Press release
September 2021

Australia’s tech leaders’ confidence in cyber-security suggests blind spot in face of growing risk

- 65% of Australian tech leaders rated their company’s IT security an 8 out of 10 or higher. 10% rate themselves 5 out of 10 or lower.
- 37% don’t think their organisation currently has the necessary skillsets to mitigate security threats.
- Network security (27%) and security architecture (27%) are the most common missing skills across Australian organisations.

Sydney, 17 September 2021 – The latest Annual Cyber Threat Report by the Australian Cyber Security Centre shows cyber-security incidents rose by 13% compared to 2020, with an attack occurring every eight minutes. As the report demonstrates, some businesses are struggling to evolve their protective measures and strategies at the same pace as the cyber-attacks, as evidenced by the increasing cost, severity and frequency of cyber-security attacks year-on-year.

New independent research by specialised recruiter, Robert Half, however, finds that companies are overwhelmingly confident in their ability to prevent and respond to attacks. On a scale of 0-10 where 10 equals ‘perfect’, 65% of leaders rated their company’s IT security an 8 or higher. Just 10% rate themselves below a 5.

While the majority of companies rate their IT security as very strong, the ACTR report demonstrates that companies are not only vulnerable, but that the rate and intensity of attacks are increasing. This raises the question: what threats are Australian tech leaders underestimating, and do they have the skills to address it?

Where cyber-security skills are companies missing?

Cyber-threats evolve in tandem with an organisation’s dependence on technology. As businesses move to decentralised operations to allow for remote work, more vulnerabilities are exposed which requires an always-on approach to cyber-risk management.

In spite of this, 63% of surveyed Australian tech leaders believe their organisation has all of the necessary skillsets to successfully mitigate known and unknown security threats and risks currently in-house. Over a third (36%) of CIOs responded that they have some of the skillsets necessary while just 1% of leaders don’t think their organisation currently has the necessary skillsets to mitigate security threats.

Of the 37% who believe they do not have all the necessary skillsets, network security (27%) and security architecture (27%) are identified as the most common missing skills followed by cloud security and data privacy (24% respectively).

Andrew Brushfield, Director at Robert Half says: “*While Australian leaders are confident in their companies’ existing capabilities, to stay protected, businesses must evolve their cyber-security talent pipeline and expertise in line with evolving cyber-security threats. The rapid uptake of remote technologies has also exposed growing gaps in cyber-security, data exposure and user error. These range from enterprise-level threats like the exploitation of cloud infrastructure vulnerabilities to access corporate networks right down to targeting an individual working remotely on a personal device that is not protected by corporate control measures.*”

"Cyber-threats are as pervasive as they are insidious so companies must adopt a pre-emptive and pro-active approach to ongoing risk management and ensure they have access to the required talent capable of reducing risk to their digital assets and infrastructure. As it stands, however, demand for the niche skillsets required for an effective security strategy is significantly outpacing supply, so companies need to prioritise internal training and upskilling to sustain their talent pipeline into 2022," concludes **Andrew Brushfield**.

Robert Half has outlined the 5 cyber-security skills Australian organisations that are in high demand:

- **Information security (InfoSec):** Organisations will need InfoSec skills to protect their electronic data from unauthorised access. In-demand skills include authentication/authorisation (including single digital identity security across devices), malware analysis, incident response, risk management and data recovery.

- **Network security**: Organisations face increasing breaches and threats in their IT networks, including malware and hacker attacks. Skills required include wireless network security, firewalls and IDS/IPSes, VPNs and remote access, as well as endpoint security.

- **Cloud security services**: There will be growing demand for security skills applicable to public and hybrid cloud platforms such as Amazon Web Services (AWS) and Azure, as more organisations use them to support both at-office and home-based working environments. This includes implementation of policies, controls, procedures, and technologies that protect cloud-based systems, devices, and infrastructure.

- **Web security**: With the growth in employees accessing office applications from their home internet and mobile devices, enterprises will need to secure their websites and web applications from threats including viruses, ransomware, and distributed denial of service (DDoS). Relevant skillsets span network, application, and OS security.

- **Security architecture**: With many employees likely to continue working from home at least part-time for the foreseeable future, more organisations will be looking to build IT security into all aspects of their operations, including organisational structure, company policies, processes, and customer products. Relevant top-level skills in this area include knowledge of security hardware and software, analysis of organisational needs, and the ability to manage cyber-security risks in relation to organisational policies and industry standards.

##

Notes to editors

About the research

The annual study is developed by Robert Half and was conducted online in May 2021 by an independent research company, surveying 300 hiring managers, including 100 CFOs and 100 CIOs, from companies across Australia. This survey is part of the international workplace survey, a questionnaire about job trends, talent management, and trends in the workplace.

About Robert Half

Robert Half is the global, specialised talent solutions provider that helps employers find their next great hire and jobseekers uncover their next opportunity. Robert Half offers both contract and permanent placement services, and is the parent company of Protiviti, a global consulting firm. Robert Half Australia has offices in Brisbane, Melbourne, Mount Waverley, Perth and Sydney. More information on More information on roberthalf.com.au.

Follow Robert Half Australia

Read related articles on our Robert Half's work*life* blog

For more information
Katherine Mills
Public Relations Manager Robert Half Asia Pacific
katherine.mills@roberthalf.com.au
(02) 8028-7757