UNISYS

Unisys Security Insights: Australia

A Consumer Viewpoint 2015




How Australian consumers feel about

- Personal data security, ranked by industry

Research by NEWSPOLL
WHEN THE ANSWER MATTERS

Table of Contents

Executive Summary

Unisys plays a prominent role in efforts to combat risk through the technology products and services it provides to the government and major industries in Australia.

The Unisys Security Insights is a snapshot of the nation's sense of security, and it provides a statistical measure of consumer concerns to enable organisations to make informed security decisions. The research is conducted in Australia by leading market research company NewsPoll.

This study builds on a body of 10 years body of research into the nation's sense of security.

A proactive outlook to security goes beyond bits and bytes, recognizing that the most effective solutions are going to be those formed through collaboration across interests.

See also www.unisys.com/usi-australia

For more information on Unisys security offerings, visit www.unisys.com/security

Unisys Outlook: Data Security Ranked by Industry

In 2015 the Australian Unisys Security Insights reveals Australians believe telecommunications companies and government agencies are more likely to experience a data breach of their customers' personal data in the next 12 months than other types of organisations.

The survey asked consumers in 12 countries about the likelihood that their personal data held by seven types of organisations (airlines, banking/finance, government, healthcare, retail, telecom, and utilities) would be accessed by an unauthorised person, either accidently or deliberately, within the next year. The findings reveal which organisations the public perceives to be most vulnerable.

Fifty-eight percent of Australians surveyed expect a personal information data breach in the next 12 months at a telco. Nearly half of Australians believe their personal information is likely to be breached by a government organisation in that same period of time. And more than one-third of Australian respondents felt a data breach is likely at a healthcare provider, airline and transport company, or bank.

Many Australians have personally experienced a data breach or have seen media reports of high profile breaches by government and telcos, which is likely to have contributed to their low level of trust in the ability of those organisations to protect their data. Conversely, public scrutiny around the introduction of e-health records and the resulting assurances for how data would be protected appears to have built community trust in healthcare providers' ability to protect personal information.

Airlines and other transport companies are currently the most trusted organisations included in the survey. However, they will need to work to maintain this trust as they continue to capture more and more information about their passengers in a bid to provide personalised end-to-end services – including assistance with border security measures.

Putting this in a business context, previous Unisys research[1] revealed that data breaches significantly impact a consumer's willingness to deal with an organisation: The majority of Australians surveyed in 2011 (85 percent) said that they would stop dealing with an organisation if their data was breached. Sixty-four percent said they would publicly expose the issue and nearly half said they would take legal action. This highlights that public confidence in an organisation's ability to protect data must be a business priority.

