

Cyber Optimist Top Eight

Software and Network Security

- ☐ Invest in cybersecurity software, hardware, effective cyber policy development, and security controls.
- ☐ Conduct independent audits.
- ☐ Keep software patched and up-to-date.
- ☐ Employ email and web protection tools.
- ☐ Encrypt data.
- ☐ Implement a centrally managed anti-virus solution.

Vendor and External Party Management

- ☐ Ensure vendors with access to data and systems are actively managed and meet agreed levels of security. Agreements should regulate how vendors meet security requirements.

Training and Awareness

- ☐ Provide regular cybersecurity awareness training for all employees, tailored to real life situations.
- ☐ Provide specialized training for cybersecurity staff.
- ☐ Share challenges and how they were overcome with your network.
- ☐ Help others take steps to secure their systems.

Device Security

- ☐ Implement mobile device management to secure data on laptops, tablets and smartphones. Employ firewalls.
- ☐ Use remote access tools and ensure they are up-to-date.

Incident Response and Planning

- ☐ Develop a formal, documented Incident Response Plan with clear guidelines, roles, and responsibilities.

Physical Security

- ☐ Wherever important information resides, physical controls should be employed.
- ☐ Securely store company laptops or phones.
- ☐ Enable auto lock functions.

Data Backup and Cloud Security

- ☐ Automate back-ups where possible or maintain regularly.
- ☐ Copy your data to a separate, encrypted service, or a device that you can disconnect, store offline, or isolate.
- ☐ Test often.
- ☐ Refer to cloud security guidelines.
- ☐ Select providers that follow and regulations.
- ☐ Use access management, intrusion detection, 24/7 monitoring.

Passwords and Authentication

- ☐ Use "passphrases" instead of passwords.
- ☐ Do not reuse passwords, do not share.
- ☐ Enable MFA.
- ☐ Use a Password Manager.