THE FUNDAMENTAL 4 IN SECURITY

Unsure where to start with assessing or improving your business' security? Here are Brennan IT's 4 security fundamentals:

1

CONDUCT A VULNERABILITY ASSESSMENT

WHY? Many cyber incidents involve the exploitation of vulnerabilities. Since Australia's *Notifiable Data Breaches Scheme* began, there have been an average of 2.6 breaches reported every single day. 139 data breaches were the result of a malicious or criminal attack, and of these, 69% involved cyber incidents.[1]

HOW? Brennan IT can help by conducting a high-level assessment of your internal and external networks, and determining where potential problems exist. We conduct vulnerability assessment scans and provide you with a report which can help you prioritise risk remediation efforts and help during internal audit or security reviews

2

USE OUR TECHNICAL SECURITY MODIFICATIONS SERVICE

WHY? Your security settings play an essential role in safeguarding your organisation against external threats. Yet many organisations are using dated or inappropriate settings, which limit the effectiveness of testing.

HOW? Brennan IT can review and update your technical security settings so as to harden your overall resilience and remove common exploits typically used during internal penetration testing. When your next internal penetration test is conducted, the tester will need to find other methods to exploit the network, resulting in increased value from the testing and an improved security posture.

3

CONDUCT A USER ACCESS REVIEW AND PASSWORD AUDIT

WHY? Unnecessary access rights and obsolete accounts are among the most common causes of security compromise. The issue and risks are amplified when combined with weak and poor password practices. *Verizon's recent Data Breach Report*[2] showed the use of stolen credentials (hacking) is the number 1 threat action in confirmed data breaches.

HOW? Our team will conduct an account review and password exposure audit against your Windows/Azure active directory domain. The audit analyses active directory to look for different failure types which can leave your organisation vulnerable to an attack.

4

UNDERTAKE A SECURITY MATURITY ASSESSMENT

WHY? As IT environments become increasingly complex and technology changes constantly, it can be difficult to stay on top of your organisation's security or even know where potential issues exist.

HOW? Our team will help you understand your security threats and any associated risks and provide you with a roadmap for mitigating cyber-security incidents and increasing your overall security maturity level.

1 OAIC, *Quarterly Statistics Reports – Notifiable Data Breaches Quarterly Statistics Report*, accessed 20 September 2018, [online], <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics-reports/notifiable-data-breaches-quarterly-statistics-report-1-april-30-june-2018#executive-summary>

2 *Verizon, 2018 Data Breach Investigations Report, 11th Edition*, accessed 4 February 2019, [online], <enterprise.verizon.com./resources/reports/DBIR_2018_Report.pdf>

BRENNAN IT