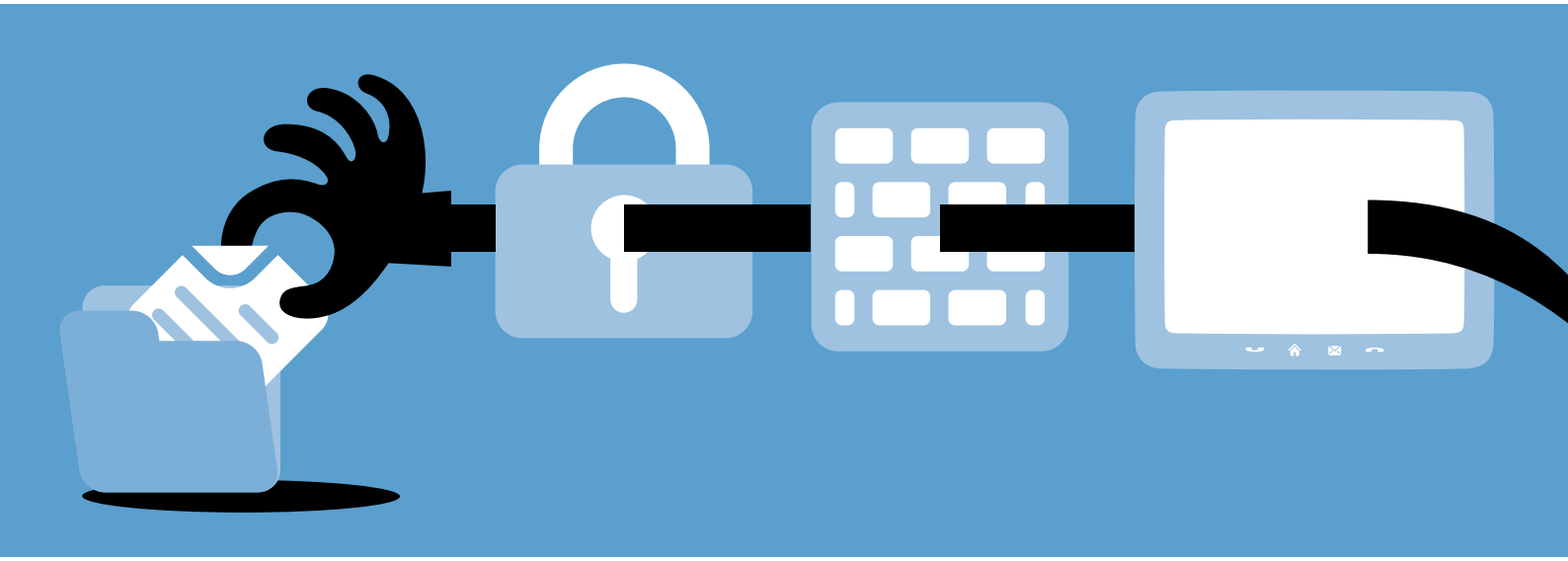
RACGP
Royal Australian College *of* General Practitioners

Healthy Profession.
Healthy Australia.

Fact sheet

Responding to a cybersecurity incident



Just as practice staff must prepare for medical emergencies and natural disasters, your practice should be prepared for a cybersecurity incident.

A cybersecurity incident can be devastating for a general practice. In addition to the very serious risk of compromising patient data and other sensitive information, it can lead to financial loss, reputational damage, possible legal liability, identity theft, and potential for loss of access to critical business systems, resulting in downtime.

Healthcare businesses are particularly vulnerable to cyber threats, because they hold valuable data and are seen as a 'soft target'.[1] Malicious or criminal attacks accounted for over 60% of all notifiable data breaches in 2019.[2,3]

The Royal Australian College of General Practitioners (RACGP) recommends that all practices develop a cybersecurity incident response plan. The current document can be used to help you develop your plan, or respond to an incident in the event that you don't have an appropriate plan in place.

Signs of a cybersecurity incident

A cybersecurity incident is an event involving an information system, service or network, and can include attempts to steal data, money or intellectual property; destroy data; or prevent computers or networks from operating.

It might involve:[4]

- suspicious system or network activity
- receipt of emails with suspicious attachments or links
- unauthorised access to a system, or attempts to access a system
- suspected tampering of electronic devices.

20893.6

Signs that you might be experiencing a cybersecurity incident include:[5]

- being unable to access a network or system accounts
- passwords not working
- computer hard drive running out of space
- data missing or appearing altered
- computer taking a long time to start up, or starting up incorrectly
- computer running slower than usual
- computer crashing frequently for no discernible reason
- practice email accounts sending spam to contacts
- pop-up ads continually appearing
- internet browser automatically directing you to unsafe or suspicious websites.

