Is Privacy and Data Security one of your key Risks?

New Notifiable Data Breaches requirements

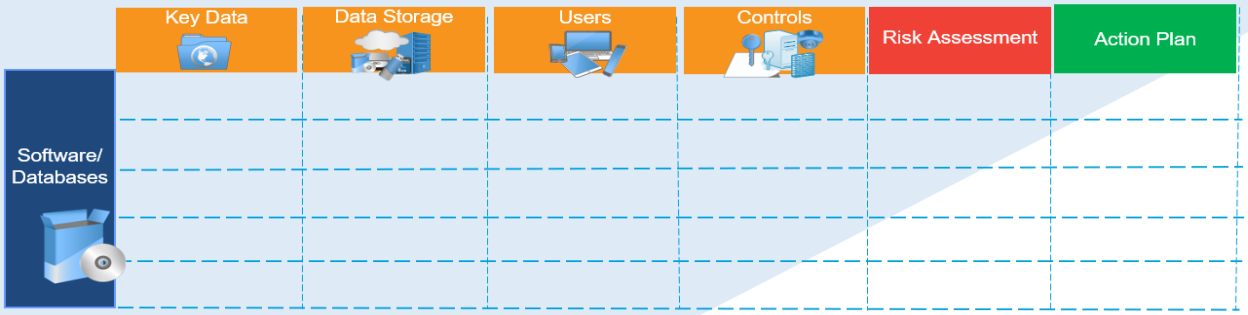
On 22 February 2018, the cost of poor data security increased significantly and this should be flashing red on Board's and Executive's agendas. The Privacy Amendment (Notifiable Data Breaches) Act 2017 requires entities with a turnover of more than $3m to have appropriate security controls in place to protect "personal" data and if that data is lost or inadvertently disclosed, processes in place to report and rectify the breach. Failure to respond appropriately could result in penalties up to $360,000 for individuals and $1.8m for organisations.

These days, to obtain a competitive edge, organisations are collecting and storing more personal information. This has resulted in the proliferation of digital and social media platforms, internet enabled devices, online shopping and use of cloud-based services. At the same time there has been an explosion in cybercrime, where the "dark net" monetises stolen data. The Australian Cyber Security Centre says the cyber threat is undeniable, unrelenting and continues to grow.

So what do Boards and Management need to do?

This is an ideal time to obtain a comprehensive understanding of the risks to the security of your key data. JNW encourages organisations to start with a data inventory self-assessment to determine what key data is maintained, where is it stored, who uses it, how is it accessed and what controls currently support its safety. Once this information is known, you can use your risk methodology to evaluate control effectiveness, likelihood and consequence to identify vulnerabilities and develop improvement action plans.

Self-Assessment of Data Security Weaknesses



Control Posture Tips

The following are focus areas an organisation should assess:

- IT digital governance and culture, including policies, Disaster Recovery Plan, system protection (password access, antivirus/malware software, firewalls, patching), use of encryption, education, deleting of fake emails, etc
- Third party agreements, such as cloud computing. It is critical these agreements protect your data and are clear as to how the third party notifies you in the instance of a data breach. Seek annual security audit certifications, such as ISAE 3402 or ISO 27001 to reconfirm the third parties security protocols
- External storage devices such as USB sticks. Also, hygiene over retiring equipment and phones, as well as printer/scanners, as data may be saved on them
- Establishing a breach response plan, clarifying roles and responsibilities. This could be included as a scenario in the business continuity plan
- Evaluating the benefits of obtaining cyber insurance, as the cost of recovery could be significant
- If you do business in Europe, or hold personal data of EU residents, be aware that new General Data Protection Regulations (GDPR) come into effect from May 2018. Whilst many of the GDPR provisions are similar to the Australian Privacy Act, they do require more compliance activities.

Do you have processes in place to recover from an attack?

Cyber and data security can have a significant, immediate and long term impact on your organisations reputation. Should you like to know more about data privacy governance or need assistance with undertaking a data inventory risk assessment to identify possible security vulnerabilities, please contact Jeff Webb on 0437-539-015.

STRATEGIC CONSULTING
Business Process Risk Professionals

Valued Risk Insights through:
- Experience
- Professionalism
- Industry Expertise
- Personal Delivery

Contact Us: Jeff Webb
Managing Director
m. +61 0437 539 015
e. jeffwebb@jnwstrategic.com.au
w. jnwstrategic.com.au

For information on our clients and services visit our website: www.jnwstrategic.com.au

Disclaimer | This publication contains general information only. By no means is this publication rendering professional advice or services. JNW Strategic Consulting Pty Ltd (JNW) will not be responsible for any loss whatsoever sustained by any person who relies on this publication. Copyright © 2018 JNW. All rights reserved. Liability limited by a scheme approved under Professional Standards Legislation. For more information, contact JNW.