#GenMobile workforce compromising Australian business data security

Global study by Aruba Networks confirms the need to identify and support high-risk, security-lax employees to protect sensitive data Forty-three percent (43%) of Australian employees admit to having lost data due to the misuse of a mobile device High earning Australian males almost twice as likely as females to experience data loss

SYDNEY, Australia – 15 April 2015, – Aruba Networks, Inc. (NASDAQ: ARUN) is calling for businesses worldwide to take action as a new mobile security risk report reveals businesses are ill prepared for the high-risk, high-growth mindset of the #GenMobile workforce, creating alarming disparity around security practices in the corporate world. The chasm that is exposed between age, gender, income level, industry and geographic location has a direct effect on the security of corporate data.

The 'Running the Risk' security threat study, which surveyed more than 11,500 workers across 23 countries worldwide, including Australia, showcases that employee attitudes are swaying towards more sharing of devices yet an indifferent view to security in the workplace. The study shows that highly regulated and tech savvy industries, higher-earning males, and emerging markets pose the greatest risk to enterprise data security.

The report highlights three key trends for #GenMobile, who are paving the way for risk-prone behaviour in the workforce – which can be both good and bad for business.

Sharing becomes the norm: Six in ten share their work and personal devices with others regularly. Nearly a fifth of employees don't have passwords on devices, with 22% of those stating they don't have security measures in place so that they can share more easily and over half (54%) of the Australian respondents were not worried about the threat. Indifferent attitudes toward security arise: Nearly a third (31%) of workers admit to having lost data due to the misuse of a mobile device. Security ranks fifth behind brand and operating system when #GenMobile is making buying decisions for new devices. Alarmingly in Australia, almost nine in ten (88%) assume their IT departments will keep them protected; however, nearly half (43%) have lost data due to the misuse of a mobile device. Self-empowerment succeeds: Over half (56%) of Australian workers today said they are willing to disobey their boss to get something done, another 40% say that mobile technologies enable them to be more productive and engaged, and over three quarters (77%) are willing to perform self-service IT.

"The findings highlighted that while #GenMobile workers are willing to proactively drive productivity and business growth, these employees are also far more relaxed with sharing company data. Most notably, #GenMobile workers are oblivious to security threats or risks," said Steve Coad, Managing Director of Aruba Networks in Australia and New Zealand.

However, as this high-risk culture enters the enterprise, the report finds an alarming level of disparity among industries, individuals and countries when it comes to the treatment of mobile devices and data:

The Discrepancy Between Industries Finance is leaking data: Believe it or not, 39% of global respondents from financial institutions admit to losing company data through the misuse of a mobile device, which is 25% higher than the average across all industries surveyed. Conversely, Australian financial institutions appear to be leading the way with more stringent security measures in place, with only 11% admitted to losing company data through the misuse of a mobile device. High tech is at high risk: High tech employees are nearly two times (46%) more likely than hospitality or education workers to simply give up their device password if asked for it by IT. Worryingly, 93% of high tech workers in Australia have already or would consider sharing their password.

Spotting the Risky Individual

Males more prone to data theft: Men are 20% more likely to have lost personal or client data due to the misuse of a smartphone, and 40% more likely than females to fall victim to identity theft. Younger employees wreak havoc on company security: Respondents over the age of 55 are half as likely to experience identity theft or loss of personal/client data compared to younger employees. The age bracket with the highest propensity of data and identity theft are employees between 25-34 years old.

Mapping Global Risk Trends

High-risk, high growth: The emerging and growth markets of China, Thailand and the United Arab Emirates (UAE), are found to exhibit the highest risk behaviours worldwide suggesting that greater risk-taking is linked to increased growth and opportunity as much as it relates to security risk. West is playing it safe: To support this connection, the least risk-prone countries are the westernised markets, including the USA, UK and Sweden.

Businesses lacking adaptability

The study suggests that businesses may not be prepared for what lies ahead with over a third (37%) not having any type of basic mobile security policy in place.

Aruba contends that if businesses strategically measure and intelligently manage their security, the more flexible, open methods of working and information exchange that #GenMobile workers bring can drive new business innovation.

“The arrival of the always-on, mobile-office and #GenMobile employee is as tangible and impactful on industry as the arrival of the Internet itself. #GenMobile workers demonstrate a much higher willingness to exhibit behaviour that is prone to risk,” says Coad.

“As such, Australian and New Zealand organisations and their IT departments need to be smarter about managing this behaviour of sharing without sacrificing the security of corporate data and information. In a connected world, businesses need to nurture creativity, while simultaneously planning for the security risks these behaviours bring with them.”

Run Your Risk

Using this global data, Aruba has developed an online Security Risk Index tool to allow organisations to benchmark their Mobile Security risk levels relative to organisations in their country and industry.

About Aruba Networks, Inc.

Aruba Networks is a leading provider of next-generation network access solutions for the mobile enterprise. The company designs and delivers Mobility-Defined Networks that empower IT departments and #GenMobile, a new generation of tech-savvy users who rely on their mobile devices for every aspect of work and personal communication. To create a mobility experience that #GenMobile and IT can rely upon, Aruba Mobility-Defined Networks™ automate infrastructure-wide performance optimisation and trigger security actions that used to require manual IT intervention. The results are dramatically improved productivity and lower operational costs.

Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, Africa and Asia Pacific regions. To learn more, visit Aruba at http://www.arubanetworks.com. For real-time news updates follow Aruba on Twitter and Facebook, and for the latest technical discussions on mobility and Aruba products visit Airheads Social at http://community.arubanetworks.com.

For more information, please contact:
Ashleigh, Jennifer or Sarah at DEC PR
+61 2 8014 5033 and aruba@decpr.com.au

Contacts

Sarah Bullen
02 8014 5033
mailto: s.bullen@decpr.com.au