Screening expert warns firms to be prepared ahead of August legislation change in Australia

Submitted by: BlueSky Public Relations Ltd
Wednesday, 15 May 2024

Firms supplying critical infrastructure solutions across Australia need to begin preparations as the compliance date for the amended Security of Critical Infrastructure Act (SOCI) nears. That's according to employment screening and identity expert, Sterling.

The Act – which was initially rolled out in 2018 – has been expanded to place requirements on responsible entities across 11 critical sectors, with August 2024 marking the end of all legislative grace periods and the time at which businesses need to be prepared. While compliance with the legislation is only required for those firms that supply into the critical infrastructure of Australia, Sterling has urged all companies that provide services in the country to check if they are liable under the reforms.

The core purpose of SOCI is to enhance the country's resilience and mitigate against national risks. Responsible Entities and Direct Interest Holders that own and operate critical infrastructure assets in any of the 11 sectors need to be able to demonstrate they have plans in line with three core Positive Security Obligations (PSOs):

• An Information Provision PSO: Requires firms to register critical assets with the federal government now and as new assets are added to the company's infrastructure.
• A Mandatory Cyber Incident Breach Notification PSO: Outlines that a business will immediately notify the Australian Cybersecurity Centre (ACSC) via phone or the ACSC website of any cyber incident, before providing written notification.
• A Risk Management PSO: Defines a clear plan around how the company will identify risks and deal with hazards that fall under four key categories:
• Supply Chain Hazards
• Cyber & Information Hazards
• Physical Hazards
• Personnel Hazards

As Mick Roche, ANZ Head of Sales Sterling explained, this is a positive, but complex initiative from the Australian government, with the personnel hazards presenting a core challenge:

"There's no doubt that this move will be beneficial to Australia, its citizens, and businesses. A failure in services or a cyber-attack on any sector or firm that falls under the critical infrastructure category could have a domino impact on others, so mitigating risks and planning for hazards is crucial.

"Of all the areas that employers need to create plans for, though, it is the personnel hazards that arguably present the greatest challenges and the biggest threats. Employees are the ones controlling critical infrastructure assets and have access to multiple facets within companies which could expose infrastructure and systems to risks. It's vital that employers put the necessary screening and re-screening programs in place now to meet the SOCI Act legislation requirements ahead of the 11 August deadline.

“While it may seem like an overwhelming and difficult challenge to navigate, there are a wealth of resources available to support businesses as they prepare for the August deadline. From a personnel screening point of view, I would urge employers to be mindful of the fact that the cost of implementing the required checks are minimal in comparison to the potentially catastrophic impact of inaction.”

Ends

Press contact
Vickie Collinge
vickie@bluesky-pr.com
+441582 790 705