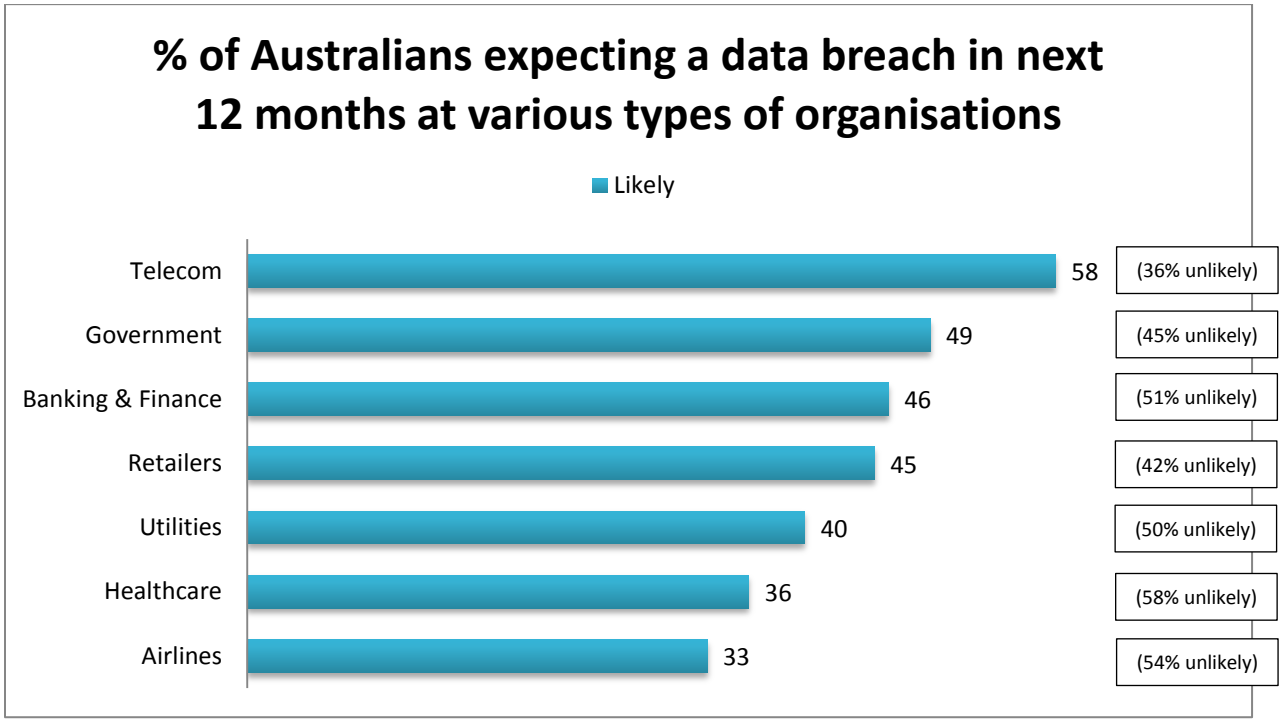
These findings remind Australian organisations of the importance of earning and maintaining consumer trust – or facing the consequences. To build trust, an organisation needs to not only take preventative measures, but also make those measures visible to build public confidence.

[1]Unisys Security Index research 2011 – The Australian public was asked what actions they would take if they found out their personal information being held by an organisation had been accessed by an unauthorised person

Results

Detailed Findings: For each of the following types of organisations that collect your personal information, how likely do you think it is that your personal information will be accessed by an unauthorised person, either accidently or deliberately, within the next 12 months?

Telecommunications providers are the least trusted by Australian consumers to protect their data compared to the other industries polled, with 58% of Australians believing a data breach at a telco is likely in the next 12 months



Almost half the Australian public expects a data breach by a government agency in the next year

