Managing cyber security risks

From report 9: 2021/22 – Cyber Security in Local Government

Office of the Auditor General
Serving the Public Interest

The following table outlines guiding principles for entities to consider when managing their cyber security risks. This is not intended to be an exhaustive list. Further guidance can be obtained from the Australian Cyber Security Centre (ACSC). [1]

Guiding principles	
Understand cyber security risks	Identify and assess cyber risks to systems and information and implement appropriate plans to address them.
Develop a cyber security policy	Develop and implement a cyber security policy that aligns with better practice frameworks such as the Australian Information Security Manual.
Regularly test control effectiveness	Regularly test the effectiveness of security controls which protect against cyber-attacks and address vulnerabilities in a timely manner.
Develop response plans	Develop incident response, business continuity and disaster recovery plans to manage and recover from cyber security incidents. Test these plans regularly.
Secure emails	Secure emails with controls such as sender policy framework and domain-based message authentication. Implement controls to detect suspicious emails and attachments (e.g. phishing).
Educate staff	Develop awareness programs that are not overly technical to educate staff on cyber and information security risks.
Intrusion detection	Implement controls to identify and block malicious intrusions.
Protect endpoints	Use application control and modern anti-malware software to protect endpoints from threats, including mobile devices.
Use encryption	Use encryption to protect data from theft. This should apply to data at rest and in movement and include mobile devices.
Limit administrative privileges	Administrators should have separate accounts to perform privileged tasks. These should be regularly reviewed to ensure only appropriate staff have these privileges and that they still require it.
Apply software updates	Implement processes to receive alerts when patches are released by vendors and apply them to applications and operating system software in a timely manner.
Use passphrases	Develop and implement passphrase policies to manage authentication on supported systems.
Multi-factor authentication	Implement multi-factor authentication to protect systems from unauthorised access.
Backup systems and information	Regularly backup and test restoration of systems and information. Protect the integrity of backups in case the primary dataset is compromised or infected with malware.
Harden user applications	Disable or remove unwanted applications and features such as unnecessary browser plugins and software frameworks.
Cyber security monitoring/ situational awareness	Use event data to know what is occurring on your network. Develop processes to receive alerts if accounts, passwords or vulnerabilities related to your entity are disclosed through breaches.
Collaborate	Liaise with key cyber security entities such as the ACSC and their Joint Cyber Security Centre.

Source: OAG

[1] https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents (current as at 22/11/2021)