Cybercriminals love healthcare — AI could be making it easier

4 December 2025

phn
GOLD COAST
An Australian Government Initiative

AGENDA

- Why is Healthcare a target for Cybercriminals? (2 Minutes)
- Top Threats / Risks to GP Practices (4 Minutes)
- What GP's Do to Prevent/Prepare for Cyber Risks (4 Minutes)
- Takeaway - Useful Resources

Why is Healthcare a target for cybercriminals?

phn GOLD COAST
An Australian Government Initiative

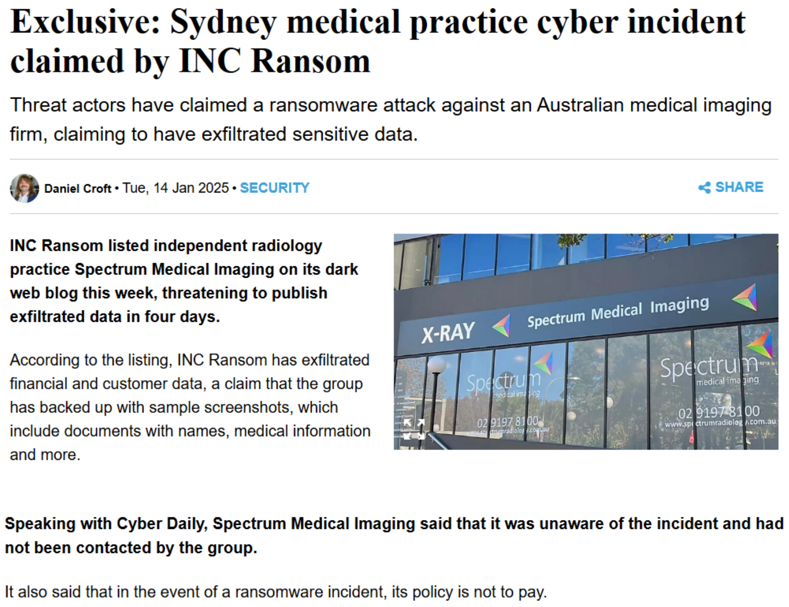
🩺 High-Value Data & Critical Services

- Healthcare organisations hold highly sensitive, valuable patient data — medical history, Medicare numbers, diagnoses, financial info
- This data is extremely attractive to cybercriminals for: identity theft; black-market; fraud; & ransom
- Disruption of healthcare systems (patient records, labs, imaging, prescriptions) can have life-threatening consequences, making healthcare a “critical infrastructure” target

📈 Rising Cyber Threats and Sector Vulnerability

- Research from this year has shown that non-hospital clinical providers (e.g. GP clinics) were among the most targeted sub-sectors, receiving nearly 10× the publicly reported attacks than hospitals
- Rapid digitisation, legacy/low-maturity systems, and widespread adoption of digital tools (EHRs, cloud, AI) increase attack surface and “tech debt,” which threat actor's exploit.

CASE STUDY



Exclusive: Sydney medical practice cyber incident claimed by INC Ransom

Threat actors have claimed a ransomware attack against an Australian medical imaging firm, claiming to have exfiltrated sensitive data.

Daniel Croft • Tue, 14 Jan 2025 • SECURITY

SHARE

INC Ransom listed independent radiology practice Spectrum Medical Imaging on its dark web blog this week, threatening to publish exfiltrated data in four days.

According to the listing, INC Ransom has exfiltrated financial and customer data, a claim that the group has backed up with sample screenshots, which include documents with names, medical information and more.

Speaking with Cyber Daily, Spectrum Medical Imaging said that it was unaware of the incident and had not been contacted by the group.

It also said that in the event of a ransomware incident, its policy is not to pay.

🧩 Rise of AI

- Growing use of AI (i.e. AI scribes) may accelerate risk, as AI-enabled tools increase the number of digital touchpoints and may introduce new vulnerabilities if not properly safeguarded

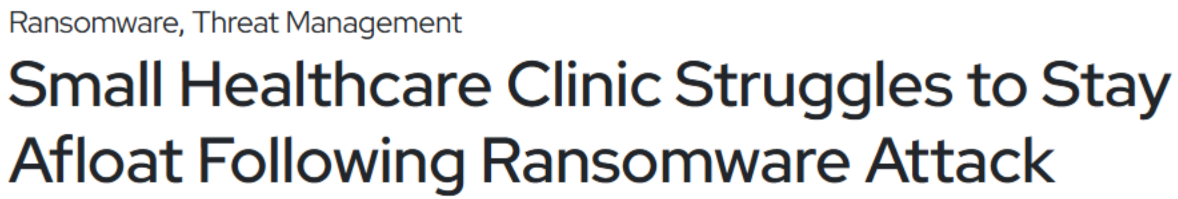
⚠️ Unique Pressure & Low Tolerance for Disruption