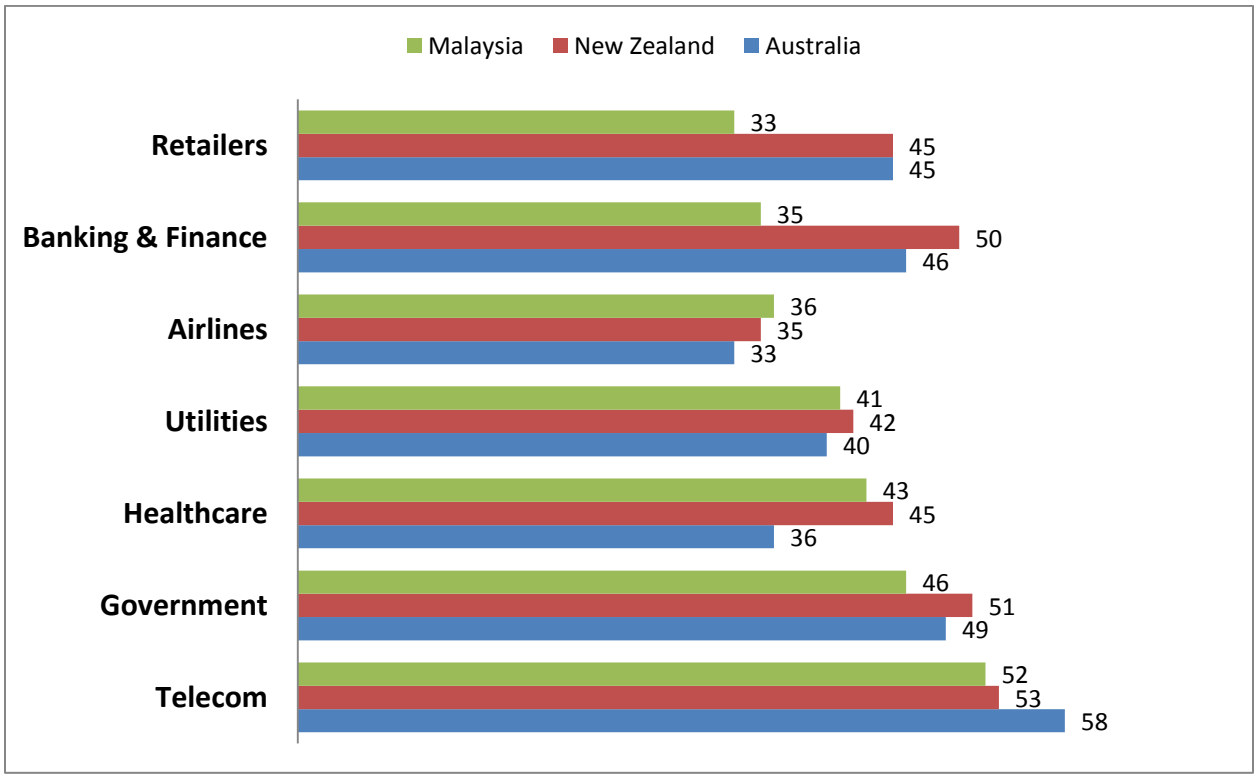
Airlines and healthcare are the most trusted industry sector with only 1 in 3 Aussies saying that a data breach is likely in these types of organisations

The Australian public perceives banks and retailers to be almost equally likely to suffer a data breach

Results

Regional Comparison: Asia Pacific

Consumer expectation of a data breach in the next year at various types of organisations in Australia, Malaysia and New Zealand



Telecom providers are the least trusted by Australians (58%), New Zealanders (53%), and Malaysians (52%) to protect personal data

