Article

Aug 2024

An Australian Businesses Guide for: Navigating the Cybersecurity Landscape

If you're an Australian business, you've likely noticed the recent surge in cyber-attacks nationwide. These incidents, growing in scale and sophistication due in part to the increased accessibility of AI for malicious purposes, have impacted companies of all sizes. The consequences range from widespread disruption and halted operations to the theft of consumer information, which if then leaked on the dark web, can lead to severe legal consequences.

Craig Archdeacon
Director - APAC

Email craig.archdeacon@waterstons.com

If you're an Australian business, you've likely noticed the recent surge in cyber-attacks nationwide. These incidents, growing in scale and sophistication due in part to the increased accessibility of AI for malicious purposes, have impacted companies of all sizes. The consequences range from widespread disruption and halted operations to the theft of consumer information, which if then leaked on the dark web, can lead to severe legal consequences.

However, change is on the horizon. Our national government is taking action. The newly launched 2030 Australian Cyber Security Strategy delineates Australia's determination to counteract criminal syndicates. As the standard now indicates, it's not a question of "if" you'll be attacked, but "when." It's no longer permissible for Australian businesses to operate status quo without complying with the forthcoming cyber legislation.

Should your business fail to take action, it's improbable that you'll be considered for tenders, contract bids, or even retain your existing clientele or supply chain—unless they, too, demonstrate adherence to the minimum baseline measures against the escalating threat environment.

So, what changes are forthcoming? There's a plethora of standards circulating, such as the Australian SOCI Act, the Essential 8, the Australian ISM, and other internationally recognized standards and frameworks like ISO27001 and NIST. It can seem like a labyrinth that requires careful navigation to determine which is suitable for your business, which is obligatory, or which might simply be impractical.

That's where we come in. Waterstons Pty is here to assist. In the upcoming months, we will unveil a series of articles, webinars, and materials designed to demystify the subject and guide you in identifying pragmatic next steps for your organization.

This month, our focus is on the Essential 8: The mitigation strategies comprising the Essential Eight include patching applications, updating operating systems, implementing multi-factor authentication, restricting administrative privileges, controlling applications, limiting Microsoft Office macros, hardening user applications, and conducting regular backups.

Waterstons is here for you, and we're eager to hear your preferences. Should you face challenges you'd like us to address, or if there's specific content you wish to see, please reach out to us. Let's navigate this complex cybersecurity landscape together.

craig.archdeacon@waterstons.com + 02 9160 8430