Responding to a cyber security incident

Quick guide

- When responding to a cyber security incident it is critical to respond in a timely manner
- Seek immediate help from your IT provider/forensic specialist as soon as you have identified a cyber security incident
- Having a business continuity and disaster recovery plan is critical to allow you to continue to care for your patients during a cyber security incident

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.

A cyber security incident is an event or a series of events that compromise or threaten to compromise the confidentiality, integrity, or availability of information or information systems. These incidents can range from simple attacks like phishing or malware infections to more sophisticated attacks like network breaches, ransomware attacks and advanced persistent threats. Cyber security incidents can also lead to the theft of sensitive patient information, financial losses and reputational damage to yourself and the practice, and disruption to critical operations.

Recognising an incident

Recognising a cyber security incident is not always easy as they can take many different forms and can be subtle or sophisticated. There are some signs you can look out for that may indicate you are experiencing a cyber security incident.

- Unusual activity on your computer or network, such as new software installations, unauthorised access attempts or unusual network traffic.
- Unusual pop-ups or warning
- Changes to system settings such as a change in your browser homepage without your knowledge or consent
- Unexplained slowdowns or crashes
- Unexpected emails or messages.

If you experience any of these issues and suspect that you are experiencing a cyber security incident, it is important to take immediate action.

Responding to an incident

There are several things you can do to help minimise the impact of a cyber incident and prevent them in the future.

- **Disconnect from the internet.** If you suspect that your computer or network has been compromised, disconnection from the internet can prevent the attacker from accessing your system or stealing your data.

- **Turn off all computers.** Remove the power cord from the wall and do not connect the back-up data or any portable devices such as laptops to the network.
- **Alert your IT service provider or forensic specialist.** It is important to report any cyber security incidents to your IT service provider or forensic specialist as soon as possible. They can help you investigate the issue and take the necessary steps to mitigate the damage.
  Have the number for IT service provider/forensic specialists somewhere, so you do not require computer access to locate it. Your IT service provider or forensic specialist should also be able to identify if any of your patient records or other data has been lost or exfiltrated.

Retrieve backups

You should be able to retrieve medical and other practice records from your back-up files if the files have not been infected. The Australian Cyber Security Centre (ACSC) recommends back-up files be retained for at least three months. Check all back-up data servers are operating. Disconnect your back-ups when not in use and keep a back-up offline, and at a secure location offsite.

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

- are regularly tested for viability so they can be used when needed; and
- contain all the information needed to run your practice such as medical, accounts and personnel records.

The ASCS has further information on how to back up your files and devices. How to backup your files and devices | Cyber.gov.au

Responding to a ransomware demand

If a ransomware email or message is detected which demands money or Bitcoin, you must decide how to respond. The ACSC and the police advise against paying ransom demands as doing so does not guarantee your files will be restored, nor does it prevent the publication or sale of any stolen data. It may also increase the likelihood of your practice being targeted again. It can increase the viability of the ransomware market putting other healthcare practices at risk.

In response to a ransom 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?
- How much are the cyber criminals demanding to release your data? What are the likely financial costs if the ransom is not paid? For example, 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 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 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. For example you may have to revert to paper and treat every patient as a new patient.

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 that the medical records system is unavailable so you will need some information from them. You may also 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. secure disposal bins)
- Pathology/imaging companies can provide copies of recent results and reports.
- Specialists should contact GPs for copies of referral letters and vice versa.
- Local pharmacies may have medication histories.
- Nursing homes will have medication charts/notes.
- Hospitals can provide discharge summaries.

Communications with patients and providers

Develop a plan for what you are going to tell patients, other providers, external stakeholders and the media. Your communications to patients will be different if data has been lost or exfiltrated, or if data has been encrypted but not lost.

We recommend you have a communications plan that covers how to deal with media inquiries and external stakeholders. In the case of a significant incident, consider obtaining advice from a public relations company.

Reporting requirements

If patient data has been lost, the incident may be a notifiable data breach that needs to be reported to the Office of the Australian Information Commissioner and impacted persons under the Notifiable Data Breach scheme. See Avant's Notifying a data breach under the Notifiable Data Breach scheme for further guidance.

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 reports as the basis for providing assistance to organisations.

References and further reading

Avant resources

- Avant – Data Breaches: all you need to know
- Avant – Avant – Data breach notification under the Notifiable Data Breaches Scheme
- Avant – Notifiable data breach flowchart

Australian Cyber Security Centre

- Preparing for and Responding to Cyber Security Incidents | Cyber.gov.au
- How to backup your files and devices | Cyber.gov.au

For more information preparing a data breach response plan under the Privacy Act.

- Data breach response plan | OAIC

A data breach response plan for the My Health Record

- My Health Record Data Breach Response Plan (oaic.gov.au)

For more information or immediate medico-legal advice, call us on **1800 128 268**, 24/7 in emergencies.
avant.org.au/mlas

avant.org.au/avant-learning-centre