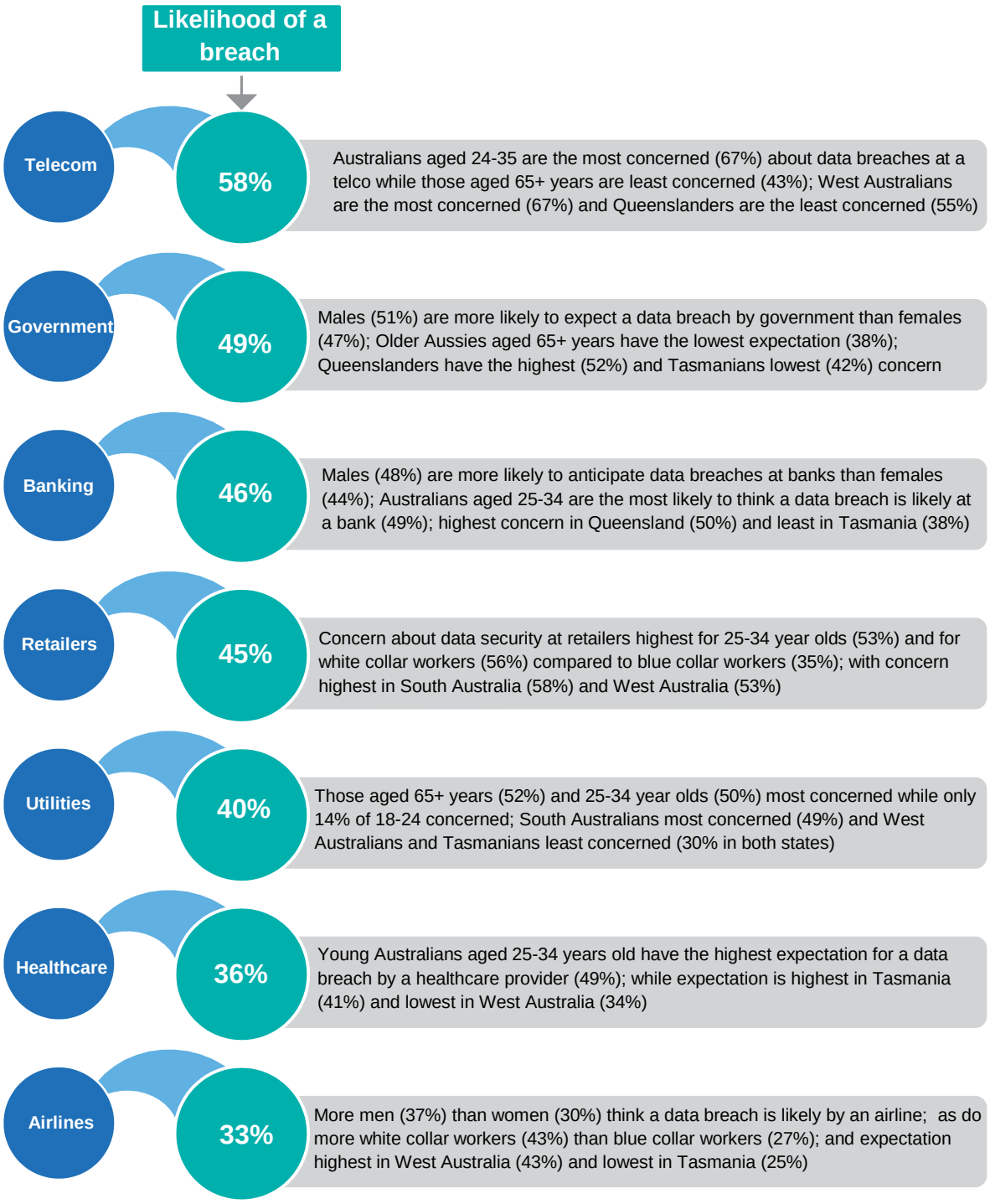
There is a high expectation of a data breach by **government** in the next 12 months in all 3 countries: Australia (49%), New Zealand (51%) and Malaysia (46%)

There is high trust in **airlines** to protect personal data in all 3 countries

Retailers and Banks are more trusted by Malaysians (ranked 5/6 most likely to have a data breach) to protect personal data than by Kiwis or Aussies (ranked 3/6 in both)

Results

Key Demographics by Industry: Australia



Results

Demographic detail: Australia

% of Australians expecting a data breach in next 12 months at various types of organisations
State vs State Comparison

	National	Male	Female	18-24	25-34	Total 18-34	35-49	50-64	65+	Total 50+
Telcos	**58%**	59%	57%	49%	67%	59%	63%	63%	43%	54%
Government	**49%**	51%	47%	43%	56%	51%	49%	57%	38%	48%
Banking & Finance	**46%**	48%	44%	45%	55%	51%	50%	49%	30%	40%
Retailers	**45%**	45%	45%	40%	53%	48%	49%	45%	35%	41%
Utilities	**40%**	39%	41%	14%	50%	35%	41%	52%	31%	43%
Healthcare	**36%**	37%	35%	36%	49%	43%	31%	37%	32%	34%
Airlines	**33%**	37%	30%	34%	37%	36%	32%	37%	27%	33%

% of Australians expecting a data breach in next 12 months at various types of organisations
Age-group Comparison

	National	NSW/ ACT	VIC	QLD	SA	WA	TAS
Telcos	**58%**	57%	56%	55%	62%	67%	56%
Government	**49%**	48%	47%	51%	51%	52%	42%
Banking & Finance	**46%**	456%	46%	50%	40%	44%	38%
Retailers	**45%**	42%	45%	43%	56%	53%	33%
Utilities	**40%**	40%	44%	38%	49%	30%	30%
Healthcare	**36%**	36%	35%	39%	37%	34%	41%
Airlines	**33%**	30%	34%	34%	34%	43%	25%

