Cybersecurity Threats in Healthcare

Reading time:
Tom Wilson
Date created: 15/01/2021

Tags: Medical Practitioner | Dental Practitioner | General Surgery | Technology

There has been an increase in cyberattacks on Australian healthcare data in recent years. There was a marked increase in cyber security incidents between July 2019 to June 2020 according to the Cyber Security Strategy 2020 report[1]. In June 2020, Australia's Notifiable Data Breaches scheme reported 518 breaches over the previous six months, of which the health industry was the highest reporting sector, accounting for 22% of all breaches[2], following the same trend of the previous semester[3]. Despite these alarming statistics, low awareness in industry of this risk still prevails[4].

Healthcare is an attractive target for cyberattacks for two reasons:

1. it is a rich source of highly sensitive information, and
2. its cybersecurity capability maturity is the lowest compared to other industries[5].

Once an individual's health information is breached it can be used for a variety of crimes from identity theft to medical fraud. An individual's health information is valued at a significantly higher value on the dark web than a credit card number; it can sell for up to 20 times more[6].

Current cyber menaces in the Australian healthcare sector

"In Australian cybersecurity, there are only two types of healthcare organisations – those that know they've been hacked and those that don't know they've been hacked[7]" .

Earlier this year, Offner et al (2020)[8] analysed recent trends in healthcare cybersecurity breaches in Australia and worldwide. The authors identified several threats and attacks summarised below.

Threat category	Attack type	Definition
Accessibility and Integrity	Hacking	Using a computer to access unauthorised data to enable theft or destruction.
	Phishing	Indiscriminate scam emails that contain computer codes created with malicious intent. This allows attackers to enter systems by installing a virus or by enticing users to reveal personal information.

	Sinkhole	Medical device compromise at network level which diverts all network traffic to a compromised sensor node. It is an active attack, which can escalate to denial of service.
Accessibility, Integrity and confidentiality	Ransomware	Encrypts files on compromised computers installing malicious software that demands a fee or 'ransom' to be paid before allowing the system to function again. Potentially life threatening as decryption key may not be provided after payment.
	Malware	Computer code created with malicious intent. Can be masqueraded as legitimate upgrades to disrupt an entire organisation or lie dormant until initiated.
	Command and Control Obfuscators	Has been used to exploit Windows vulnerabilities, can re-direct network traffic to alternate hosts/ports.
	Lateral Movement Frameworks	A continued penetration tool that escalates privileges, collects credentials, and allows information download.
	Wormhole	Attack where two attackers to sensitive data locate themselves strategically in the network. They can listen and record the wireless information being transmitted.
	Spear phishing	Carefully targeted emails to small groups or individuals using personalised information to 'verify' the message and links.
Confidentiality	Hello Flood	Attackers with high powered transmitters can create a signal to broadcast data to the entire network.
Accessibility	Distributed Denial of Service (DDoS)/Denial of Service (DoS)	These are the main threats to the availability of physical and network systems. They create traffic jamming, disrupt communication through interference or collision, and exhaust network resources making it unavailable to the authentic users. Able to spread by mobile applications and can also extra filtrate information.

Table 1: Common healthcare systems' cybersecurity attacks and threats. Adapted from Offner (2020)[8].

In the general practice setting, cyber-attacks commonly occur as phishing, malicious software, ransomware, or as attacks on websites which alter the visual appearance of it[9]. Across the entire health industry, the latest Notifiable Data Breaches scheme reported in June 2020, showed that majority of attacks were attributed to compromised or stolen credentials (phishing or unknown method), malware and ransomware. Human errors included wrong email recipient, unauthorised disclosure, paperwork and device loss, and wrong blank copy recipient in emails.

