

# THE UNISYS SECURITY INDEX – 2013



Over 50 billion apps have been downloaded from the Apple App store<sup>1</sup>, and business and government services are increasingly using mobile apps to engage with their customers, citizens and employees.

Some apps are upfront about gathering user data, but others can gather and transmit personal details without users being aware of it.

**Unisys asked Australians, New Zealanders and Malaysians who they hold responsible mobile app data security.**

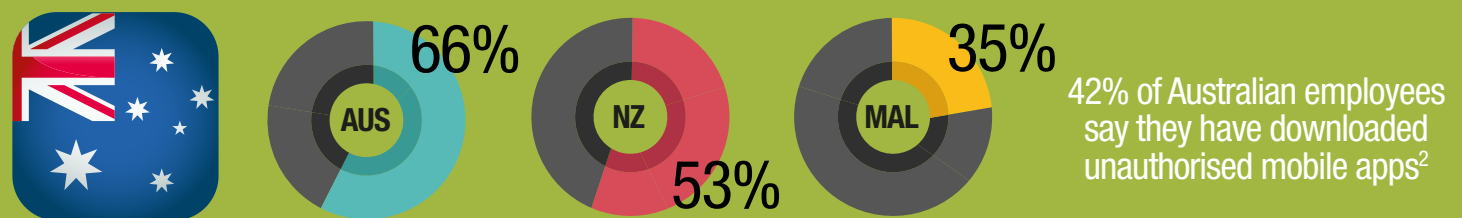
## AUSSIES & KIWIS HOLD THE ORGANISATION THAT PROVIDES THE APP (EG AIRLINE, BANK OR INSURER) & GOVERNMENT MOST RESPONSIBLE FOR SECURING ANY PERSONAL DATA COLLECTED



## MALAYSIANS SAY GOVERNMENT & TELCOS ARE MORE RESPONSIBLE FOR MOBILE APP SECURITY THAN ANY OTHER ORGANISATION



## AUSTRALIANS ARE MORE AWARE OF THEIR INDIVIDUAL RESPONSIBILITY FOR THE SECURITY OF THEIR PERSONAL OR BUSINESS DATA THAN NEW ZEALANDERS AND MALAYSIANS



## UNISYS TIPS TO ENSURE SECURITY OF PERSONAL INFORMATION WHEN USING APPS

1 Read the licensing agreement and privacy policy before downloading the app to make sure your info is not being shared with third parties

2 Avoid apps and games that require you to enter your birth date or place of birth

3 Conduct an Internet search and read user reviews on the app to see if there are any reports of it containing malicious code

4 If a free app looks too good to be true, it probably is – treat it with caution

5 If it's an app you want to use for work, check if your employer has a corporate app store that contains apps they have already reviewed and vetted as safe to use