- Healthcare cannot simply “pause” — patient care, chronic treatments, prescriptions, pathology—all depend on constant access to digital systems
- Smaller practices often have limited cyber-security resources or budget

Top Threats / Risks to GP Practices

phn GOLD COAST
An Australian Government Initiative

CASE STUDY



Ransomware, Threat Management

Small Healthcare Clinic Struggles to Stay Afloat Following Ransomware Attack

Common Threats GPs Face

📧 Phishing emails: fraudulent emails designed to trick staff into revealing credentials or malware

🌐 Malvertising via search engines / malicious web links: harmful adverts or links that infect systems when clicked

☁ Password/credential compromise in cloud services — weak or reused passwords increase risk

Key Risks for GP Practices

Growing Attack Surface & Cybersecurity Vulnerabilities in Digital/AI Tools

- As practices adopt more digital/AI-enabled tools, the "attack surface" increases — offering more entry points for cybercriminals or data breaches. This overlaps with broader cyber risk to healthcare IT
- Without robust cybersecurity frameworks and regular audits, the risk of ransomware or data breach attacks are increased
- One of the key reasons for payments of ransoms is data breach/data extortion

Use of AI within your Practice

- The rise of using AI within GP practices for tasks like doctor scribing introduces the issue of liability when AI generates incorrect or misleading data
- Lack of formal guidelines/governance frameworks for AI use increase the risk of data breaches, misuse, bias or compliance failures, leading to erosion of patient trust and ethical / liability concerns

What GP’s Do to Prevent/Prepare for Cyber Risks

phn GOLD COAST
An Australian Government Initiative

✅ **Build a Solid Cybersecurity Foundation**

- Adopt a formal cybersecurity & information-security framework
- Assign a designated team member (or external provider) to manage IT / cyber-security responsibilities
- Ensure all software are up to date and patched

@ **Mitigate Common Cyber Threats (Phishing, Credential Theft, Ransomware)**

- Implement strong password policies
- Enable multi-factor authentication (MFA) on all systems where possible
- Use email filtering / spam-filter tools to block suspicious emails or attachments before they reach staff.
- Train all staff to recognise phishing, malvertising, and suspicious links
- Maintain reliable, secure back-up processes (preferably including offline or offsite backups)

☁ **Manage Risks from Digital Transformation & Data Handling**

- Before adopting cloud-based services or AI tools (for admin, diagnostics, record-keeping), evaluate the vendor’s security protocols — data encryption, storage location (onsite vs overseas), retention policies, breach response.
- Ensure compliance with privacy laws
- Establish a culture of security awareness: make cyber hygiene part of staff orientation, training and ongoing operations (e.g. email & device use, secure handling of patient info, device access).

