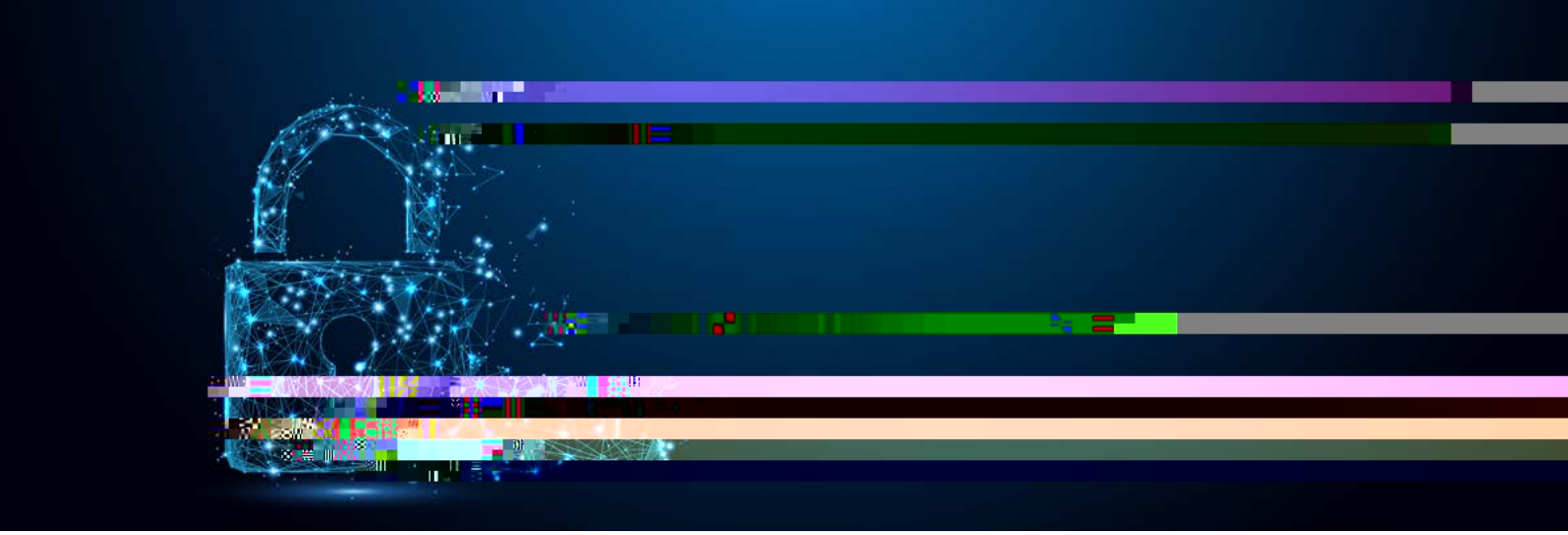

Cyber Security and Data Privacy Audits

- ☐ Have you recently conducted a cyber security and data privacy audit?
- ☐ Do you know exactly how and when you collect data, the types of data you collect, current and proposed uses, location of data (electronic and hard copy), who has access to data, whether you transfer data overseas (including to third party service providers or hosts)?
- ☐ Have you reviewed your IT systems from a cyber security and organisational privacy by design perspective to ensure they are compliant with applicable laws and consistent with company policies?

Tip: If your last cyber security or data privacy Audit was over 12 months ago or pre-2018, you should conduct another audit or takes steps to update existing systems, policies and procedures to ensure compliance with noti able data breach laws and the GDPR. If your business has never done a focused data privacy and cyber security Audit, we highly recommend you do so to ensure you identify critical gaps in compliance and practical steps for recti cation to protect your business and minimise unnecessary risk.

Privacy Policy

- ☐ Do you have an up-to-date, compliant privacy policy?
- ☐ Does your privacy policy cover the list of compulsory items set out in the Australian Privacy Principles?
- ☐ Has your business recently changed its products, services, systems, processes, structure or otherwise evolved and grown?
- ☐ If yes, have you checked your privacy policy to ensure it accurately covers all current purposes

- ☐ Do you have a Data Breach Response Plan?
- ☐ Does your board and staff know what to do to meet mandatory reporting and other legal obligations

- ☐ If your business is online or international, have you considered if the GDPR applies to your business?
- ☐ If so, does your privacy policy comply with the stricter requirements under the GDPR?
- ☐ Do you have systems and processes in place to ensure your business can implement the additional GDPR obligations?

Tip: Given the high penalties and international reach under the GDPR, it is worth seeking advice on whether the GDPR applies to your business and how your compliance stacks up. The GDPR obligations are much stricter than Australian privacy laws and require businesses to take additional steps to protect consumer data rights and control over their data.

- ☐ Have you TJ ET 422(e sy)-6.8 (t583.3835 Tm ( )Tj, 11<</Actd0Tm ([29.2 (n)22.2u3)-9 (l).2 Td-0.34)-6.6 ( )-3.1 T

l-1.9
y(9.52r)28

- ☐ How does your organisation report cyber security and data breach incidents to the Board, if at all?
- ☐ Is there suf cient funding for cyber security and data privacy compliance measures?
- ☐ With human error the most common cause of cyber security and data breach incidents, are staff encouraged to disclose cyber security and data breach incidents to management and the board as part of the organisation's culture?
- ☐ Does the board often discuss cyber security trends and management of customer data?
- ☐ D