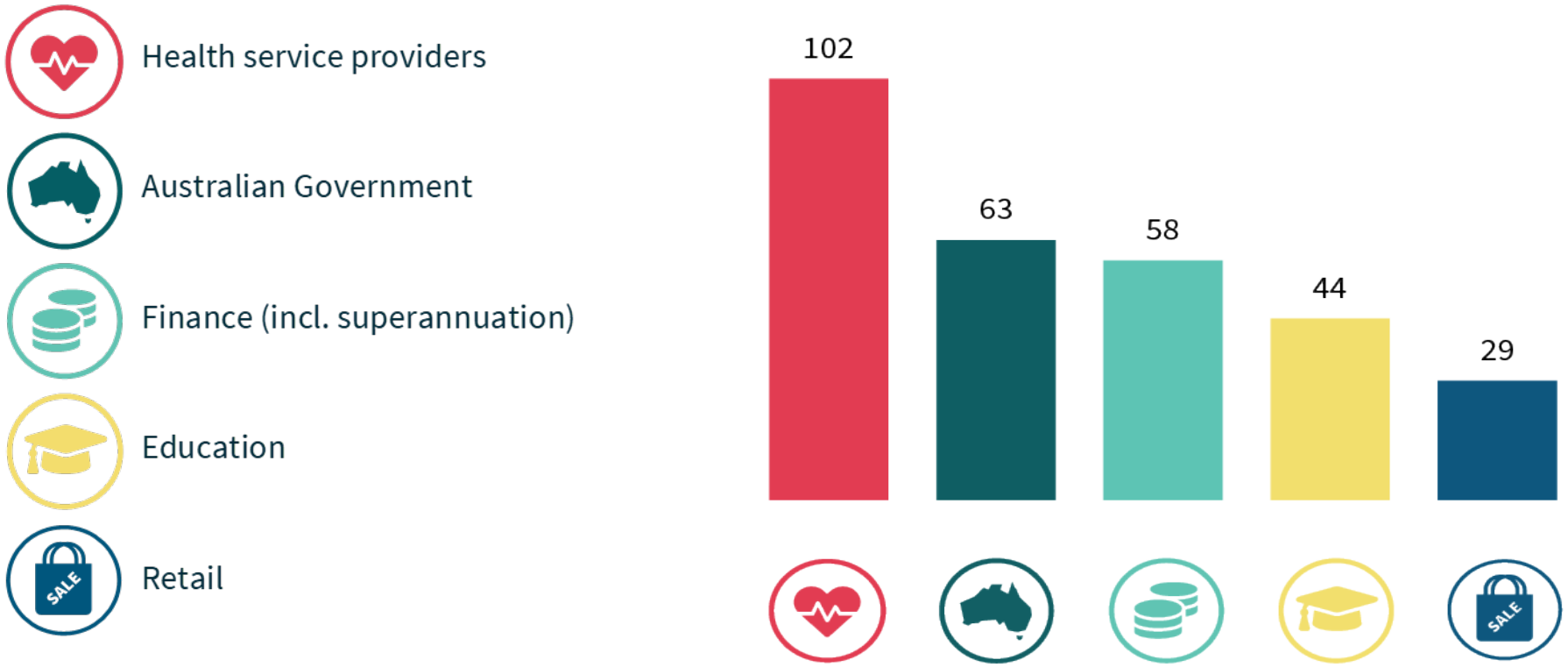
Cyber Security in General Practice

Avant
Practice
Solutions

Top 5 sectors which experienced notifiable data breaches from January to June 2024



Source: Australian Government Office of the Australian Information Commissioner (2024) Notifiable Data Breaches Report; accessed 13 January 2025.

Avant Practice Solutions

Types of cyber security threats

- Phishing
- Malware
- Ransomware
- Theft of patient data
- Insider threats
- Hacked devices

Steps to help protect practices from a cyber security incident

- Policy and procedures
- Business continuity and information recovery plan
- Review and update contracts with third party providers
- IT service provider.

Source: Avant (2024) Steps to protect your practice from a cyber security incident; accessed 13 January 2025.

Avant Practice Solutions

Six steps to help protect your systems

Check your network security controls

- Your IT provider should check network security controls.
- Check how your network and computing systems can be accessed and who will have access.
- Check that all personal computing devices are also secure.

Update your systems and software with patches

Regularly installing operating system (security) and software updates is one of the most effective ways to keep healthcare systems protected against cyber intrusions and viruses.

Use anti-virus and ad-blocking software

Cyber criminals commonly use malicious software (malware) to target computers with viruses, spyware, trojans and worms.

To prevent these attacks compromising your systems, ensure anti-virus software and an ad-blocking browser plug-in is installed and up-to-date, and allow automatic updates from the vendor.

Avant Practice Solutions

Six steps to help protect your systems

Use strong passwords

- Change passwords regularly and/or set a password expiry
- Inform staff they must never share passwords
- Passwords should contain alphanumeric characters and at least one special character (such as !, @, #, $, &, *, ?)
- Change temporary passwords upon successful login.

Use multi-factor authentication

Multi-factor authentication is a powerful security measure that helps provide an additional layer of protection for online accounts, reduces the risk of password-related breaches, and enhances overall security and privacy for users.

Back up your business systems and files

Backing up computer systems and files is crucial to protect against data loss, whether due to hardware failures, software issues, accidental deletion, or security breaches. Hackers may also use malware to deny access to files and can demand a ransom to regain access.

Avant Practice Solutions

Responding to a cyber security incident

1. Recognising an incident
2. Minimising damage
3. Seeking immediate help
4. Retrieving back-ups
5. Responding to a ransomware demand
6. Continuing practice while cyber incident is resolved
7. Retrieving patient information
8. Reporting requirements.

Get in touch with us today

practicesolutions@avant.org.au

1300 469 866

Avant
Practice
Solutions