YOUR RESULTS

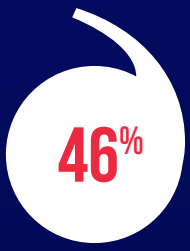
LOW RISK

YOUR RESULTS SUGGEST YOU CURRENTLY HAVE ADEQUATE CONTROL OF YOUR CYBERSECURITY RISKS.

It looks like you're taking the lead when it comes to recognising cybersecurity as a serious business risk, not defaulting to an IT problem. Each business is different, and with the ever changing cybersecurity landscape, including the development of millions of new forms of malware and threat vectors being developed annually, regular health checks are recommended to maintain an effective level of protection.

DID YOU KNOW

Increase in new downloader variants



Increase in new malware variants

Symantec's most recent Internet Security Threat Report (ISTR) uncovered that there was a 92% increase in new downloader variants and 46% increase in new malware variants between 2016 and 2017. This means that cybercriminals are committed to constantly developing new ways to infiltrate organisations. Increased regulation and loss of data responsibilities for businesses on a local and global level also require high levels of vigilance in protecting private and sensitive information.

Following the introduction of the Australian Notifiable Data Breaches (NDB) Scheme, it's important for businesses to be aware of their obligations and responsibilities. The Office of the Australian Information Commissioner quarterly NDB report revealed that 242 data breach reports were received between April and June 2018. 59% of these breaches were due to malicious or criminal attack including phishing or malware and the vast majority (89%) involved the retrieval of contact information such as an individual's home address, phone number or email address.

It is up to each individual organisation to assess suspected data breaches and if it is likely to result in serious harm to those affected. Once aware of an eligible breach, they are obligated to notify individuals as promptly as possible.

HUMAN ERROR ACCOUNTED FOR 36% OF DATA BREACHES

Interestingly, human error accounted for 36% of data breaches, which demonstrates that many cyber criminals exploited vulnerabilities involving a human factor (such as clicking on a phishing email or disclosing passwords). So it's important that education about cybersecurity is carried through all layers of an organisation.

As your organisation and infrastructure changes, it's important to assess exposure to new threats and risks that naturally arise with growth. It's all about giving you the best chance to protect the value of what's being created in your business - your relationships, your reputation and your expertise. Compromised cybersecurity can change things very quickly, and we can help ensure that your business is covered holistically and not just from an IT perspective, but an end-to-end strategy that's designed to mitigate potential risks.

ARE YOU TAKING STEPS TO PROTECT THE FUTURE OF YOUR BUSINESS?

If you see the value in assessing cybersecurity with a business-centric approach, get in touch with CSO Group to find out exactly what walking the walk means for your organisation.

info@csogroup.com.au