CYBER SECURITY CHECKLIST

Every day, Australian organisations are targeted by sophisticated cyber-attacks. Our Cyber Security checklist is designed to give you an understanding of critical baseline security practices and identify areas of weakness.

IS YOUR BUSINESS PREPARED FOR A CYBER ATTACK? FIND OUT NOW.

DIAMOND IT

ESSENTIAL EIGHT MATURITY

The Australian Cyber Security Centre's Essential Eight is a series of baseline mitigation strategies taken from the "Strategies to Mitigate Cyber Security Incidents" publication, recommended for organisations, making it harder for cybercriminals to compromise your systems.

- [ ] Application Control – Actively control what software applications, executables and scripts can be installed on work computers and devices through control protocols such as Microsoft block rules.

- [ ] Patch Applications – Automated systems are used in conjunction with Managed IT Services to ensure an 'always on' approach to monitoring and patching all endpoint vulnerabilities.

- [ ] Configure Microsoft Office Macro Settings – Control the configuration of Microsoft Office Macro settings.

- [ ] User Application Hardening – Actively take action to harden and secure user applications by disabling relevant programs and actions.

- [ ] Restrict Administrative Privileges – Authorise administrative privileges to sensitive data on a case-by-case basis and only the required information, and review these privileges routinely.

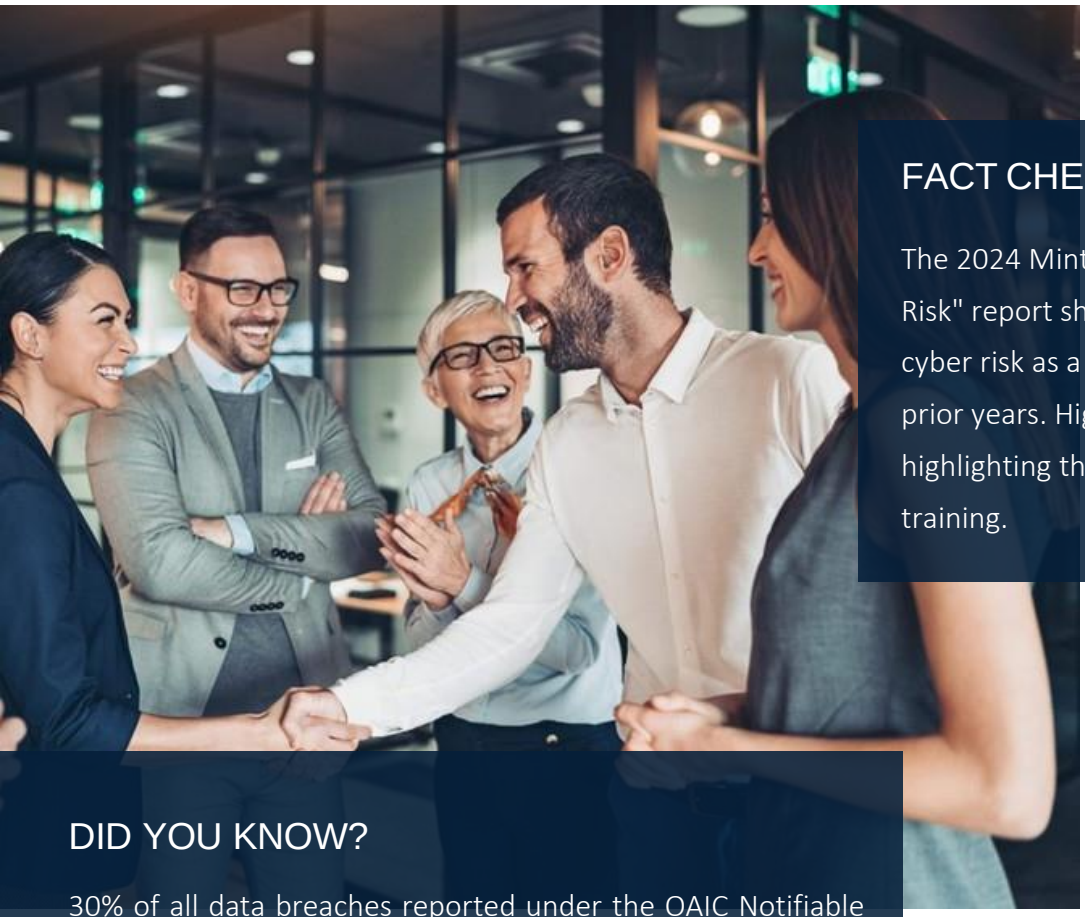
- [ ] Patching Operating Systems – Engage a Managed IT Service Provider to ensure operating systems are continuously monitored and patched.

