OPERATIONAL CONTROLS

1. Have you ever undertaken a security risk assessment?
2. Do you have a written security plan?
3. Do you have written security policies, procedure, guidelines and standards, or use those specified by standards bodies (like NIST or ISO-27001), by vendors (like Cisco), or industry (like PCI-DSS)?
4. Is there compliance with the plan, policies, procedure, guidelines and standards?
5. Have you adopted any approach to gain assurance for cyber security?
6. Do you have a designated cyber security officer who can provide expert guidance, and who is empowered to make enforceable security decision?
7. Have you ever undertaken a security and/or a data audit?
8. Do you implement all of the recommendations arising from security audits?
9. Do you have a disaster recovery plan?
10. Have you ever tested your disaster recovery plan?
11. Do you have agreements and/or infrastructure in place to support a cold site or hot site?
12. Do you conduct criminal history checks on all employees?
13. Are cleaners and contractors ever left unsupervised in your building?
14. Do you have strategies and/or software in place to prevent data exfiltration?
15. Do you have processes in place to detect malicious or unauthorized activity?
16. Do you have an incident response process in place, including communications?
17. Do you have the capacity to undertake a cyber investigation, including forensics, if your systems and networks are compromised?
18. Do you have a cyber security awareness programme for all staff?
19. Do you have a cyber security training programme for all staff?
20. Have staff been evaluated for their likelihood to disclose sensitive information?
21. Have you taken out cyber insurance?
22. Have you ever undertaken a Red Team activity or had a penetration test?
23. Do you have processes to identify and remove unused or inactive users?
24. Have you enabled logging of event data across devices, systems and networks, and is this data monitored?
25. Have you created a risk-rated inventory of all systems, networks and data owned by your organization?

TECHNICAL CONTROLS - SYSTEMS

1. Does every system or device have up-to-date anti-virus protection, including ransomware detection?
2. Are all of your systems password protected?
3. Do you enforce password expiry of 3 months or less?
4. Do you enforce standards for password complexity?
5. Do you use password managers?
6. Have you enabled two-factor authentication to access critical systems and data?
7. Have you setup appropriate groups to support access control, based on the principles of “least privilege” and “separation of duties”?
8. Are your users forced to use access control?
9. Do you have a Standard Operating Environment (SOE)? With the most secure baseline?
10. Do you protect the Master Boot Record (MBR) of each system?
11. Do you force BYOD devices to have the same technical controls as company-owned systems?
12. Do you have a system for encrypting data (files, databases etc) and removeable devices, such as USB memory sticks?
13. Do you use public key cryptography for emails?
14. Are all of your operating systems and applications patched and up-to-date?
15. Do you backup your data and applications?
16. Have you ever tried to restore data and applications and verify that everything operates as expected?
17. Have you disabled all unnecessary network ports, protocols and services on all systems?
18. Have you changed all default passwords on all systems and hardware devices?
19. Have you allocated administrative (or “root”) privileges appropriately and proportionately?
20. Have you disabled local administrator accounts on PCs?
21. Have you implemented application whitelisting?
22. Do you use cryptography to protect the confidentiality of sensitive data?
23. Do you block access to untrusted macros in Microsoft Office products?
24. Have you enabled domain management and/or single sign-on?
25. Have you enabled Data Execution Prevention (DEP) and Address Space Layout Randomisation (ASLR)?

TECHNICAL CONTROLS – NETWORKS, APPLICATIONS, SERVICES and THE CLOUD

1. Do you have a network firewall?
2. Is your firewall configured with the most restrictive set of rules possible?
3. Do you use non-routable IP addresses behind the firewall?
4. Do all of your systems have their own firewall with appropriate rules?
5. Have you enabled IPv6 and/or IPSec?
6. Do you have an Intrusion Detection System (IDS)?
7. Do you have an Intrusion Prevention System (IPS)?
8. Have you designed and deployed a honeypot?
9. Are your hosted applications vulnerable to SQL-injection or cross-site scripting attacks?
10. Do you have a bandwidth manager to limit the impact of DDoS attacks?
11. Have you implemented blackholing and sinkholing to deflect malicious traffic?
12. Do you use an upstream or web content filtering service?
13. Have you disabled all non-TLS services on public-facing interfaces?
14. Do all wifi routers have a minimum of WPA2 authentication?
15. Have all applications been developed using secure coding practices?
16. Have all applications been tested for vulnerabilities, including checks for buffer overflows?
17. Have you enabled the most restrictive configurations for systems, networks and devices where available?
18. Have you changed all default passwords on all databases and applications?
19. Do you log all network events and actively check for intrusions?
20. Have you customized error pages on all web pages to prevent stack trace displays and disclosure of sensitive information, such as physical filesystem paths and source code vulnerabilities?
21. Have you checked all configuration files to make them as restrictive as possible?
22. Do you understand what security controls your cloud provider has in place, and what you are responsible for?
23. Does your cloud provider restrict outbound traffic?
24. Have you restricted SSH and/or Remote Desktop access in your cloud environment?
25. Does your cloud provider have physical access to your encryption keys?

LEGAL AND REGULATORY CONTROLS

1. Have you conducted due diligence on all entities in your supply chain?
2. Have you registered all of your intellectual property in an appropriate way?
3. Do you actively search online for intellectual property breaches?
4. Do you issue takedown notices under the Digital Millennium Copyright Act (1998) or similar legislation where appropriate?
5. Do you monitor your employees’ activity to detect illegal activity which could leave you liable, including the Criminal Code Act 1995?
6. Do you know if your business is subject to the Privacy Act 1988?
7. Have you implemented sufficient controls to comply with the Australian Privacy Principles?
8. Do your policies, procedures, guidelines and standards ensure compliance with the Cybercrime Act 2001?
9. Is your digital marketing compliant with the Spam Act 2003?
10. Are your telecommunications practices consistent with the Telecommunications (Interception and Access) Act?
11. If you process credit card payments, are you compliant with PCI-DSS?
12. Do you know if you are required to report notifiable data breaches to the Office of the Information Commissioner (OAIC)?
13. Are you compliant with the surveillance, telecommunications, cyberbullying, information and privacy protection Acts in your state(s) of registration and/or operation?
14. If you offer financial services, are you compliant with CPG-235, PPG-234, RG-104.93 and RG-104.96?
15. If you are a Director, are you aware of your obligations under the Corporations Act as they relate to cyber security?
16. If you are you an ISP, are you retaining customer data as per the Data Retention amendments to the Telecommunications (Interception & Access) Act?
17. Do you any controls or systems in place to detect fraud?
18. Do you report any suspected cybercrime activity using ACORN?
19. If you sell to or deal with international suppliers or customers, are you aware of the cybercrime laws in their countries that might impact you, such as China’s Cybercrime Law?
20. Are you required to comply with cross-border data flow rules, such as Safe Harbor provisions or EU Binding Corporate Rules?
21. Do you know if you have obligations to remove material that contravenes the provisions of the Online Safety for Children Bill 2014?
22. Are you aware if you have obligations to report under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006?
23. If you sell or provide services to customers within the European Union, are you compliant with the General Data Protection Regulation (GDPR)?
24. Are you aware of the physical location of your cloud data and applications?
25. Are you aware of, and compliant with, the data protection and/or state security laws of the countries where your cloud data and applications are hosted?