Unisys Perspectives on Security

The survey suggests that consumers are concerned about their personal data collected, used and held by organisations. With an ever increasing hyper-connectivity of consumers across various digital platforms, the traditional mechanisms to protect sensitive personal data against advanced attacks are proving to be insufficient. Unisys recommends that organisations maintaining personal or sensitive data look beyond traditional security mechanisms to protect against advanced attacks and accidental data disclosures. In particular:

- Converged physical and logical security approach – as logical and physical security measures are converging, leading enterprises across the world should seek ways to solve critical challenges at the point of convergence. Such measures help integrate sensors, consolidate data, provide central or dispersed command and control, use the identity information and support real time as well as offline analytics. Converged security provides seamless monitoring from the "door to the desk" and to the data.
- Biometrics for superior authentication – A robust security strategy incorporates multifactor authentication methods that provide assurance. The authentication can be provided via various biometric techniques like face recognition, DNA matching, fingerprints, voice recognition and vein structure in hands.

  Like organisations, mobile devices too allow for advanced authentication techniques to prevent intrusions and information theft. The opportunity for organisations is to grow in tandem with consumer preferences while ensuring highest levels of protection.
- Isolation and compartmentalisation for data protection – Protecting sensitive information from unauthorised access is the core objective for any security strategy. This typically involves two key activities of identifying the scope of data protection task, and isolating the people, processes and technologies that interact with the sensitive data. Data isolation is achieved by using access controls and encryption to ensure only authorised systems and users can access sensitive information. In addition, compartmentalisation of user groups also result in minimising the threat.
- Comprehensive Security Strategy – Maintaining superior security monitoring, awareness and reporting capabilities within a holistic cybersecurity framework helps protect data and networks from internal and external threats. An all-encompassing security strategy would encompass predictive, preventive, detective and retrospective capabilities.

For information on Unisys security offerings, visit: www.unisys.com/security

Polling methodology

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

The survey was conducted in April and May 2015 by Lieberman Research group in Latin America, Europe, Malaysia and the U.S.; and by Newspoll in Australia and New Zealand. Responses are from nearly 11,000 people in 12 countries: Australia, Brazil, Colombia, France, Germany, Malaysia, Mexico, the Netherlands, New Zealand, Spain, the United Kingdom and the United States.

The Australian survey, on which the latest results are based, was conducted nationally in April 2015 by market research firm Newspoll using a nationally representative sample of 1,210 respondents aged 18 years and over. All results have been post-weighted to Australian Bureau of Statistics data.

For more information, please visit: www.unisys.com/usi-australia

About Unisys

Unisys is a global information technology company that solves organisations' most pressing IT and business challenges. With more than 20,000 employees serving clients around the world, our offerings include cloud and infrastructure services, application services, business process outsourcing services, and high-end server technology.

We deliver solutions for 10 of top 15 global banks, 15 of top 25 global airlines and more than 200 airlines worldwide. 10 million user incidents are handled in 26 different languages every year and 130 million health and human services transactions are processed each year by Unisys systems. Our processes are end-to-end ITIL v3 compliant and Global ISO 20000, 27001 and 9001 certified. Unisys holds over 1,500 U.S. and non-U.S. patents.

Unisys security offerings are trusted by government and commercial clients around the world to deliver advanced security to counter advanced threats. As logical and physical security threats converge, the world's most important enterprises seek a partner that can bring new ways to solve critical challenges at the point where they converge. Our award-winning, time-tested portfolio of professional services, products, and managed services delivers mission-critical security at scale, helping clients mitigate risk while reducing complexity and cost, and navigating regulatory compliance requirements.

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
Alison Chu, Unisys
email: alison.chu@au.unisys.com