What GP’s Do to Prevent/Prepare for Cyber Risks

📄 Prepare for Incidents & Plan for Recovery

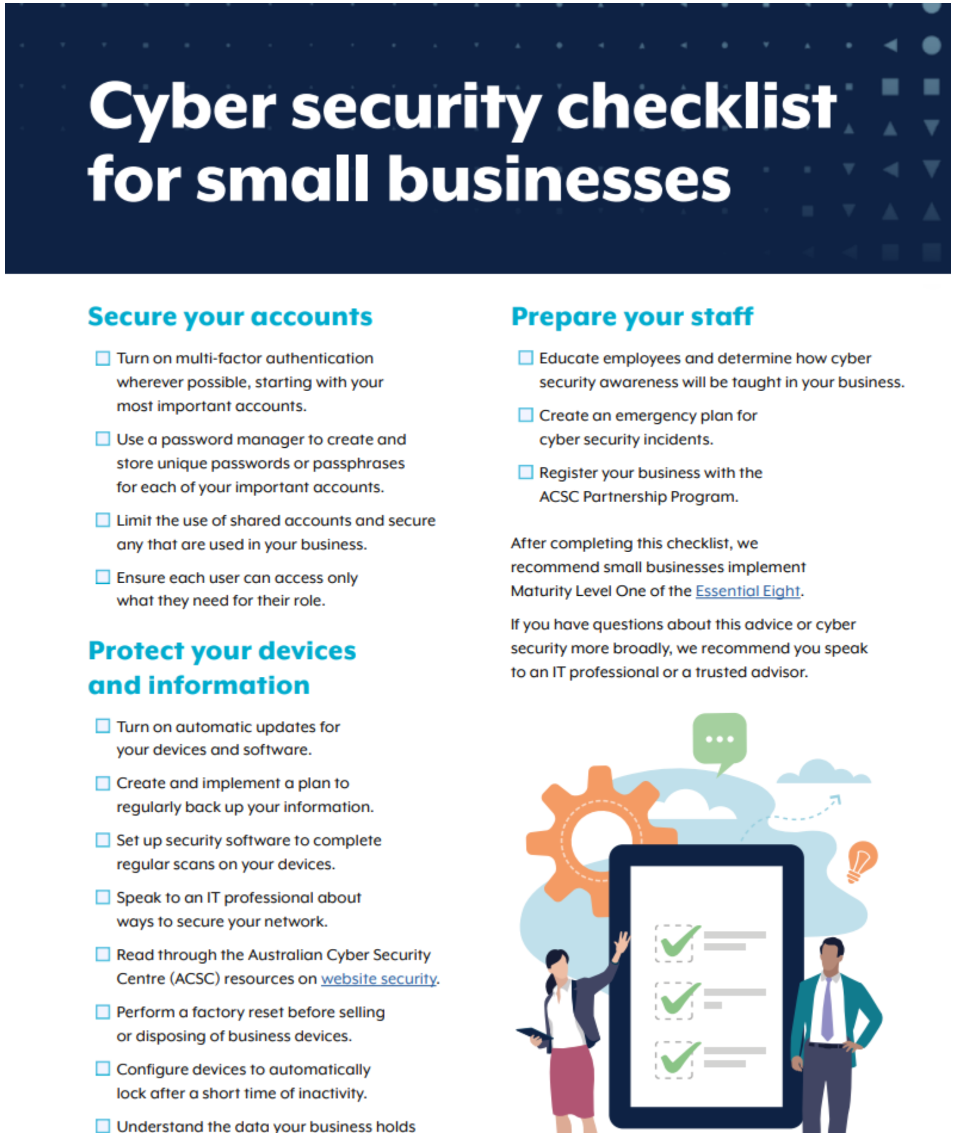
- Develop and maintain a cyber-security incident response plan (to support your BCP)
- Regularly backup and test data recovery processes — practice restoring from backups to make sure recovery works before disaster strikes.
- Engage external IT / cyber-security experts for periodic reviews and audits — especially if using cloud services, remote access, or third-party vendors.

🎯 Key Takeaway for GP Practices

- Implementing simple but consistent cyber-hygiene practices — strong passwords, MFA, staff training, email filtering, secure backups — along with robust policies and incident-response planning, dramatically reduces the risk of breaches.
- Given the sensitivity of patient data and reliance on digital systems, cybersecurity should be considered as important to patient safety and practice resilience as clinical governance.
- Ensure your patients feel confident in the confidentiality of their data if you are using AI in your practice and have information guidance available.
- Help is available!

Useful Resources

phn GOLD COAST
An Australian Government Initiative



Cyber security checklist for small businesses

Secure your accounts

- □ Turn on multi-factor authentication wherever possible, starting with your most important accounts.
- □ Use a password manager to create and store unique passwords or passphrases for each of your important accounts.
- □ Limit the use of shared accounts and secure any that are used in your business.
- □ Ensure each user can access only what they need for their role.

Protect your devices and information

- □ Turn on automatic updates for your devices and software.
- □ Create and implement a plan to regularly back up your information.
- □ Set up security software to complete regular scans on your devices.
- □ Speak to an IT professional about ways to secure your network.
- □ Read through the Australian Cyber Security Centre (ACSC) resources on website security.
- □ Perform a factory reset before selling or disposing of business devices.
- □ Configure devices to automatically lock after a short time of inactivity.
- □ Understand the data your business holds

Prepare your staff

- □ Educate employees and determine how cyber security awareness will be taught in your business.
- □ Create an emergency plan for cyber security incidents.
- □ Register your business with the ACSC Partnership Program.

After completing this checklist, we recommend small businesses implement Maturity Level One of the Essential Eight.

If you have questions about this advice or cyber security more broadly, we recommend you speak to an IT professional or a trusted advisor.

