Press release
February 2018

Australian IT leaders take proactive approach to tackling internal IT risks

- 87% of Australian CIOs have experienced an internal IT security breach within their organisation in the past three years, with 96% already implementing measures to enhance internal IT security.
- The most common internal IT security breaches within Australian businesses are: social engineering (48%), information leakage (48%) and deliberate cyber-attacks (41%).
- Australian CIOs rate their employees' knowledge of potential IT security risks and the company's security policy an average of 7 out of 10.

Sydney, 26 February 2018 – Most businesses understand they're facing increasing external cyber-security threats, however many IT leaders are also battling the growing risk from security breaches present from within their own company. Independent research commissioned by specialised recruiter Robert Half confirms almost nine in 10 (87%) Australian CIOs have experienced an internal IT security breach in the past three years, thereby potentially facing a range of devastating financial, operational, and reputational consequences, with the average cost of a data breach to an Australian business being $2.51 million[1].

According to the research, which surveyed 160 Australian CIOs, the most common types of internal IT security breaches experienced by Australian companies in the past three years are social engineering (48%), information leakage (48%), deliberate cyber-attack (41%) and staff downloading malicious internet content (35%).

Andrew Brushfield, Director of Robert Half Australia said: "*While the response to IT security has traditionally been to find the optimum way to protect a business' assets from external security attacks, companies now face a growing risk in the form of potential internal security threats. Many internal IT security breaches take place inadvertently by company employees. Businesses must take a proactive, rather than reactive, approach when addressing their internal IT security infrastructure and policies. Maintaining the integrity of internal IT security systems will be essential for the long-term viability of companies as we change the way we work through digitisation.*"

While as many as 96% of IT leaders are already implementing a range of security measures to combat internal IT security threats, the research has found Australian CIOs rate their existing employees' knowledge of potential IT security risks and the company's security policy an average of 7 out of 10, highlighting there is room for improvement when it comes to raising employee awareness.

"All staff – from senior to junior – in the company need to be aware of the risks associated with email, social media and confidential information. Providing regular training – that go beyond the obligatory email – of all personnel on cyber-security policies and corporate practices will be essential if companies want to have an efficient cyber-security approach."

The measures CIOs **have already taken** to enhance internal IT security include conducting an internal IT security audit (41%), conducting security awareness training for employees (39%), implementing secure backup and recovery processes (36%), implementing remote access policies and procedures (35%), and hiring permanent and temporary IT staff to strengthen IT security processes (34%).

"While there is already a nation-wide understanding that companies need to act proactively when it comes to internal IT security, taking the steps necessary to protect themselves against internal IT

[1] https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130AUEN&

breaches is an ongoing process for businesses. Companies should take on a continuous enterprise-wide approach that combines both the technological means and the talent to manage it. This means onboarding skilled IT security professionals, such as IT security analysts, information security officers and IT security engineers, to address sophisticated cyber-security threats – both internal and external," added **Andrew Brushfield.**

Meanwhile, there's a common understanding in the sector that enhancing internal IT security is an ongoing process, as 96% plan to take additional measures. The top five internal IT security measures CIOs **are planning to take** are: implementing secure backup and recovery processes (39%), monitoring and logging employees' online actions (37%), conducting security awareness training for employees (35%), conducting an internal IT security audit (33%), and hiring permanent and temporary IT staff to strengthen IT security processes (30%).

In a further sign of the growing demand for IT security specialists, the **2017 Robert Half Salary Guide** has identified substantial year-on-year salary growth for both cyber-security specialists (+6.2%) and IT security specialists (+4.8%), indicating IT security roles are in high demand with companies willing to increase salaries to secure top talent.

"Not only are companies battling their own internal IT security threats, they also have to contend with a very limited pool of IT security candidates in Australia, highlighting that IT security professionals with the most sought-after skills are in a very favourable position to negotiate above-market salary increases," concluded **Andrew Brushfield.**

##

Notes to editors

About the research
The annual study was developed by Robert Half Australia and was conducted in June-July 2017 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 more than 300 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 ways to check whether your company is prepared for cyber-attacks

As new technologies spread, businesses across multiple sectors are coming to terms with a growing and rapidly evolving landscape of cyber-threats. With much of this risk associated with 'third platform' enterprise technologies, many businesses are having to adopt new strategies in their fight against cyber threats. Read here for more on how to protect your company against cyber-attacks.

Should my business have a Bring Your Own Device (BYOD) policy?

Ask yourself how many of your employees already own a smartphone. Now ask yourself whether you're willing to leverage that access with a Bring Your Own Device (BYOD) policy in your workplace. If you answered yes, you're with the majority. Read here for more.

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