

Unisys Security Index

Australian public 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 – November 2011

As part of the Unisys Security Index™, we regularly survey Australians on a range of additional security issues. This time we asked them to indicate what action they would take if they found out their personal information being held by an organisation had been accessed by an unauthorised person.

The majority of Australians (85%) said that they would stop dealing with an organisation if their data was breached. Of the 12 countries surveyed in the global research study, Australians were the most likely to say they would take this action.

The survey also found that many Australians would consider a range of other responses to a data breach, with 47% saying they would take legal action and 64% saying they would publicly expose the issue.

The responses are not restricted only to online interaction. When asked if they would continue dealing with the same organisation but not use online services, only 24% of Australians said that they would continue.

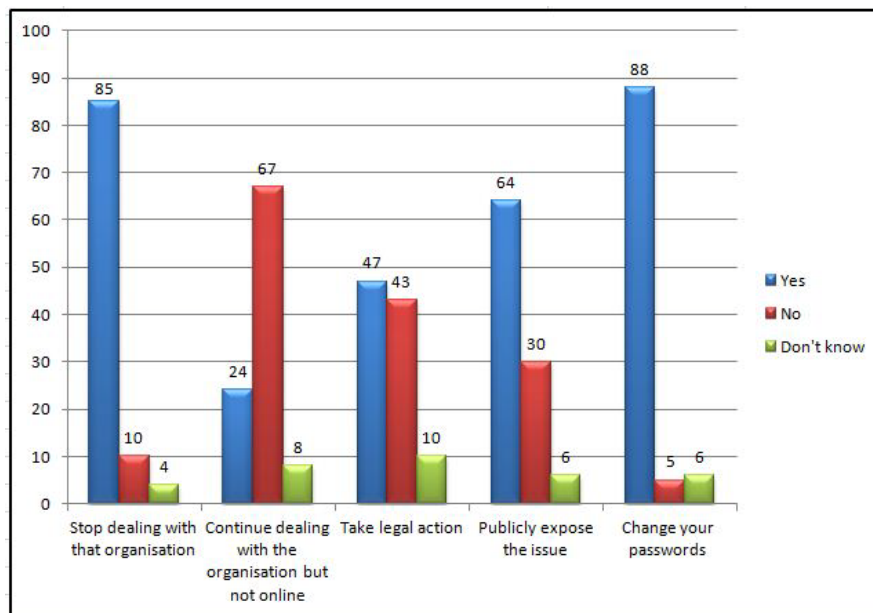


Chart 1: Key actions of Australians aware that their personal information held by an organisation they dealt with had been accessed by an unauthorised person

These findings highlight the potential business and financial implications arising from the loss of customer trust and confidence following a data breach. Therefore data security is not just an IT issue – it is a business issue.

The results are also a signal to organisations that hold customer or client information that Australians will be unforgiving if their private information is accessed by unauthorised people – whether accidentally or as part of a malicious attack. It appears consumers today recognise their power to fight back and will take action that has the potential to impact the bottom line.

Of the 12 countries surveyed, the US and Australia were the two countries where people are most likely to expose the issue publically – suggesting that the Australian public expects organisations to be held accountable for data breaches.

However there is also recognition of personal responsibility to reduce vulnerability following a data breach with 88 percent of Australians saying they would change passwords on the affected organisation’s website and any others they might be concerned about.

Percent saying they would take the following action following a data security breach					
	Change passwords on that organisation’s websites and other websites you use	Stop dealing with that organisation, such as close the account	Publicly expose the issue	Take legal action	Continue dealing with that organisation, but not online
Australia	88	85	64	47	24
Belgium	88	73	52	32	19
Brazil	90	79	56	86	37
Colombia	92	73	62	60	23
Germany	82	79	52	60	21
Hong Kong	79	81	60	40	36
Mexico	86	84	62	61	44
Netherlands	88	69	42	23	22
New Zealand	91	80	48	36	26
Spain	88	81	61	64	27
UK	83	82	56	54	25
US	87	76	65	53	31

Chart 2: Responses from 12 countries regarding their actions if aware that their personal information held by an organisation they dealt with had been accessed by an unauthorised person

Background

These results represent findings asked as part of the 2011 Unisys Security Index program. The Unisys Security Index is a global study that provides insights into the attitudes of consumers on a wide range of security related issues.

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 16 – 18 September 2011 by Newspoll using a nationally representative sample of 1,205 respondents aged 18 years and over. All results have been post-weighted to Australian Bureau of Statistics data.

Similar research was conducted in 12 countries: Australia, Belgium, Brazil, Colombia, Germany, Hong Kong, Mexico, Netherlands, New Zealand, Spain, UK and US.

For more information on the Unisys Security Index including additional resource material visit: www.unisyssecurityindex.com.au.

Respondents were asked to answer yes, no or don't know to:

Thinking now about security related issues. If you became aware that personal information that was being held by an organisation you dealt with had been accessed by an unauthorised person, would you take any of the following actions?

1. *Stop dealing with that organisation, such as closing your account*
2. *Continue dealing with the organisation but not online*
3. *Take legal action*
4. *Publicly expose the issue*
5. *Change your passwords on that organisation's website and any other sites you are concerned about*

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

For more information on the Unisys Security Index visit: www.unisyssecurityindex.com.au
For more information on Unisys Security offerings visit: www.unisys.com.au

©2011 Unisys Corporation. All rights reserved.

Unisys and the Unisys logo are registered trademarks of Unisys Corporation. All other brands and products referenced herein are acknowledged to be trademarks or registered trademarks of their respective holders. Printed in Australia 11/11