial of service or inability to gain access to your own system and data. This can be financially devastating and possibly fatal if the situation cannot be rectified within a reasonable time.
2. Phishing attacks that result in the practice's financial or the patient's dental data being made available to a hacker. This may have economic costs as well as regulatory costs if fines or sanctions are imposed.
3. Malware attacks that result in the system getting a virus, which is often spread to patients or associates. This can seriously damage the reputation of the dental practice resulting in loss of patient trust, loss of current and future customers, and poor media coverage.

How to minimise your risks

Lock them out: Ensure your passwords are strong. They should be a minimum of eight characters, mixture of upper and lower case, containing numeric and alpha fields. You should also use multifactor authentication, where you login with your username and password, and the system sends an authentication code to your phone. This means that without your phone, your account can't be accessed. Passwords should be regularly changed and not the same for each application. Passwords should not be shared. Ensure you have the most up-to-date anti-virus software.

Don't invite them in: Be careful with unsolicited emails, making sure not to click on any link or attachment provided. Think twice before you click any link or download anything online. Ensure your staff are educated about cybercrime and their Internet responsibilities. Understand that your mobile device is also a computer and should have the latest available security updates. Do not use USB or external hard drives from an unfamiliar source, and consider the possibility of sensitive data being intercepted when using public Wi-Fi.

Action plan: Backup all important data daily. Ensure you have cybersecurity services included as part of your IT service like continuous threat monitoring, regular vulnerability assessments, incident response and data breach investigations. Prepare a cyber security policy and procedures document that everyone is aware of. This should identify who to contact in the event of a security breach, example emails to be sent to affected patients/contacts and a data recovery plan.

A friend of mine has a security system in his house where the cameras can livestream to his phone. He is alerted when there is unexpected motion in his home, and he can then use his phone to identify the cause. This is very similar to cybersecurity network monitoring whereby the IT company can monitor for potential threats and conduct data breach investigations where necessary. A good IT company will provide continuous threat monitoring and perhaps do a gap analysis to identify your weakest points.

This article has been written with the assistance of Edgar Rodriguez, CEO of Secoura (continuous threat monitoring services). Look out for the webinar in February where I will be conducting an in-depth interview with Edgar Rodriguez on cybersecurity risks for dental practice owners. Edgar was formally at ANZ Bank building cybersecurity practices to reduce cyber risk exposure, he is a qualified cyber security adviser and understands the dental industry through his wife who is a dental surgeon.

MW Partners specialises in providing strategic tax advice to dentists and dental practice owners. We have strong relationships with advisers in other fields (e.g. banking, marketing, cybersecurity) who can provide specialist advice to meet your needs. If you would like a review of your tax structure or business operations, contact our office on 8825 5400 for a free consultation.

MW Partners
CHARTERED ACCOUNTANTS
Specialist Dental Accountants

MW Partners is an ADAVB member benefits partner. mwpartners.com.au

Disclosure: ADAVB receives referral fees in recognition of our marketing service alliance.

Top: MW Partners Principal Albert Gigl