Avant factsheet:
Responding to a cyber security incident

Quick guide:

1. Minimise the damage if an attack is suspected by turning off all computers and not connecting your back-up
2. Seek immediate help from your IT provider
3. Follow your business continuity plan so you can continue to care for patients

This factsheet aims to help you prepare for and respond to a cyber security incident. It provides a quick guide on the following issues:

- how to recognise a cyber security incident
- minimising the damage
- when to seek expert advice
- retrieving back-up data
- how to respond to ransom demands
- maintaining continuity of your practice
- reporting requirements.

Recognising an incident

It can be difficult to identify a cyber security incident. Staff can often assume the problem is with the internet connection or service provider rather than having a more malicious cause. Many practices have infected their secure back-up files by seeking a solution to what is perceived as a smaller issue. If in any doubt you should always assume the worst until other information becomes available and seek expert advice.

Typical symptoms of a cyber incident include the system not starting normally or repeatedly crashing for no obvious reason. The internet browser may go to unwanted pages or advertisements may pop up on the screen in an unusual manner.

Minimise the damage

Immediate action should include turning off all computers, removing the power cord from the wall and not connecting the back-up data or any portable devices such as laptops to the network.

Seek immediate help

Seek immediate help from your IT service provider or forensic specialists to help you understand the incident, how it can be contained and eradicated, and to avoid the attacks moving to other computers in the practice.

Your IT service provider or forensic specialist will aim to identify all files that have been encrypted or modified and when this occurred. This will allow you to target the relevant back-up data to be retrieved as quickly as possible.

Your IT service provider or forensic specialist can also check if a 'decryption key' is accessible due to weaknesses in the malware. This may be used to restore access to your files.

Retrieve backups

You should be able to retrieve medical and other practice records from your back-up files if they are not also affected. The Australian Cyber Security Centre (ACSC) recommends back-up files are retained for at least three months. Check all back-up data servers. Are any hard drives in safes or at the homes of staff?

If the IT service providers or forensic specialists are confident your data will be retrieved from back-up systems you need to know how long this will take.

Responding to a ransomware demand

If a ransomware email is detected demanding money or Bitcoin, you must decide how to respond. The ACSC and the police recommend that you don't pay the ransom for ethical reasons and because it can encourage further attacks.

There is no guarantee the records will be decrypted if the ransom is paid. A 2017 Telstra cyber security report found about one in three surveyed businesses that paid ransom demands did not recover their files. Paying the ransom also identifies you as a compliant victim, increasing the risk of being targeted by ransomware operators in the future.

In response to a ransomware demand, consider the following:

- What is the subject of the ransomware attack – specific data files or devices, or your whole system?
- Is your data backed up? How long will it take and what will it cost to restore your data?

- How much are the cyber criminals demanding to release your data? What are the likely financial costs if the ransom is not paid? E.g. the cost of the destruction of or loss of data, lost productivity, business interruption, investigation, public relations, attempted restoration and recovery of systems.
- What about non-financial costs? Will lack of access prevent you from providing key services?
- What is your practice's tolerance for payment of ransoms? Will it refuse to pay them on principle?

Continuing your practice while the cyber incident is resolved

A business continuity plan that outlines procedures to maintain patient care is essential.

Lack of access to electronic medical records is not in itself a reason to decline to see patients. Lack of access to electronic medical records will impede patient care and make it difficult to continue to practise, but patients will still expect to be seen. This should be covered in your business continuity plan.

If your patients have a My Health Record they may be able to access relevant details on their phones.

If the appointments system has been lost, access to an appointment or day sheet printed the previous day should see you through the first 24 hours. However, if the system remains down patients may continue to turn up for appointments. Reception staff should take each patient's details and note the time of the appointment in a manual diary.

Retrieving patient information

Explain to patients there is an IT issue and the medical records system is unavailable so you will need some information from them, or ask the patient to access their My Health Record.

In some cases, without access to a patient's medical records you may need to go back to basics and take a history. Check with the patient for allergies before prescribing medication and if any pathology or imaging results are outstanding.

Staff will need note pads and script pads so they can document notes in paper-based records. Secure these records in filing cabinets/cupboards.

It is important to keep all staff updated on a regular basis about how long the systems are likely to be unavailable.

If back-ups are not available or will take time to retrieve you may need to consider other ways to recreate a patient's record. The following are examples of steps you can take to retrieve information from other sources:

- Check if hard copies of results or referrals have been retained (e.g. in secure disposal bins)
- Pathology/imaging companies can provide copies of recent results and reports.
- Specialists should contact referring GPs for copies of letters sent back to them outlining consultations with patients.
- GPs can contact specialists for copies of referral letters.
- Local pharmacies may have medication histories.
- Nursing homes will have medication charts/notes.
- Hospitals can provide discharge summaries.

Reporting requirements

Check if the incident is a notifiable data breach that needs to be reported to the Office of the Australian Information Commissioner and patients under the Notifiable Data Breach scheme.

Consider whether the breach is likely to result in 'serious harm'. If the data remains encrypted, has not been transferred from the system and is not being used by the hackers the breach will not necessarily cause serious harm. This should be considered with your IT service provider or forensic specialist.

You may also wish to report the incident to the ACSC, which uses cyber security incident reports it receives as the basis for providing assistance to organisations.

For more information

For more information on notifiable data breach see Data Breaches: all you need to know

For more information on responding to a cyber security incident see the Australian Cyber Security Centre's Preparing for and Responding to Cyber Security Incidents

For more information preparing a data breach response plan under the Privacy Act see oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response#part-2-preparing-a-data-breach-response-plan

For more information on a data breach response plan for the My Health Record see oaic.gov.au/updates/videos/data-breach-requirements-in-the-my-health-record-system/

Avant mutual
by doctors for doctors

1800 128 268
avant.org.au