- [ ] Multi-Factor Authentication – Implement Muti-Factor Authentication across your technology environment, including staff policies and procedures around its required use.

- [ ] Regular Backups – Perform backups daily, and regularly test your Disaster Recovery Plan.

CYBER SECURITY UPSKILLING

- [ ] Provide your employees with annual baseline Cyber Security awareness training.
- [ ] Provide short monthly Cyber Security awareness online refresher sessions that test their knowledge.
- [ ] Ensure your staff know how to safely identify and manage phishing emails and regularly send simulated phishing attacks to test their knowledge.
- [ ] Ensure your employees understand the importance of setting strong passwords and understand safe password storage practices.
- [ ] Regularly review and test the understanding of Cyber Security knowledge within your business to identify any areas of weakness.



FACT CHECK

The 2024 MinterEllison "Perspectives on Cyber Risk" report shows 72% of organisations now rank cyber risk as a 'top 5' priority, up from 56% in prior years. High-profile breaches drive this focus, highlighting the need for stronger cyber security training.

DID YOU KNOW?

30% of all data breaches reported under the OAIC Notifiable Data Breaches Scheme between January to June 2024 were caused by human error.

CYBER SECURITY POLICIES & PROCESSES

- [ ] Ensure your employees have read, understood, and signed off on the following policies and procedures:
  - [ ] ICT Acceptable Usage Policy
  - [ ] Privacy and Confidentiality Policy
  - [ ] Anti-Bribery and Corruption Policy
  - [ ] Internet Access Policy
  - [ ] Email and Communication Policy
  - [ ] Remote Access Policy
  - [ ] BYOD Device
  - [ ] Data Breach Response
- [ ] Ensure your business is aware of its obligations to report data breaches.
- [ ] Implement internal processes to ensure any payment requests from clients or third parties received via email are also verified by a phone call to the original contact number listed.
- [ ] Maintain up-to-date computer and software asset lists.

DID YOU KNOW?

According to the ACCC, Australian businesses lost $2.74 billion in 2023 due to scams.

As of June 2024, the Office of the Australian Information Commissioner (OAIC) reported 527 data breaches—the highest number since late 2020 and a 9% increase from the previous six months.

DID YOU KNOW?

Having policies and a clear process on what is required if you receive a malicious attempt, all form part of this risk reduction activity.

DISASTER RECOVERY AND CYBER SECURITY INCIDENT RESPONSE PLAN

- [ ] Create a Disaster Recovery Plan for your business & ensure it is tested every 12 months.
- [ ] Create a Cyber Security Incident Response Plan & ensure you conduct regular rehearsals with your staff.
- [ ] Ensure your Business Continuity Plan accommodates working remotely if your employees are unable to work from their normal location.
- [ ] Enable a secure and remote backup solution that protects against threats such as Ransomware.
- [ ] Complete regular and systematic reviews of log files and backup logs to make sure there are no errors or suspicious activity.
- [ ] Consider Cyber Insurance as part of your Disaster Recovery Plan.

THE IMPORTANCE OF A DRP

Is your business prepared for when disaster strikes? How will you recover critical business information and restore operations?

