Avant factsheet:

Steps to protect your practice from a cyber security incident: things to consider

Preparation is your best defence to minimise the chance of a cyber security incident. This factsheet provides a quick guide on the following issues:

- the importance of policies and procedures
- implementing a business continuity plan
- updating contracts with third party providers
- how to use an IT service provider
- five steps to protect your IT system.

Policies and procedures

Your practice should have a policy that covers current expectation of staff in relation to cyber security, including:

- not sharing passwords
- use of the internet
- downloading of software to the practice system
- caution when opening unusual emails.

The policy should outline your protocol for backing up data and a recovery plan if an incident occurs. All staff should be trained and regularly updated on their responsibilities if an incident occurs [See *Cyber security checklist*].

Business Continuity Plan

It is essential to have a business continuity plan. The plan should outline your data back-up procedures and contain details on patient care management if there is a major incident. For example, we recommend that you have a supply of paper prescription pads, a hard copy appointment diary and patient history forms available to use if a cyber incident occurs.

Review and update contracts with third party providers

Ensure third party providers who store information (e.g. in the cloud) or outsourced back-up providers have security measures in place to protect private information.

Contracts with IT software and hardware providers should include a clause that protects the practice if there is a security breach due to a system error or fault on the part of the provider.

IT service provider

An external expert view can be helpful. Consider hiring an IT consultant to undertake a security audit or risk assessment to test potential threats to the practice and help implement mitigation strategies.

Talking to your IT service provider about cyber security protections

There is no 'one-size-fits-all' IT solution for medical practices to reduce the risk of a cyber incident. For example, the risk profile and IT needs of a busy metropolitan practice, with 30 doctors and an electronic health records system and online appointments, will be different to a sole practitioner in a remote town with limited access to the internet who uses mostly paper-based records.

A risk assessment of your practice is vital to identify:

- how you use technology
- where the risks are
- the staff most likely to be a target for a cyber incident, e.g. those with IT administration privileges.

An IT service provider should explain what they propose for your practice and why in simple language. Be wary if they use a lot of jargon. They should be able to guide you through the requirements for your practice, not just try to sell you new software.

Five steps to protect your systems

These steps can help you navigate discussions with your IT service provider and protect your network and systems.

1. Check your network security controls

Your IT service provider should check your network security controls including:

- remote desktop privileges (e.g. logon from home or remote IT support)
- firewall (network and/or local computer)
- virtual local area networks (vLANs)
- intrusion detection and protection.

Ask your provider the following questions to help facilitate this process:

- How are these maintained?
- Is there a monitoring process in place?
- How are unusual behaviours tracked, reported and addressed?

Check how your network and computer systems can be accessed and who will have access.

- How are user IDs created and managed?
- Are certain users granted access to systems administration (more advanced than the usual staff role) and is this access regularly reviewed and managed?
- When a staff member moves to another role or leaves the practice, how is their access changed, deactivated or deleted?
- Do you have password standards (e.g. complexity, expiry, secure communication of passwords) that leverage best practice? Are they being followed?
- How is compliance monitored and reported? If there is non-compliance, how is it managed?

Check that all personal computing devices, i.e. laptops, desktops and mobile phones, are also secure.

2. Update your systems and software with patches

Pop-up alerts for software updates can easily be ignored. However, regularly installing operating system (security) and software updates is one of the most effective ways to keep healthcare systems protected against cyber intrusions and viruses.

These updates, known as patches, resolve any issues in your operating system, applications and programs. If there is a known security risk patches should be applied immediately. If there is no security risk identified, they should be installed within 48 hours of the alert.

Keep applications (e.g. Adobe Flash, web browsers, Microsoft Office, Java, PDF viewers) and operating systems up to date as some may no longer be supported by the manufacturers, increasing vulnerabilities to your systems. Your IT service provider should advise you when to change your systems.

3. Use anti-virus and ad-blocking software

Cyber criminals commonly use malicious software (malware) to target computers with viruses, spyware, trojans and worms. These can be delivered by email or while browsing the web. Some malware is also delivered through advertisements on the web.

To prevent these attacks compromising your systems, ensure antivirus software and an ad-blocking browser plug-in is installed and up-to-date, and allow automatic updates from the manufacturer.

4. Use strong passwords

Strong passwords are vital to keep sensitive health information safe and to prevent cyber intrusions. Hackers can use automated methods to guess a password, so avoid using personal information in your password. This includes anything that can be found on social networking sites, even if the words are slightly altered. Consider implementing the following in your practice:

- passwords should not be displayed in clear text when entered
- change passwords regularly and/or set a password expiry period
- staff must **never share** passwords
- Passwords/passphrases are at least eight characters in length, with a combination of upper and lower case, numbers and symbols. Passphrases are encouraged as length and memorability are important security considerations
- temporary passwords are changed on a successful login
- the login account is locked after a set number (such as 3), unsuccessful attempts to log in.

5. Back-up your business systems and files

Hackers use malware to block access to files and can demand a ransom to regain access. Malware can usually only be removed by wiping the computer and reinstalling the operating systems, applications and data from backups. Therefore, it's important to keep frequent back-ups of all critical information and systems. Backups should also be stored securely offsite and not connected to the network to prevent their loss due to malware, fire or theft.

The following resources have more information about information security in your practice:

Information Security Guide for small healthcare businesses (Australian Digital Health Agency and Stay Smart online)

Toolkit for selecting secure IT products and services (Australian Digital Health Agency)

Computer and information security standards (Royal Australian College of General Practitioners)

Strategies to mitigate cyber-security incidents (Australian Cyber Security Centre)