Unisys Security Index™ Report
Australia – Mobile App Data Security

Australians hold organisations and government responsible for securing data collected by mobile apps

Australians on Mobile App Data Security

As part of the Unisys Security Index™, we regularly survey Australians on a range of security issues. This time we asked the Australian public to tell us who they thought should be responsible for protecting personal or financial data collected and stored in mobile applications. Results showed that 8 out of 10 Australians think the provider of the service a mobile app links to, such as a bank or airline, is responsible for protecting personal or financial data collected. Government ranked second most responsible, despite previous[1] Unisys research indicating the majority of Australians opposed greater government surveillance of the Internet.

% of Australians say should be responsible for security of data gathered by mobile apps:	
Provider of the service that the app links to such as the bank or airline	80%
Government	75%
Internet and telecommunications providers	67%
Individuals	66%
Social media companies	60%
Mobile app market place such as Apple App Store or Google Play	59%
Developer of the app	54%

Many apps are clearly designed to gather information about the people who download them. The Unisys Security Index findings send a clear signal to organisations that the public expects them to protect any personal data they collect via mobile apps. In the business environment, where there is a high rate of bring-your-own apps used in the workplace, it is concerning that only 66 percent of Australians said they are responsible as individuals for securing data collected by mobile apps. Some mobile apps may contain hidden malicious code designed to secretly gather and transmit data. Employees could inadvertently put their employers at risk by allowing mobile apps to capture sensitive information such as unencrypted data, location tracking, contacts and sign-on details. Therefore, individuals must also take personal responsibility to be aware of what information their mobile apps are accessing, particularly if the mobile device the app sits on is being used in the workplace and take steps to minimise the chance of mobile apps accessing data without permission.

[1] Unisys Security Index April 2010 *Additional Research: Increased Surveillance* – found only 40% of Australians were in favour of the government increasing surveillance of personal Internet usage while 54% were opposed – see here.

Unisys Security Index – Australia

In May 2013 the Australia Unisys Security Index stands at 129/300, up 19 points from the previous survey in May 2012.

Index results for each area of concern are:

- National Security Index – 128
- Financial Security Index – 139
- Internet Security Index – 123
- Personal Security Index – 124

About Unisys Security Index

Unisys Security Index is a global study conducted to gauge the attitudes of consumers on a wide-range of security-related issues.

Launched globally in October 2007 and conducted bi-annually, it provides a statistically robust measure of concern around four areas of security – National, Financial, Internet and Personal.

Conducted in Australia by market research firm Newspoll the Unisys Security Index provides a regular, statistically robust measure gauging levels of concern about various aspects of security.

The survey, on which the latest results are based, was conducted nationally 12 – 14 April 2013 by Newspoll using a nationally representative sample of 1,200 respondents aged 18 years and over. All results have been post-weighted to Australian Bureau of Statistics data.

Globally the study consists of native-language surveys across twelve countries – Australia, Belgium, Brazil, Colombia, Germany, Malaysia, Mexico, the Netherlands, New Zealand, Spain, the United Kingdom and the United States – and provides an overall rating out of 300.

For more information, please visit: www.unisyssecurityindex.com.au

Respondents were asked:
Many organisations - such as banks, government departments, insurance companies, airlines, etc - offer mobile apps for you to interact with them. Which of these do you think should be responsible for protecting personal or financial data collected and stored in mobile apps?

- Provider of the service that the app links into
- Government
- Internet and telecommunications providers
- Individuals
- Social media companies
- Mobile app market place such as Apple iTunes or Google Play
- Developer of the app

Contact Information

Media Requests
Julian Brophy, Perception Partners
ph: 02 9699 2722 or 0408 276 749
email: julian@perceptionpartners.com.au

Claire Hosegood, Unisys
ph: 0411 253 663
email: claire.hosegood@au.unisys.com

Briefing Requests
Nick Lake, Unisys
ph: 0424 648 285
email: nick.lake@au.unisys.com