Cybersecurity

mhcc.org.au

mhcc
mental health coordinating council

Cybersecurity is the practice of protecting systems, networks, programs, and personal data from digital attacks. Cybersecurity risks or threats are typically aimed at accessing, changing, or destroying sensitive information, extorting money from staff or consumers, or interrupting normal processes in an organisation.

Common examples of cyberattacks include ransomware (a type of malicious software that blocks access to the victim's data or threatens to publish or delete it until a ransom is paid) or phishing (cyber attackers pretending to be a reliable source to trick someone into providing personal information). Community-managed organisations can be just as vulnerable as commercial businesses.

Cybersecurity is becoming increasingly important as more services are delivered online and consumers' personal and health information is at risk. Your organisation's approach to privacy should include plans for managing cybersecurity risks and threats.

Good cybersecurity practice is broader than using software to protect against attacks. You can keep your organisation safe through simple prevention measures that are consistently applied, for example, automating software updates or training staff to identify phishing emails. All staff in your organisation can play a part in keeping their personal and professional information safe and developing a culture of ongoing cyber security awareness is important.

Your organisation should also consider purchasing cyber insurance providing cover for first, and third party, exposures, in relation to any cyber or privacy event that impacts your organisation. For example, it may include costs to restore data, legal costs assisting with privacy notifications, or claims arising from network security failures.

Checklist: Cybersecurity

- ☐ Does your organisation have a cybersecurity plan? For example, does your organisation have policies that:
  - assign responsibility and accountability for information security
  - complete and maintain an information and data inventory
  - protect data in transit and at rest
  - protect against interruption, damage or disconnection of the service
  - assess the size and extent of cybersecurity threats
  - consider and mitigate vulnerabilities and threats
  - conduct regular updates, reviews and audits of information security
  - detect, respond and report to the governing body, workforce, service users and their supporters on information security incidents and technical faults.
- ☐ Does your organisation provide cybersecurity training and hold ongoing discussions about cybersecurity? For example:
  - Building security awareness throughout the organisation with the Digital Health Security Awareness eLearning course
  - Keeping your software up to date
  - Training staff to use strong passwords and implement multi-factor authentication
  - Ensuring your organisation backs up data regularly

Continued on next page

- Training staff not to respond to unsolicited phishing emails, texts and calls
- Training staff to have appropriate responses to ransomware
- Subscribing to new alerts for cybersecurity threats

☐ Are there clear procedures in case of a breach? For example:

- notify the Office of the Information Commissioner in the case of a notifiable data breach
- incident logging, response, handling, escalation, and recovery?

Further resources

- The Digital Health Agency's Cyber Security Centre works with the healthcare sector to maintain cybersecurity. It offers free training and offers a number of resources that can assist to community managed organisations.
- The Australian Cyber Security Centre is the Australian Government's leading agency in relation to cyber security. It provides helpful information about common cyber threats, step-by-step guides for improving cybersecurity and more.
- In the event of a cybersecurity breach, contact Australian Cyber Security Hotline 1300 CYBER1 (1300 292 371).