Unisys Security Insights: Global Summary
A Consumer Viewpoint - 2015

How consumers in 12 countries feel about:
- Personal data security, ranked by industry
- Region-specific security perceptions
# Table of Contents

Executive Summary 3  
Unisys Outlook 4  
Findings 5  
  (a) Industries ranked most vulnerable, across all countries 5  
  (b) Country Summary 6  
  (c) Industry Summary 7  
  (d) Detailed Findings 8  
Unisys Perspective on Security 12  
About Unisys Security Insights 13  
Polling Methodology 13  
About Lieberman Research Group 14  
About Newspoll 15  
About Unisys 16
**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 across the world. Unisys’ commitment to public and financial safety and security are the reasons for survey research to monitor progress in these areas.

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 organizations make more informed security decisions. The study measures concern around personal data security across industries such as banking, government, airlines, healthcare, telecom, retail and utilities.

Independent research agencies, Lieberman group and Newspoll conducted the survey in Australia, Brazil, Colombia, France, Germany, Malaysia, Mexico, New Zealand, Spain, the Netherlands, the United Kingdom and the United States.

For the 2015 survey, consumers in 12 countries were asked about their perceptions regarding

- Personal data security, ranked by industry
- Region-specific security perceptions around emerging technologies or current events

According to the survey of 11,244 adults across 12 countries, consumers believe that telecommunications companies, government agencies and banks are the organizations most vulnerable to personal data breaches.

Among the 12 countries surveyed, consumers in the Netherlands and Germany have the highest level of concern regarding personal data security. Interestingly, despite recent instances of personal data breach, the perceived threat among consumers in U.S. and U.K. is low.

These findings serve as a reminder for organizations across the world to review and deploy advanced security measures, to protect consumers from cyber as well as physical threats. A proactive outlook to security is at the heart of an organization’s ability to effectively mitigate risk environment. The Unisys approach 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/securityinsights](http://www.unisys.com/securityinsights)

For more information on Unisys security offerings, visit: [www.unisys.com/security](http://www.unisys.com/security)
Unisys Outlook

Consumers are most concerned about their personal data held by telecom, government and banking industries

Unisys Security Insights asked respondents across 12 countries about their perceptions regarding personal data security held by organizations across various industries. The survey revealed high levels of concern among consumers for few industries like telecom, government and banking, while perceived vulnerability levels were relatively low in airlines, retail and healthcare.

- The perceived vulnerability among consumers regarding cyber security is high in telecom companies (59 percent), most likely due to increased occurrences of data theft in this industry across all countries surveyed.
- Level of concern is also high in government agencies and banks (49 and 48 percent respectively), possibly attributed to the lack of confidence-building initiatives taken up by these organizations despite the recent high profile breaches.
- Apprehension about unauthorized access in airlines scored low across all countries (34 percent), probably driven by the fact that there have been no instances of any major cyber-attacks in this industry over the last few years.

Dutch, German and Brazilian consumers are most concerned about data security

Among the 12 countries surveyed, six countries including the Netherlands, Germany, Brazil, Colombia, Spain and New Zealand, have relatively higher levels of concern regarding personal data security.

- The perceived threat of data breach is high among Dutch adults (59 percent), understandably driven by the fact that the Netherlands has one of the highest percentage of internet users in the world.
- German and Brazilian consumers are also anxious about personal data security (58 and 53 percent respectively), reflecting a need to improve cybersecurity as organizations in these countries face an increased exposure to cyber threats.

Evidently, consumers across the world are wary of losing sensitive personal information to cyber-attacks. As cyber criminals continue to design malicious software for a wide spectrum of devices, organizations should adopt a proactive security approach to mitigate risks. To inspire customer confidence while preventing loss of business and reputation, organizations must review and enhance existing security measures on a continuous basis to:

- Gain continued visibility into security gaps and remedial activities.
- Shield against evolving cyber and physical threats.
- Ensure business objectives are met within the enterprise’s security, compliance and governance framework.
Findings

(a) Industries ranked most vulnerable, across all countries

When organizations are ranked according to the percentage of consumers saying that a personal data breach in the next year is likely, telecommunications companies are consistently ranked as most likely and are thus seen as most vulnerable. The perceived threat of data breach is also high in government agencies and banks.

Meanwhile, airlines, utilities and healthcare organizations are seen as least vulnerable to personal data breaches.
(b) Country Summary: Likelihood of a data breach in next 12 months, by country

Concern about personal data security is high in some countries, and the expectation of a data breach ranges from 31 percent for U.S. to 59 percent for Netherlands.

Consumers in six countries have high levels of concern about personal data security (scored above the 12-country mean of 45 percent), and includes the Netherlands, Germany, Brazil, Colombia, New Zealand and Spain.