Common cybersecurity incidents affecting general practice

Phishing

Phishing refers to the use of fake websites or deceptive messages sent via email, SMS, or direct messaging through social media networks. Phishing messages and sites are designed to appear as if they are from individuals or organisations you know. The aim of phishing is to gain confidential information, such as passwords, identifying information or credit card details.[6]

Malware

The term 'malware', short for 'malicious software', refers broadly to any use of code or programs to cause harm. Possible results of a malware attack include the theft of confidential information, transfer of funds or the secret installation of files on a computer.[7]

Ransomware

Ransomware is a type of malware that renders the computer or its files unusable, then issues a ransom demand for access to be restored. Ransomware can infect the device when the user clicks a link or opens an attachment on a deceptive email, visits a malicious website, or downloads a useful-looking file from a peer-to-peer network. Typically, the computer's files are encrypted and the user is instructed to pay the ransom in the form of cash or cryptocurrency.[8]

Website defacement

Changing the content of a website without authorisation is known as website defacement or website vandalism. It can involve making obvious changes, like leaving 'graffiti', or tampering with code with the aim of infecting others' computers with malware.[9]

How to prepare for a cybersecurity incident

All general practices should have a cybersecurity incident response plan in place and test it regularly. The Australian Cyber Security Centre (ACSC) provides guidance on developing a cybersecurity incident response plan, including the types of information it should contain and potential impacts to consider. For example, such a plan should include an analysis of threats specific to healthcare businesses and a plan for each type of threat. The theft of patient data will have a different impact and response to website defacement, and this should be reflected in the plan.

How to prevent a cybersecurity incident

Taking steps to prevent a cybersecurity incident before it occurs is also important:

- Ensure appropriate firewall and intrusion detection hardware and software is in place on all devices used in the practice.
- Ensure software and hardware are updated and upgraded as needed.
- Develop and implement practice policies for the use of systems, internet, email and mobile devices (and who can use particular systems, devices and software).
- Use strong password controls on all applications.
- Provide training for staff on how to identify risks to practice information systems and report suspicious activity.
- Periodically test the effectiveness of the practice's information security controls and audit access to servers.
- Engage an IT specialist to consider technical issues and solutions (eg disabling macros, email filtering, geo-blocking, 'blacklisting' and 'whitelisting' websites, multifactor authentication and data encryption).

The RACGP resource *Information security in general practice* provides detailed information on how to prepare for a cybersecurity incident.

How to respond to a cybersecurity incident

Phase 1: Contain and report

Limit the damage

If you suspect a cybersecurity incident has occurred, turn off all computers in the practice and remove their power cords from the walls to try to isolate the affected systems. Do not connect backup systems or portable devices such as laptops to the network, as this can spread an infection.

Enact your cybersecurity incident response plan

Next, carry out your cybersecurity incident response plan. Ensure that relevant staff members are aware of their roles in carrying out the plan.

Seek help

Contact your IT provider or a forensic IT specialist so that they can identify the cause of the cybersecurity incident, limit further damage by containing and eliminating the threat, and repair and restore your key business systems. Consider how best to contact these people, as it may be safest not to use your practice email accounts.

Consider whether you need to contact police and/or your medical defence organisation. Your practice may also have insurance that offers specific coverage for cybersecurity incidents.

Report to relevant authorities

A cybersecurity incident can result in a data breach, where personal information held by the practice is lost, or is disclosed or accessed without authorisation.[10] Data breaches satisfying particular criteria are subject to a mandatory notification process. To determine whether the cybersecurity incident needs to be reported to the Office of the Australian Information Commissioner (OAIC) and patients, refer to the RACGP's fact sheet and flow chart on the Notifiable Data Breaches scheme.

The ACSC asks that individuals and organisations who have experienced a cybersecurity incident use their site ReportCyber. Reporting assists the ACSC in developing advice, capabilities and techniques to prevent and respond to cyber threats, which helps them to disrupt criminal operations.

Avoid responding to a ransom demand

If you're faced with a ransomware demand, it's best not to pay. There are no guarantees that the files will be decrypted if you pay the ransom, and paying makes you vulnerable to being attacked again as it marks you as an easy target.

No More Ransom!, an initiative supported by the Australian Federal Police and international law enforcement and IT security companies, provides free advice on recovering data without paying cybercriminals.

The ACSC advises victims of a ransomware attack to report the infection, seek help from an IT professional, consider the data lost and use backup files.[8]

Phase 2: Continue care

Retrieve backups

Your practice should already have a policy pertaining to backups and a reliable backup system that allows you to access business-critical and clinical information when disaster strikes. Your IT provider can help you safely retrieve your backup data without compromising your systems further.

