

The protection of personal data against accidental loss, theft or deliberate hacking is a key security issue for Australians

Australians on Data Breaches

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 if they are personally concerned, or not, about a data breach by accidental loss, theft or deliberate hacking at a range of organisations.

We found that the majority of Australians are concerned that a range of commercial and government organisations are vulnerable to an accidental or malicious data breach, particularly financial institutions, telecommunication providers and government services.

Percentage of Australians concerned about a data breach by accidental loss, theft or deliberate hacking at the following types of organisations:	
Financial services such as credit card companies, banks	74%
Telecommunication providers and Internet Service Providers	67%
Government services such as social welfare, tax office or immigration	59%
Health organisations, hospitals and doctors	56%
Airlines and hotels including frequent flyer programs	51%

While the highest result was recorded for Banking and Financial institutions, the broad picture shows the majority of Australians are concerned about data breaches across many different sectors of government and business that consumers trust to hold and protect sensitive personal information such as financial, taxation and medical details.

All of the organisations surveyed recorded levels of concern by 50 percent of the population or greater, with millions of Australians expressing their worry about the protection of data from theft, hacking or accidental loss. This sends a message to governments and companies that the public perception of data security has been compromised by high profile breaches, undermining customer confidence, and that much work needs to be undertaken to regain that trust.

As the federal government finalises its mandatory data breach notification laws these results show that the public is very aware of the threat of data breaches and expects organisations to be accountable. However, for

compliance to be manageable, Unisys recommends that notification be triggered by those data breaches that have most real risk of harm and that the laws focus on the consequences of those impacted by the data breach.

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

Respondents were asked:

We hear a lot about data breaches in the media. For each of the following organisations that may store personal data about you please tell me if you are personally concerned or not concerned about a data breach by accidental loss, theft or deliberate hacking? Firstly...

(Options: Very concerned, Somewhat concerned, Not at all concerned, Don't know)

1. Banking & financial institutions (such as credit card companies, banks)
2. Health organisations, hospitals & doctors
3. Government (such as social welfare, tax office, immigration department)
4. Telecommunication providers & Internet Service Providers
5. Airlines & hotels including frequent flyer programs and online bookings web sites

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