On average, more than half of Dutch (59 percent), German (58 percent) and Brazilian (53 percent) adults see the likelihood of a data breach in the next 12 months.
(c) Industry Summary: Likelihood of a data breach in next 12 months, by industry

Concern about personal data breach is high in some industries, and the expectation of a data ranges from 34 percent for airlines to 59 percent for telecommunications companies.

Consumers across the 12 countries are most likely to name telecommunications companies, government agencies, banks and utilities as high concern industries (scored above the 7-industry mean of 45 percent).

On average, data security concern about telecom put this industry in a class by itself as perceived vulnerability is the highest (59 percent). Airlines is perceived as the least vulnerable industry (34 percent).
(d) Detailed Findings

1. Likelihood of data breach in telecommunications companies

Six countries have high levels of data concern (scored above the mean of 59 percent), and the proportion seeing a data breach ranges from 35 percent for U.S. to 78 percent for Germany.

The proportion of consumers seeing a possibility of data breach in government agencies ranges from 36 percent to 69 percent.
3. Likelihood of data breach in banks and other financial institutions

Among the 12 countries, the proportion of consumers seeing a data breach in banks ranges from 24 percent to 63 Percent

<table>
<thead>
<tr>
<th>Country</th>
<th>Likelihood of data breach in banks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Germany</td>
<td>63%</td>
</tr>
<tr>
<td>Netherlands</td>
<td>63%</td>
</tr>
<tr>
<td>Colombia</td>
<td>57%</td>
</tr>
<tr>
<td>Brazil</td>
<td>53%</td>
</tr>
<tr>
<td>Mexico</td>
<td>52%</td>
</tr>
<tr>
<td>Spain</td>
<td>52%</td>
</tr>
<tr>
<td>France</td>
<td>50%</td>
</tr>
<tr>
<td>New Zealand</td>
<td>50%</td>
</tr>
<tr>
<td>12-country mean</td>
<td>48%</td>
</tr>
<tr>
<td>Australia</td>
<td>46%</td>
</tr>
<tr>
<td>Malaysia</td>
<td>35%</td>
</tr>
<tr>
<td>UK</td>
<td>25%</td>
</tr>
<tr>
<td>US</td>
<td>24%</td>
</tr>
</tbody>
</table>

4. Likelihood of data breach in utilities companies such as water, gas and electricity

The perceived likelihood of a security breach in utility companies ranges from 21 percent to 62 Percent

<table>
<thead>
<tr>
<th>Country</th>
<th>Likelihood of data breach in utilities companies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netherlands</td>
<td>62%</td>
</tr>
<tr>
<td>Germany</td>
<td>60%</td>
</tr>
<tr>
<td>Spain</td>
<td>54%</td>
</tr>
<tr>
<td>Brazil</td>
<td>50%</td>
</tr>
<tr>
<td>Colombia</td>
<td>46%</td>
</tr>
<tr>
<td>Mexico</td>
<td>45%</td>
</tr>
<tr>
<td>12-country mean</td>
<td>45%</td>
</tr>
<tr>
<td>France</td>
<td>43%</td>
</tr>
<tr>
<td>New Zealand</td>
<td>42%</td>
</tr>
<tr>
<td>Malaysia</td>
<td>41%</td>
</tr>
<tr>
<td>Australia</td>
<td>40%</td>
</tr>
<tr>
<td>UK</td>
<td>33%</td>
</tr>
<tr>
<td>US</td>
<td>21%</td>
</tr>
</tbody>
</table>
5. Likelihood of data breach in healthcare organizations including hospitals and doctors

The perceived threat of data breach among consumers in healthcare organizations ranges from 28 percent to 59 percent.

6. Likelihood of data breach in retailers

Consumers across eight countries have high levels of concern about personal data security in retail (scored above the mean of 42 percent), and the proportion ranges from 27 percent to 55 percent.
7. Likelihood of data breach in airlines and other transportation related companies

Among the 12 countries, the proportion seeing an airline data breach ranges from 23 percent in Spain to 45 percent in Germany.

<table>
<thead>
<tr>
<th>Country</th>
<th>Likelihood of data breach in airlines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Germany</td>
<td>45%</td>
</tr>
<tr>
<td>Netherlands</td>
<td>41%</td>
</tr>
<tr>
<td>Brazil</td>
<td>39%</td>
</tr>
<tr>
<td>Colombia</td>
<td>36%</td>
</tr>
<tr>
<td>Malaysia</td>
<td>36%</td>
</tr>
<tr>
<td>New Zealand</td>
<td>35%</td>
</tr>
<tr>
<td>France</td>
<td>34%</td>
</tr>
<tr>
<td>12-country mean</td>
<td>34%</td>
</tr>
<tr>
<td>Australia</td>
<td>33%</td>
</tr>
<tr>
<td>Mexico</td>
<td>31%</td>
</tr>
<tr>
<td>UK</td>
<td>29%</td>
</tr>
<tr>
<td>US</td>
<td>25%</td>
</tr>
<tr>
<td>Spain</td>
<td>23%</td>
</tr>
</tbody>
</table>
Unisys Perspective on Security

The survey suggests that consumers are evidently concerned about their personal data held by organizations. Consumers’ confidence and trust were generally low for telecom companies, government agencies and banks, as these organizations have not succeeded in their confidence-building measures to win back trust. 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. For organizations to regain trust in the face of such an uncertain security environment, they should follow:

- **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, and utilize 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 multi-factor 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 Organizations, mobile devices too allow for advanced authentication techniques to prevent intrusions and information theft. The opportunity for organizations is to grow in tandem with consumer preferences while ensuring highest levels of protection.

