4SIGHT RISK PARTNERS | Business Protection & Confidence

CYBER SECURITY
SELF-ASSESSMENT TOOL

FOR CEO'S AND BUSINESS LEADERS

Empowered by

INSURANCE ADVISERNET
Advice you can trust

AUSTRALIAN INSURANCE INDUSTRY AWARDS
WINNER
2018 - 2022

4SIGHT RISK PARTNERS | Business Protection & Confidence

Cyber Security Self-Assessment Checklist
For: CEO's and Business Leaders

Below is a 25-point 'Cyber Security Self-Assessment' Checklist designed to help business leaders assess their knowledge of the cyber landscape, understand their business's vulnerability, and evaluate their threat detection and prevention measures in relation to their cyber risk exposure.

We appreciate that cybercriminals are becoming more sophisticated, and business leaders are finding it increasingly challenging to manage this potential risk, to not only their systems but also to their businesses. It's fair to say that it is not a matter of if, but a question of when your business will be affected by a cyber-attack.

If you answer 'no' or 'unsure' to any of the items below, it is essential that you review your business's cybersecurity measures and coverage. As a business leader, you need clarity despite the complexity of cybersecurity.

4Sight Risk Partners work with our clients to ensure that their cyber risk profile and insurance are current and cover includes (but not limited to)…

- Pecuniary costs and compensation to parties who have had their private information stolen from your systems.
- Mandatory reporting costs.
- Legal costs incurred in defending any civil and regulatory actions.
- Business interruption (loss of income/ profits, trading losses) resulting from a data breach.
- Costs associated with ransomware, threats and extortion.
- Emergency response costs and data and systems recovery costs.
- Regulatory fines.
- Telecommunication fraud.
- Social engineering fraud, phishing, telephone phreaking, identity theft and crypotojacking.
- Hardware repair or replacement costs.

1. Do you comply with the 12 requirements of PCI DSS?
   - ☐ Yes
   - ☐ No
   - ☐ Unsure

2. Do you comply with the Privacy Act? Does your website comply?
   - ☐ Yes
   - ☐ No
   - ☐ Unsure

3. Do you have a formal data protection and Privacy Policy?
   - ☐ Yes
   - ☐ No
   - ☐ Unsure

4. Do all your employees and contractors receive data protection, Privacy Policy induction and annual cyber threat training?
   - ☐ Yes
   - ☐ No
   - ☐ Unsure

5. Do you have firewalls protecting your own and customer/ client data?
   - ☐ Yes
   - ☐ No
   - ☐ Unsure

6. Do you use up to date antivirus software including spyware and malware software?
   - ☐ Yes
   - ☐ No
   - ☐ Unsure

7. How often do you update your antivirus spyware and malware software?
   - ☐ Weekly
   - ☐ When patches are issued
   - ☐ Monthly
   - ☐ Unsure

8. Do you require passwords to be changed regularly?
   - ☐ Yes at least quarterly
   - ☐ No
   - ☐ Unsure

9. Do you have multi-factor authentication in place for remote access to systems (webmail, Citrix desktop, Cloud based applications) as well as a formal Remote Desktop Protocol?
   - ☐ Yes
   - ☐ No
   - ☐ Unsure

10. Do you have an e-mail filtering system (e.g. Mimecast or equivalent) in place that is activated for all email accounts?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure

11. Do you protect all personally identifiable information and other sensitive data through encryption?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure

12. Do you outsource the handling of any personally identifiable information?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure

13. Are all business critical, operational systems and data information backed up and stored at another location? If so, how often is this done?
    - ☐ Yes ☐ Hourly ☐ Daily ☐ Weekly
    - ☐ No
    - ☐ Unsure

14. Has an independent party completed and audit of your system and data security?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure

15. If your IT network failed, is encrypted, infected with ransomware, are you aware of the impact it would have on your business?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure

16. Do you have a Cyber disaster recovery plan or business continuity plan? Has it been tested in the last 12 months?
    - ☐ Yes and it has been tested in last 12 months
    - ☐ No
    - ☐ Unsure

17. Do you have mirrored infrastructure, failure mechanisms, warm or hot sites?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure

18. Do you control, limit, monitor your employees' ability to remove data or information from your network (including USB drive security)?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure
    - ☐ Not Applicable

19. Does your website use Apps?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure

20. Do you use monitored intrusion detection or intrusion prevention systems (IDS/ IPS)?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure

21. Do you deal with international customers?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure
    - ☐ Not Applicable

4SIGHT RISK PARTNERS | Business Protection & Confidence

22. Do you know your annual number of online transactions?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure
    - ☐ Not Applicable

23. Are all new payees, any changes to existing payees' banking details, double authenticated with the payee? Is one authentication done via a direct telephone call?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure
    - ☐ Not Applicable

24. Do transfers greater than $5,000 require dual signature or manager sign off?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure

25. Do you have security measures in place to detect and address threats both pre and post-breach?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure

Reach out to if you would like help reviewing your business's cybersecurity risk profile and coverage.

Gareth Jones
Managing Director
Adviser Representative No: 1251287

0499 988 980 (+61 416 204 492 if calling outside of Australia)
gareth@4sightrisk.com.au
4sightrisk.com.au