Press release
9 November 2016

Employees a potential risk to their own workplace
How Australian companies can counter the IT risks caused by BYOD

- 77% of Australian CIOs allow their employees to access corporate data on their personal devices.
- 34% state a lack of employee knowledge/skills around security is the most significant security risk for their organisation in the next five years.
- 91% say it is challenging for their company to find skilled technology professionals, with one in four (23%) saying IT professionals skilled in mobile security are the most challenging to find.

Sydney, 9 November 2016 – The increasing use of Bring Your Own Device (BYOD) practices, where employees can bring their own laptops, tablets and smartphones to work, has presented the added internal cyber-security risk of data theft to Australian workplaces. According to a recently published report, Cyber-security – Defending your future, commissioned by specialist recruiter Robert Half, over one in three (34%) Australian Chief Information Officers (CIOs) say a lack of employee knowledge and skills around data security is the most significant security risk their organisation will face in the next five years.

The risks associated with the use of personal devices and unregulated apps was made clear after it was revealed Prime Minister Malcom Turnbull frequently uses WhatsApp to communicate with his staff, raising concerns about the transmission of classified government messages[1]. While traditionally, the response to IT security has been to find the optimum way to protect a business' assets from *external* security attacks, a growing risk now faces organisations in the form of potential *internal* security threats. According to risk and business consulting firm Protiviti, the risk of data loss is significantly increased with BYOD because basic security controls may no longer be effective on mobile devices, or consistently implemented across the wide range of device types used by employees[2].

Despite the fact that over three in four (77%) CIOs allow their employees to access corporate data on their personal devices, one in four (25%) think their non-IT senior management do not possess enough understanding about information security exposures, indicating a lack of awareness across the business about IT security risks.

David Jones, Senior Managing Director Robert Half Asia Pacific said: *"Whilst BYOD can bring significant advantages for any organisation, such as higher levels of employee satisfaction, increased productivity, and cost savings, the use of BYOD also poses some serious cyber-security challenges in terms of securing corporate networks and data, mobile device management, and developing security policies."*

"Although it may not be intentional, simple human error can expose companies to increased cyber-attacks and situations where sensitive company data can be compromised. In light of this, more companies are taking steps to balance both their employees' needs and their security concerns."

[1] See more http://www.abc.net.au/news/2015-03-03/malcolm-turnbull-uses-secret-messaging-app-instead-of-sms/6276712
[2] Protiviti – "Strategic Bring Your Own Device" report

What is your company doing to protect corporate data on employees' personal devices?

Provide training to employees on maintaining security when using personal devices	56%
Request employees to sign an acceptable use policy for keeping company information secure	55%
Deployment of mobile device management technology to enforce enhanced protection	49%
Implement authentication and authorisation to grant access to corporate network	48%
Don't allow employees access to corporate data on their private devices	23%
We are not doing anything to protect corporate data on employees' personal devices	3%

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

Australian CIOs are implementing security measures to protect company data on their employees' personal devices. More than half (56%) of CIOs are providing training of all personnel on cyber-security policies and corporate practices when using their personal devices. Signing an acceptable use policy also seems to be standard practice for more than half (55%) of the Australian companies. In addition, technical applications are being implemented as 49% say they are deploying mobile device management technology and 48% are using authentication software. Merely 3% say they are not taken any actions to protect corporate data on employees' personal devices.

With 34% of CIOs saying the lack of employee knowledge around data security is one of the most significant security risks CIOs think their organisation will face in the next five years, it is not entirely surprising that almost one in four (23%) do not allow their employees to access corporate data on their private devices.

Because more companies are investing in various platforms and tools designed to protect IT systems and networks, there's an increased demand for IT security specialists with the niche skills needed to help companies protect themselves against key data security risks, including risks related to BYOD. This increased demand may prove to be challenging, as 91% of Australian CIOs say it is difficult to source skilled technology professionals, with almost one in four (23%) finding professionals skilled in mobile security the most challenging .

"Cyber-security is a crucial issue for any organisation today, and as such they need to implement security standards for employees using BYOD. The solution demands a resilient IT security strategy that goes beyond assessing a business's IT infrastructure and having the necessary IT security skills. Proactively treating IT security as a continuous enterprise-wide process while making all staff aware of the risks associated with email, social media and confidential information are also essential if companies want to protect their company data," **David Jones** concluded.

##

Notes to editors

About the research

The annual study was developed by Robert Half Australia and is conducted in April 2016 by an independent research company. The study is based on 160 interviews with CIOs/CTOs 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

4 steps to cloud security that every business should know
Many startups are adopting cloud services such as Gmail, Dropbox and Skype to run their business. As well as keeping costs down, they're easy to use, versatile and encourage collaboration. Even big businesses are adopting them rather than developing their own apps. But what about the security risks for employees and businesses? Read here to learn how to mitigate these risk by taking the appropriate measure for cloud security.

Practical experience vs. qualifications in the tech and finance industry
Which is more important when it comes to getting a job in the IT and finance sector: qualifications or experience? According to recruiters, however, these qualifications form just one part of the industry picture. Are qualifications more important than work experience in the tech and finance industry? Or vice versa? We speak with industry insiders to get their opinions.

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