Having an appropriate Disaster Recovery Plan in place will help you provide your team clarity as to what is expected of them and what actions must be taken before, during and after a disaster incident.

FACT CHECK

IBM's 2024 Cost of Data Breach Report shows the average data breach cost climbing to USD 4.88 million, up 10%. Stolen credentials caused 16% of breaches at USD 4.27 million, while phishing accounted for 12% at USD 3.59 million.

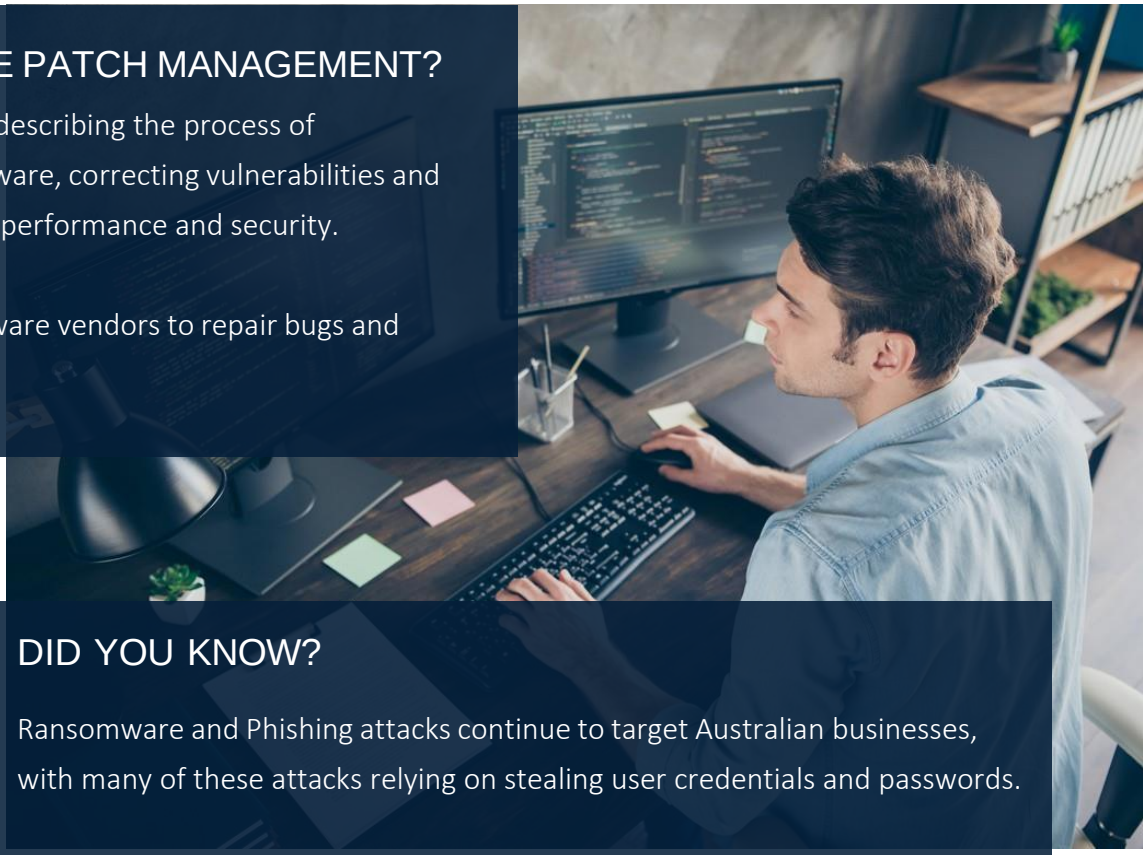
TECHNOLOGY

- [ ] Apply individual permissions to control access to business data.
- [ ] Test the strength of your system security regularly.
- [ ] Engage with independent 3rd party security providers for external penetration reviews of your defences.
- [ ] Ensure all PC's and Laptops on your network have Endpoint Detection and Response Solutions (anti-virus and anti-spam) installed with automatic updates enabled, and/or with software patch management.
- [ ] Ensure your organisation uses a Virtual Private Network if providing remote access.
- [ ] Ensure Multi-Factor Authentication enabled for all business critical systems.