For more information about creating and enacting a backup strategy, refer to the following RACGP resources:

- *Guide to information backup in general practice*
- *Information security in general practice*

Manage reputational damage if necessary

General practices should be prepared for media attention if a data breach has occurred. Your cybersecurity incident response plan should include details on how to manage media and respond to patient, stakeholder and community concerns in the wake of the incident.[11]

Resume practice

Enact your business continuity plan. A business continuity plan gives your practice a pathway back to delivering patient care following a major system failure. Such a plan should include information on the following functions of the practice:[12]

- Providing clinical care without access to patient health records
- Scheduling appointments
- Billing
- Issuing prescriptions
- Critical financial operations, such as payroll and Medicare claims

More information on business continuity planning is available in *Information security in general practice*.

Reception and clinical staff may need to use paper-based systems as an interim measure, such as hard-copy appointment diaries and paper script pads. Appropriate steps must be taken to secure those records. Any information collected on paper should be added to the patient's electronic medical record once the incident is resolved.

If you are unable to access backups, you may need to retrieve patient information from other sources to resume clinical care. Possible sources include My Health Record, pathology/imaging companies for recent results and reports, specialists for copies of letters and referrals, pharmacies and nursing homes for medication histories, and hospitals for discharge summaries.[13]

Phase 3: Consolidate learning

Review

When the threat has been contained, you have an opportunity to assess the situation and identify any systems or processes that need changing. Some issues to consider:

- Do you have appropriate practice policies on the use and security of your devices (including removable storage devices) and who can use them?
- Do staff at the practice have mandatory training in maintaining cybersecurity and recognising a cybersecurity incident? What level of training do staff need?

- Are staff aware of their roles and responsibilities in the event of a cybersecurity incident?
- Do you need to upgrade particular devices?
- Do you need to update particular software (eg clinical information system software, antivirus software, email software)? Are the latest security patches applied to all software programs and operating systems?
- Do you need to engage new service providers (eg IT specialists)?

Update your plans

When you have reviewed your response to the incident, make any necessary changes to your cybersecurity incident response plan and, if relevant, your disaster recovery plan and business continuity plan. All of these documents should be reviewed periodically.

References

1. Martin G, Martin P, Hankin C, Darzi A, Kinross J. Cybersecurity and healthcare: How safe are we? BMJ 2017;358:j3179.
2. Office of the Australian Information Commissioner. Notifiable Data Breaches Statistics Report: 1 April to 30 June 2019. Sydney: OAIC, 2019.
3. Office of the Australian Information Commissioner. Notifiable Data Breaches Report: July–December 2019. Sydney: OAIC, 2020.
4. Australian Signals Directorate, Australian Cyber Security Centre. Preparing for and responding to cyber security incidents. Kingston, ACT: Australian Cyber Security Centre, 2020. Available at www.cyber.gov.au/publications/preparing-for-and-responding-to-cyber-security-incidents [Accessed 31 July 2020].
5. Australian Government business.gov.au. How to create a cyber security policy. Canberra: Australian Government, 2019. Available at www.business.gov.au/Risk-management/Cyber-security/How-to-create-a-cyber-security-policy [Accessed 31 July 2020].
6. Australian Signals Directorate, Australian Cyber Security Centre. Phishing – Scam emails. Canberra: ACSC, 2020. Available at www.staysmartonline.gov.au/protect-your-business/recover-when-things-go-wrong/phishing-business [Accessed 31 July 2020].
7. Australian Signals Directorate, Australian Cyber Security Centre. Malware. Canberra: ACSC, 2020. Available at www.staysmartonline.gov.au/protect-yourself/recover-when-things-go-wrong/malware [Accessed 31 July 2020].
8. Australian Signals Directorate, Australian Cyber Security Centre. Ransomware. Canberra: ACSC, 2020. Available at www.staysmartonline.gov.au/protect-your-business/recover-when-things-go-wrong/ransomware-business [Accessed 31 July 2020].
9. Australian Signals Directorate, Australian Cyber Security Centre. Website defacement. Canberra: ACSC, 2020. Available at www.cyber.gov.au/acsc/view-all-content/glossary/website-defacement [Accessed 3 August 2020].
10. Office of the Australian Information Commissioner. Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth). Sydney: OAIC, 2019. Available at www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response [Accessed 31 July 2020].
11. Avant Mutual. Responding to data breach. Sydney: Avant, 2018. Available at www.avant.org.au/Resources/Public/responding-to-data-breach [Accessed 31 July 2020].
12. The Royal Australian College of General Practitioners. Information security in general practice. East Melbourne, Vic: RACGP, 2018.
13. Avant Mutual. Responding to a cyber security incident. Sydney: Avant, 2019. Available at www.avant.org.au/Resources/Public/Responding-to-a-cyber-security-incident [Accessed 31 July 2020].

We acknowledge the Traditional Custodians of the lands and seas on which we work and live, and pay our respects to Elders, past, present and future.