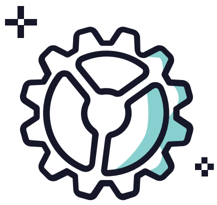
Cyber checklists

INDUSTRIES



Not for Profit

As a not-for-profit organisation you hold highly sensitive private information that may be the target of cyber-attacks. Making sure your organisation is cyber ready is imperative to reducing your risk as a business. To ensure you're across your cyber obligations and responses, you need to:

1. understand what data you hold;
2. understand general cyber risks and those specifically relevant to your industry;
3. take steps to reduce your cyber risk; and
4. be prepared to respond to cyber-attacks if that occur.

Understand your data

Understanding the data you hold is an important part of effectively assessing and reducing your cyber risk. You will likely hold sensitive information about your clients or other individuals, for example if your not-for-profit engages in research activities or community outreach services. That sensitive information could be financial information, including bank account, credit card and tax details, information about individuals' social or political opinions, race, sexuality or religion, or even health information depending upon the types of services and activities your not-for-profit participates in.

You need to be aware of the scope of information you hold about individuals and the risks which are likely to arise in the event of a data breach, which may range from financial harm (including identity theft) to reputational harm and psychological harm. You will also need to consider whether such a breach needs to be reported under the Notifiable Data Breach Scheme set out in the Privacy Act (click **here** for more information).

Understand your risks

You should be particularly wary of cyber-attacks in the form of ransomware, business email compromise and data scraping. Ransomware is malware which encrypts the data on your systems and then demands money in exchange for being decrypted or unlocked, whereas data scraping is where an attacker enters your network to access and export your data. Sometimes, these attacks can occur at the same time, meaning the hacker is able to exfiltrate your data while before your data is encrypted and you are unable to access your systems.

Business email compromise involves a hacker gaining access to one or more of your employees' email accounts and using their email account to imitate your employees and, in most cases, trick your clients into paying money into a fraudulent bank account or providing their login details.

These attacks usually start through phishing attacks, where fraudulent emails are used to trick users into revealing their login information or giving access to their network account or getting them to download malware through a document attachment or link.

Reduce your risk

There are two major areas to focus on to reduce your cyber risk: security systems and employee training.

Security systems

Accepting that not all cyber risks can be eliminated, there are steps you can take to reduce your risk. You should consider seeking the assistance of your IT provider about:

+ Setting up alert systems for suspicious or abnormal email activity.
+ Turning on comprehensive audit logging in your email systems.
+ Requiring employees to update their passwords regularly.
+ Locking user accounts after 3 failed password attempts.
+ Enabling multi-factor authentication.
+ Configuring regular back-ups of your data and regularly testing those back-ups. Ideally, these back-ups will be disconnected from your main server in case your main server is attacked.
+ Regularly updating firewall and anti-virus software.
+ Application whitelisting.
+ Patching applications immediately when a patch is available.
+ Configuring macro settings.
+ Restricting administrative privileges.

Employee training

The single biggest cause of cyber breaches is human error – be it inadvertently downloading malware from email attachments or handing over credentials via genuine looking websites. Therefore, a critical element in safeguarding your systems is employee training.

Training should be organised through your IT provider and be regular and customised according to your systems and internal structures. Training ensures that every employee understands that cyber safety is part of their responsibility and that individuals are on the alert for external threats. Have specific cyber training for employees identified as incident responders in your incident response plan.

See our comprehensive guide on cyber readiness **here**.

Respond to attacks

Responding to cyber-attacks is a three-stage process, outlined in our **Guide to Data Breaches**.