WHAT IS SOFTWARE PATCH MANAGEMENT?

Patching is a term used for describing the process of distributing updates to software, correcting vulnerabilities and improving user experience, performance and security.

Patches are written by software vendors to repair bugs and improve stability.



DID YOU KNOW?

Ransomware and Phishing attacks continue to target Australian businesses, with many of these attacks relying on stealing user credentials and passwords.

Multi-Factor Authentication is a simple security defence businesses can implement to protect their data and reduce the risk of cyber attacks.

HOW CAN DIAMOND IT HELP STRENGTHEN THE CYBER SECURITY POSTURE OF YOUR BUSINESS?

Diamond IT can help your organisation assess your current Cyber Security practices, software, policies and training programs. We can also design security solutions to help protect your business systems and confidential information.

Cyber Security Upskilling & Awareness Training

Cyber Security Upskilling educates staff on the threats and attacks they are subjected to every day. Using multiple platforms, we guide staff through the minefield that is cyber and data security and ensure they have the tools and experience to keep your organisations' systems and data safe. Through face-to-face or online delivery, our ongoing Cyber Security Awareness Training builds an internal culture of security and accountability.

Cyber Security Health Check

Our Cyber Security Health Check identifies hidden weaknesses by using advanced system monitoring tools and expert analysis to detect vulnerabilities and abnormal behaviours within your networks. We deliver a report detailing your organisations' overall Cyber Security health, helping you to understand the:

- Strength of your security and threat prevention.
- Levels of user productivity.
- Network utilisation and performance of your organisation.
- Ability of your backup and recovery plans.
- Accuracy and completeness of your policy and procedures.

Cyber Security Comprehensive

Our Cyber Security Comprehensive offering provides peace of mind with a holistic analysis of your current Cyber Security environment, delivering best practice policy and procedures, detailed data breach and disaster recovery plans, and ongoing Cyber Security awareness training for staff. Ensure your organisation's defences are prepared for a potential cyberattack, with compliant processes and plans to support your business continuity.

SPEAK WITH OUR BUSINESS TECHNOLOGY CONSULTING TEAM TODAY: 1300 307 907

USEFUL LINKS

www.cyber.gov.au

The Australian Cyber Security Centre offers news and tips on how to better secure yourself or your business online, as well as report a scam, cybercrime or identity theft issue.

www.staysmartonline.gov.au

The Australian Government's online safety and security website is designed to help everyone understand the risks and simple steps we can take to protect our personal and financial information online.

https://www.cyber.gov.au/acsc/view-all-content/essential-eight

Provides information to Australian organisations about the Essential Eight, the Essential Eight Maturity Model, and how to apply these strategies to improve your cyber security posture.

www.scamwatch.gov.au

Provides information to consumers and small businesses about how to recognise, avoid and report scams – subscribe for alerts on the latest scams.

https://diamondit.com.au/technology-security

Provides information, tips and examples for Cyber Security, Ransomware and other related updates – subscribe for monthly eNews.

This document has been prepared by Diamond IT. Please note all the information outlined in this report is provided on an “as is” and “as available” basis and you agree that you use such information entirely at your own liability.*

*Diamond IT gives no warranty and accepts no responsibility or liability for the accuracy, or the completeness of the information and materials contained in this report. Under no circumstances will Diamond IT be held responsible or liable in any way for any claims, damages, losses, expenses, costs or liabilities whatsoever (including, without limitation, any direct or indirect damages for loss of profits, business interruption or loss of information) resulting or arising directly or indirectly from your use of or inability to use this report or any reports linked to it, or from your reliance on the information and material in this report, even if Diamond IT has been advised of the possibility of such damages in advance.