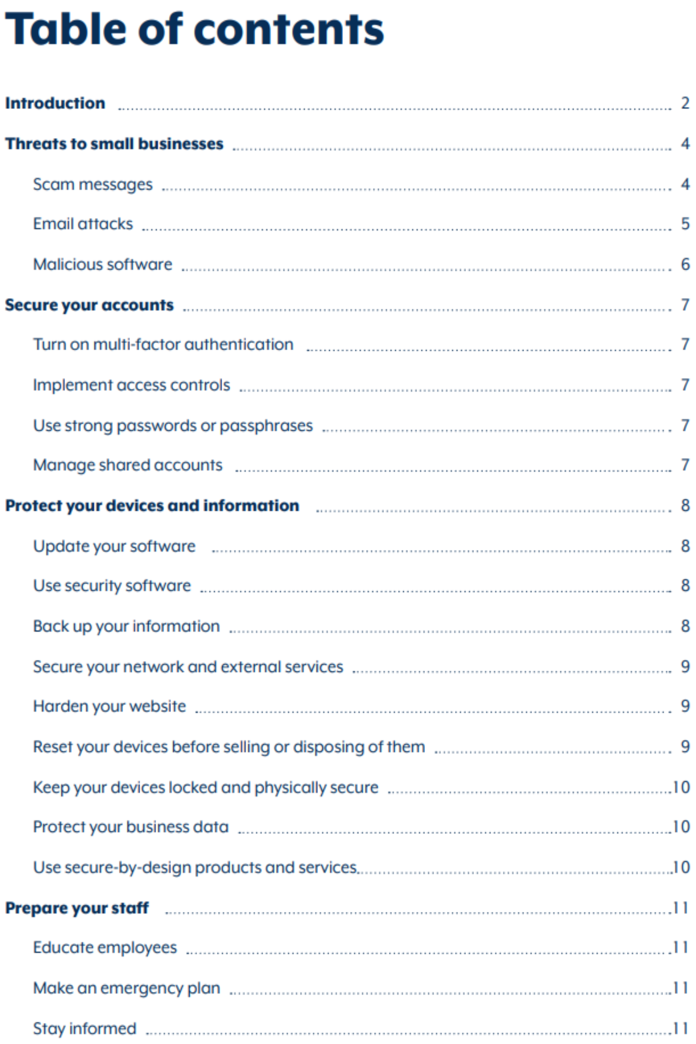
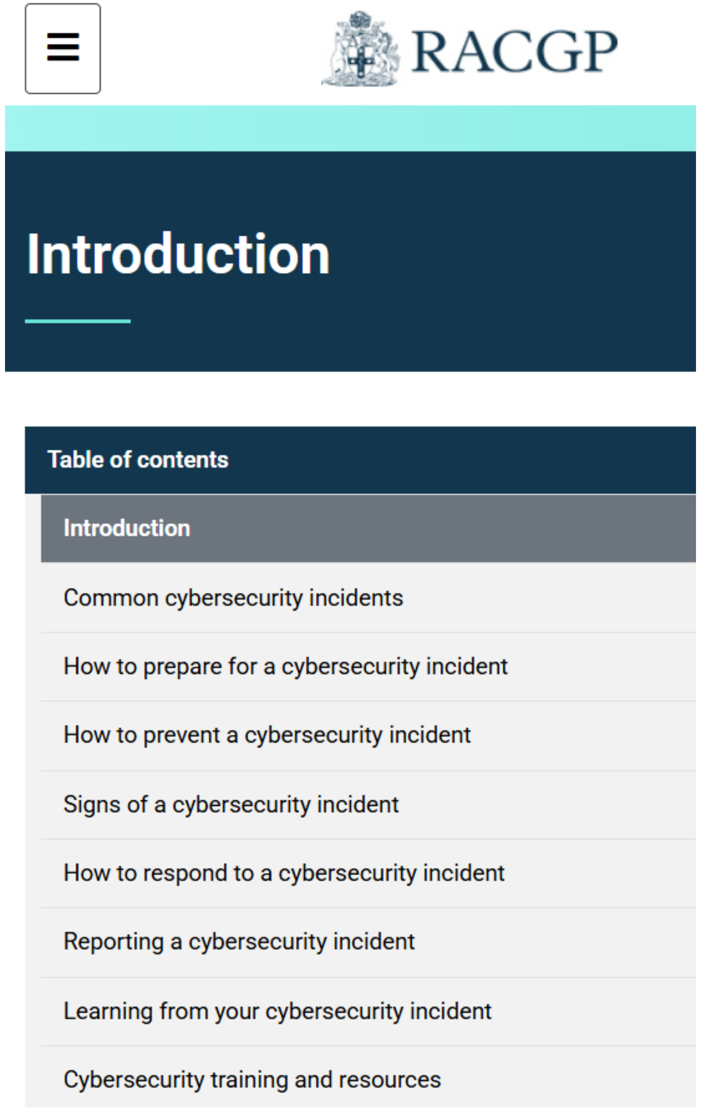


Table of contents



☰ RACGP

Introduction

Table of contents

[Small business hub | Cyber.gov.au]

[RACGP - Information and cyber security in general practice]