- **Isolation and compartmentalization for data protection** – Protecting sensitive information from unauthorized 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 authorized systems and users can access sensitive information. In addition, compartmentalization of user groups also result in minimizing 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](http://www.unisys.com/security)
About Unisys Security Insights

Unisys Security Insights is global research that provides insights into 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. For more information, visit [www.unisys.com/securityinsights](http://www.unisys.com/securityinsights)

Polling Methodology

The Unisys Security Insights research is based on national surveys covers 11,244 consumers, aged 18 and above, across 12 countries.

The respondents for the survey were interviewed by telephone except in Mexico, Spain, Colombia and France, where they were conducted face-to-face, and in the US and UK, where they were conducted online.

Independent research agencies, Lieberman group and Newspoll conducted the survey in Australia, Brazil, Colombia, France, Germany, Malaysia, Mexico, New Zealand, Spain, the Netherlands, the United Kingdom and the United States.

- The survey was conducted across randomly selected households in April and May, 2015.
- The sample is weighted with respect to national demographic characteristics such as gender, age, region, town size, education and occupation.
About Lieberman Research Group

Lieberman Research Group is a top-ranked and nationally recognized market research organization serving the business-to-business and consumer markets. Founded in 1966, it is now a $30 million custom research company. Interviewing facilities in Manhattan and Brooklyn have the capability to conduct interviews in 20+ languages.

Lieberman Research is the only U.S. member of The Global Research Alliance – an international consortium of independent market research firms in over 20 countries that provides access to interviewing facilities internationally as well as local knowledge and input critical to successful international studies.

Through its research in the U.S. and worldwide, Lieberman Research provides custom research and information analysis to its clients on a wide range of issues including customer and employee satisfaction, loyalty, multicultural and ethnic marketing, new product development, public policy, advertising, public relations and many others.

Lieberman Research Group is a proud member of the Council of American Survey Research Organizations (CASRO). As one of over 150 CASRO member companies nationwide, we subscribe to the CASRO Code of Standards for Survey Research.

This code, intended to foster the highest standards of ethical conduct in the practice of survey research, protects our clients and helps ensure an environment in which the public, our source of information in most surveys, respects and cooperates with the opinion research process.

While non-members also may subscribe to the same high standards as CASRO members, membership in CASRO is an indication that our company takes seriously its obligation to conduct its business in accordance with the highest ethical standards.

www.casro.org
About Newspoll

Established in 1985, Newspoll is Australia’s leading public opinion polling company. Our reputation is founded on our long standing and consistent track record in accurately measuring voting intentions at Australian Federal and State election surveys.

Newspoll provides a full range of market research services, including omnibus and customised research, through our client service offices in Sydney, Melbourne & Canberra and our network of associate companies in Australia & around the world. We have a state-of-the-art telephone interviewing centre at our head office in Sydney, and through our sister company, Lightspeed Research, contribute to and have access to a large, research only online panel (MySurvey).

All senior researchers at Newspoll are members of the Australian Market and Social Research Society (AMSRS) and are QPMR accredited (Qualified Practising Market Researchers), closely abiding by the society’s code of professional behaviour. Newspoll is a member of AMSRO (The Australian Market and Social Research Organisations) for which our C.E.O., Martin O’Shannessy, currently holds the position of President.

We are committed to providing our clients with research of the highest quality. Whilst we are ISO20252 accredited, which is the international quality standard for Market Research, many of our systems and procedures go beyond the requirements of this quality standard.

In 2006 Newspoll developed the Security Survey survey in collaboration with Unisys in Australia. The survey has subsequently been rolled out to many other countries around the globe, and Newspoll is responsible for coordinating the survey in the Asia Pacific region, partnering with Consumer Link, who conduct fieldwork in New Zealand.
About Unisys

Unisys is a global information technology company that solves organizations’ 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.

For more information visit www.unisys.com

© 2015 Unisys Corporation. All rights reserved.

Unisys and other Unisys products and services mentioned herein, as well as their respective logos, are trademarks or registered trademarks of Unisys Corporation. All other trademarks referenced herein are the property of their respective owners.

06/15  15-0227 (i)