Justin Fung
LL.B, B.S
Partner, Head of Commercial & Corporate
Avant Law

Cyberattack: are you prepared?

Imagine receiving a phone call from your IT team or service provider, informing you there's been unauthorised access of the entire patient record by an unknown party. Unfortunately, this is a situation many practices have faced recently and is a reminder for practice owners to be across their cyber security.

The recent Optus and Medibank cyber security incidents are high-profile instances of an increasingly common type of cyberattack using ransomware. This is a type of malware that works by locking up or encrypting files so they can't be accessed until the victim pays the ransom.

Check your preparedness

When was the practice's cyber security last assessed? Practices grow and their operations become more complex over the years, which can introduce new areas of risk. Automated activities that should be occurring regularly need to be checked to ensure that they are still performing properly, otherwise important back-ups and file transfers may not be there to use when you need them (including in the context of a cyberattack).

Long gone are the days when patient records have been stored in hard copy format in filing cabinets, as these records have likely migrated to a cloud-based platform hosted by third-party providers. These third-party providers often employ cyber security experts, however, it is good to understand how they are looking after sensitive patient data in the practice. Knowing how your business collects and handles patient data is essential and requires having the right expertise to advise the practice on privacy and IT security matters.

Signs that risks might increase

Turnover among IT staff could affect the way the business' cyber security systems are audited. This may also affect whether the latest updates to IT platforms are in place.

Are practice employees receiving unusual emails and pop-up messages requesting information? Do they know what to do if they receive a suspicious email? Employees need training and regular reminders on this to avoid complacency, and so they know what to do and how to report potential cyber threats. The majority of cyberattacks start from phishing, which means that every staff member is an essential part of the practice's first line of defence.

Consequences and costs of an attack

The cost to organisations to rectify the impacts of a ransomware attack can be in the millions of dollars. There are the direct costs of items such as the ransom, people's time, lost revenue due to downtime, IT and other consultants, hardware and network costs. In addition, there are the indirect costs of damage to the practice's brand and reputation.

Health sector a prime target

According to a report issued by IBM Security X-Force Threat Intelligence Index, ransomware was the top attack type in 2021 and comprised 21% of all cyberattacks. The health industry was the top sector affected by ransomware, as reported to the Australian Cyber Security Centre[1]. The health sector is a prime target for cyber criminals due to:

- Services delivered by the health sector are often critical to the community. Where there's a potential threat to human life, cyber criminals that target health also assume organisations are considerably more likely to pay a ransom.
- Given the general sentiment of trust communities place in medical professionals, cyber criminals anticipate that health organisations are most inclined to do 'whatever it takes' to restore business continuity as quickly as possible.
- Bigger practices operating cloud-based platforms hold sensitive data of many patients. The increased centralisation of data has made it attractive for criminals to target these bigger practices.
- As healthcare organisations are focused on delivering care to patients, cyber security can move down the priorities and practices may gradually become more vulnerable to lower levels of cyberattacks.

Reference

1. Australian Signals Directorate & Australian Cyber Security Centre, Ransomware in Australia, October 2020

Manage your risks of a cyberattack

- ✓ **Are you running up-to-date** end-point security and anti-virus software for all your digital communication and messaging platforms?
- ✓ **How often are you backing up** all of the patient records and related data?
- ✓ Have you **implemented anti-phishing campaigns** and does your business have systems in place to screen, block and restrict websites which may potentially be malicious?
- ✓ What tools do you have in place to continually **monitor for potentially malicious activity** across your systems?
- ✓ Are there **internal protocols and controls** governing who can access certain types of information with different levels of sensitivity?
- ✓ **Are your staff (especially those on the frontline) being regularly trained** and tested on their ability to identify potential concerns and promptly report unusual activity through to the correct channels?
- ✓ Have you got a **business continuity plan** which sets out clear processes and procedures to be implemented in the event of a cyberattack?
- ✓ Do you have **appropriate reporting and governance structures** in place to ensure that key stakeholders are apprised of potential vulnerabilities and relevant regulatory authorities are notified?

Avant resource

Download our Cyber security checklist

Protecting members' data

Due to its sensitive nature, Avant views member data in the same way doctors and practices view patient data. Protection of member data is taken very seriously and a top priority at Avant and covers people, processes and technologies.

- As an APRA-regulated entity, we undertake several annual audits to verify compliance against all APRA standards and to test the effectiveness of the security controls
- Use of industry leading technologies to create an external defence
- Regular external and internal cyber testing of systems
- Regular staff education and awareness on cyber security
- Annual compliance for cyber security from our employees and contractors
- Security management of vendors
- 24/7 security monitoring of the Avant systems landscape
- Compartmentalising and restricting access to different types of data
- Regular reviews of the types of data we store and for how long

As the cyber landscape is constantly evolving, Avant is always working on high alert to secure and protect your data.

We need your help too. If you never become suspicious of a message from Avant, contact us at **security@avant.org.au**.

Privacy breaches and cyber incidents can happen despite your best efforts

Avant Practice Medical Indemnity Insurance^ includes **Cyber Insurance**+, protecting against:

- cyber extortion
- privacy liabilities
- damage to digital assets.

Protect your practice, your staff and your data today.
Visit avant.org.au/practices

^Cover is subject to the full terms, conditions, exclusions and limits set out in the Policy Document and policy schedule. Avant Practice Medical Indemnity Policy is issued by Avant Insurance Limited, ABN 82 003 707 471, AFSL 238 765. +Avant Cyber Insurance cover is available up until 20/03/2023 to eligible Avant Practice Medical Indemnity Policy holders under a Group Policy between Liberty Mutual Insurance Company, ABN 61 086 083 605 (Liberty) and Avant. Practices need consider other forms of insurance including directors' and officers' liability, public and products liability, property and business interruption insurance, and workers compensation. Any advice here is general advice only and does not take into account your objectives, financial situation or needs. You should consider whether the product is appropriate for you and the Policy Document and the Policy Schedule for the relevant product, available by contacting us on 1800 128 268, before deciding to purchase or continuing to hold a policy. Information is only current at the date initially published.