How to maintain good cyber hygiene in your practice

In order to reduce the risk of cyber-attacks, a combination of technical and behavioural strategies should be implemented. Some recommendations:

- Actively encourage staff to critically examine the authenticity of any electronic communication that is different from regular work. Teach them to challenge the sender details, address and context and if in doubt, ask them to not open and seek advice of your organisational security team.
- Staff cybersecurity education has been identified as the most important strategy against data breaches[10]. Educate your staff about the potential dangers of malicious email attachments and, specifically, why they should never 'verify' any details from an email, click on hyperlinks or open unknown attachments.
- Implement additional strategies to confirm that websites are genuine, including two-factor authentication and use of user-selected images in login pages for verified sites.
- Never reply to text messages or emails asking your personal information.
- Whenever possible, increase the use of multi-factor authentication, which makes it harder for cyber criminals to access sensitive data.

Responding to cyber-attacks according to standards of best practice

Anytime an organisation's secure information is compromised, lost, accessed or disclosed without the required authorisation, there is a data breach incident. Any endpoint and any connection within a network can be vulnerable to a cyber-attack. Even though protecting every entry point to a healthcare IT system is unrealistic, having an action plan in case a breach occurs is vital.

The Office of the Australian Information Commissioner recommends a four-step strategy to contain and respond to a data breach incident that affects personal information, including the My Health Record system[11].

Step 1: CONTAIN

As soon as you realise the data breach has occurred, act immediately to prevent further access to, or distribution of, the affected information, and to minimise the likelihood of more damage being done. Follow your organisation's data breach response plan and seek professional assistance if needed.

Step 2: EVALUATE

Assess if the data breach has impacted any personal information and how likely this is to result in physical, psychological, emotional, financial or reputational harm to any person. Ask yourself if remedial action could remove the likelihood of serious damage.

If the data breach has impacted the My Health Record system, this must be reported immediately!

Step 3: NOTIFY

Once you've confirmed that a data breach has taken place, you must quickly notify all affected individuals. Your organisation must also notify the Office of the Australian Information Commissioner as soon as practicable.

If the incident impacts the My Health Record system, you must notify the Australian Digital Health Agency as soon as practicable and the **Office of the Australian Information Commissioner**. Note that public hospitals and health services are only mandated to notify the Australian Digital Health Agency.

Step 4: REVIEW

You should aim to comprehensibly investigate the causes and issues that facilitated the cyber-attack. It is recommended you develop and implement a prevention and response action plan to avoid similar incidents happening in the future. You may consider changing your organisational policies and procedures for managing sensitive data and ensure your staff is adequately trained.

The RACGP has published several resources to support healthcare practitioners in managing cyber-attacks, including:

Information security in general practice – how to prepare for a cybersecurity breach

Notifiable Data Breaches scheme – fact sheet and flowcharts to manage notifiable data breaches in general practice

Information backup in general practice guidelines – general practice information technology requirements

Using email in general practice – fact sheet on how to use of email and safely communicate sensitive information

References

[1]Cyber security strategy (n.d.). Department of Home Affairs. Retrieved October 26, 2020.

[2]Notifiable Data Breaches Report: January–June 2020 OAIC.

[3]Notifiable Data Breaches Report: July–December 2019 OAIC.

[4] Gordon, Fairhall and Landman, Threats to Information Security – Public Health Implications.

[5] Coventry, L., Branley-Bell, D., Sillence, E., Magalini, S., Mari, P., Magkanaraki, A., & Anastasopoulou, K. (2020, July). Cyber-risk in healthcare: Exploring facilitators and barriers to secure behaviour. In International Conference on Human-Computer Interaction (pp. 105-122). Springer, Cham.

[6] Raina MacIntyre C, Engells TE, Scotch M, Heslop DJ, Gumel AB, Poste G, Chen X, Herche W, Steinhöfel K, Lim S, Broom A. Converging and emerging threats to health security. Environ Syst Decis. 2018;38(2):198-207.

[7]General practice software and better healthcare systems Retrieved October 26, 2020.

[8] Offner, K. L., Sitnikova, E., Joiner, K., & MacIntyre, C. R. (2020). Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation. Intelligence and National Security, 35(4), 556-585.

[9]Health sector remains biggest reporter of data breaches (Tsirtsakis, A.) Reetrieved 28 October, 2020.

[10] Kruse, Clemens Scott et al. Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends. 1 Jan. 2017 : 1 – 10.

[11]Data breach action plan for health service providers (n.d.). OAIC. Retrieved October 27, 2020.