Press release
6 September 2016

Cyber-security threats increase as Australian CIOs face talent shortage

- 75% of Australian CIOs anticipate more cyber-security threats in the next five years due to a shortage of skilled IT security professionals.
- 64% say the number of detected security threats has increased compared with 12 months ago.
- The top three cyber-security risks facing organisations in the next five years are spying/spyware/ransomware (49%), data abuse/data integrity (49%), and cyber-crime (46%).

Sydney, 6 September 2016 – Australian companies are facing increasing security threats from cyber-criminals, a threat exacerbated by a growing skills gap within the IT industry. This growing threat is made evidently clear by recent cyber attacks, such as the hacking of the Census website. According to a recently published report, Cyber-security – Defending your future, commissioned by specialist recruiter Robert Half, cyber-attacks are becoming more sophisticated and targeted. Because cyber-attacks impact the entire business and leave a trail of financial, operational and reputational damages, companies need a robust and proactive approach to cyber-security to prevent, detect and mitigate these IT risks.

Cyber-attacks on Australian enterprises are growing, with 64% of Australian CIOs stating the number of detected security threats has increased compared with 12 months ago. According to today's IT leaders, the top three cyber-security risks facing organisations in the next five years are spying/ransomware (49%), data abuse/data integrity (49%), and cyber-crime (46%).

David Jones, Senior Managing Director Robert Half Asia Pacific said: *"The days when IT security was perceived as simply an IT problem are over. In order to successfully confront a proliferating breed of cyber-attackers, companies need a resilient cyber-security strategy that brings together the right mix of technology and people."*

As a response to a new wave of cyber-attackers, one in five (22%) Australian CIOs say they will be adding new permanent IT security professionals to their team in the next 12 months. And over one in 10 (16%) state they are planning to hire IT professionals for newly added contract positions within their team.

"The most sought after candidates are familiar with new security software and hardware, have an understanding of emerging protection systems and are able to confidently use devices and related applications," **David Jones** added.

Cyber-security experts with specialist skills are in high demand but challenging to find. This increased cyber-threat landscape is set to intensify, as 75% of CIOs expect the number of cyber-attacks to increase in the next five years due to a shortage of skilled IT security professionals.

"New technologies raise new security concerns. This trend has resulted in an IT security skills gap since the available expertise has not kept pace with the evolving IT threats," **David Jones** said.

"As demand for new cyber-specialists entering the IT market outstrips supply, companies are being forced to reconsider their training and retention programs. They are also recruiting from overseas, partnering with educational organisations, and developing flexible hiring strategies that include both permanent and contract specialists, including external risk agencies."

Popular and challening to find cyber-security skills

As organisations are confronted with additional security threats, including mobile, application and Big Data analytics security, several areas within cyber-security are experiencing higher demand for specialised skills. Whilst CIOs identify cloud security (54%), hacking and penetration testing (38%), and Big Data and data

analytics (32%) as the top three technical skills in demand, these competencies turn out to be amongst the most challenging security skills to find, thereby highlighting the IT security skills gap.

David Jones said: *"Having a robust talent management program is essential to efficiently manage the IT security skills shortage. If companies want to stay abreast of industry developments and successfully tackle IT security issues, they need to assess what areas of expertise are missing in-house and either invest in training programs for existing IT professionals or hire additional IT security experts."*

Source: Independent survey commissioned by Robert Half among 160 Australian CIOs – multiple answers allowed.

While technical skills are still must-have competencies for a specific position, the so-called soft skills have also become substantially more important. Analytical skills and providing insights, as well as strong business acumen and communication skills, have developed into highly sought-after skills for an IT security role.

"There is no doubt that highly specialised technical skills are vital, but the ability to clearly articulate cyber-security issues in a language that senior management and non-IT employees understand not only increases security awareness, it also enhances the reputation of the IT department as business partners who add value across the business," **David Jones** concluded.

##

Notes to editors

About the research
The annual study was developed by Robert Half Australia and is conducted by an independent research company. The study is based on 160 interviews with senior IT and technology executives from companies across Australia, with the results segmented by company size, sector and geographic location.

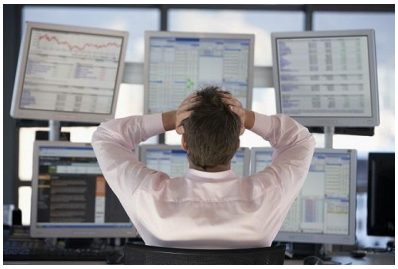
About Robert Half
Robert Half is the world's first and largest specialised recruitment consultancy and member of the S&P 500. Founded in 1948, the company has over 325 offices worldwide providing temporary, interim and permanent recruitment solutions for accounting and finance, financial services, technology, and administrative professionals. Robert Half Australia has offices in Brisbane, Melbourne, Mount Waverley, Perth and Sydney. More information on roberthalf.com.au.

Follow Robert Half Australia

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

According to IT security trends, employee security raises concern

Every organisation faces a constant battle to protect its IT infrastructure from external threats, but IT security teams are just as worried about the internal threats: employees doing the wrong thing, intentionally or otherwise.



Plugging a leak: Protecting company data from employee mistakes

While Australian businesses are becoming increasingly savvy in preventing external cyberattacks on their data, such measures have not translated to preventing data breaches by internal employee mistakes. It's a problem that has affected large corporations, world leaders and, embarrassingly, even web giant Wikipedia.

For more information

Gabrielle Nagy
Public Relations Manager, Robert Half Asia Pacific
gabrielle.nagy@roberthalf.com.au
02 8028 7751

Courtney Howe
Citadel Magnus
chowe@citadelmagnus.com
02 8234 0111