UNISYS

Unisys Security Insights: Brazil
A Consumer Viewpoint - 2015

How Brazilian consumers feel about:

- Personal data security, ranked by industry
- Security concerns related to 2016 Olympics

Research by

LIEBERMAN

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 Brazil. 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 research is conducted by leading market research company Lieberman Research Group.

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

- Personal data security, ranked by industry
- Security concerns related to 2016 Olympics

Threat to personal data security is high across some industry sectors in Brazil. Depending upon the type of organization, the expectation that a security breach is likely within the next 12 months ranges from 39 percent for airlines to 67 percent for telecommunications providers.

Brazilians also have security concerns related to 2016 Olympic Games, as a majority of consumers surveyed have expressed at least one concern.

These findings serve as a reminder for Brazil businesses and institutions 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

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

Unisys Outlook

Unisys Security Insights Report – Brazil

The results of Unisys' Security Insights 2015 indicate that Brazilians are most concerned about their personal data held by telecom companies, as around two thirds expect a data breach in the next 12 months (67 percent). The perceived vulnerability of telecom companies stand out, most likely due to the recent high profile cases of data breach. Consumers in Brazil are also apprehensive about cybersecurity threats in government agencies and retailers (60 and 55 percent respectively), with retail recording the highest level of concern for all countries surveyed. The threat of data breach in the next 12 months is low in airlines and healthcare organizations (39 and 47 percent respectively).

For a majority of industries, cybersecurity concerns are consistently significant for above average social class.

There is clearly a considerable level of concern among consumers on matters relating to personal data security. Organizations should deploy security solutions with visibility across all aspects of operations, to prevent data losses and regain consumer confidence.
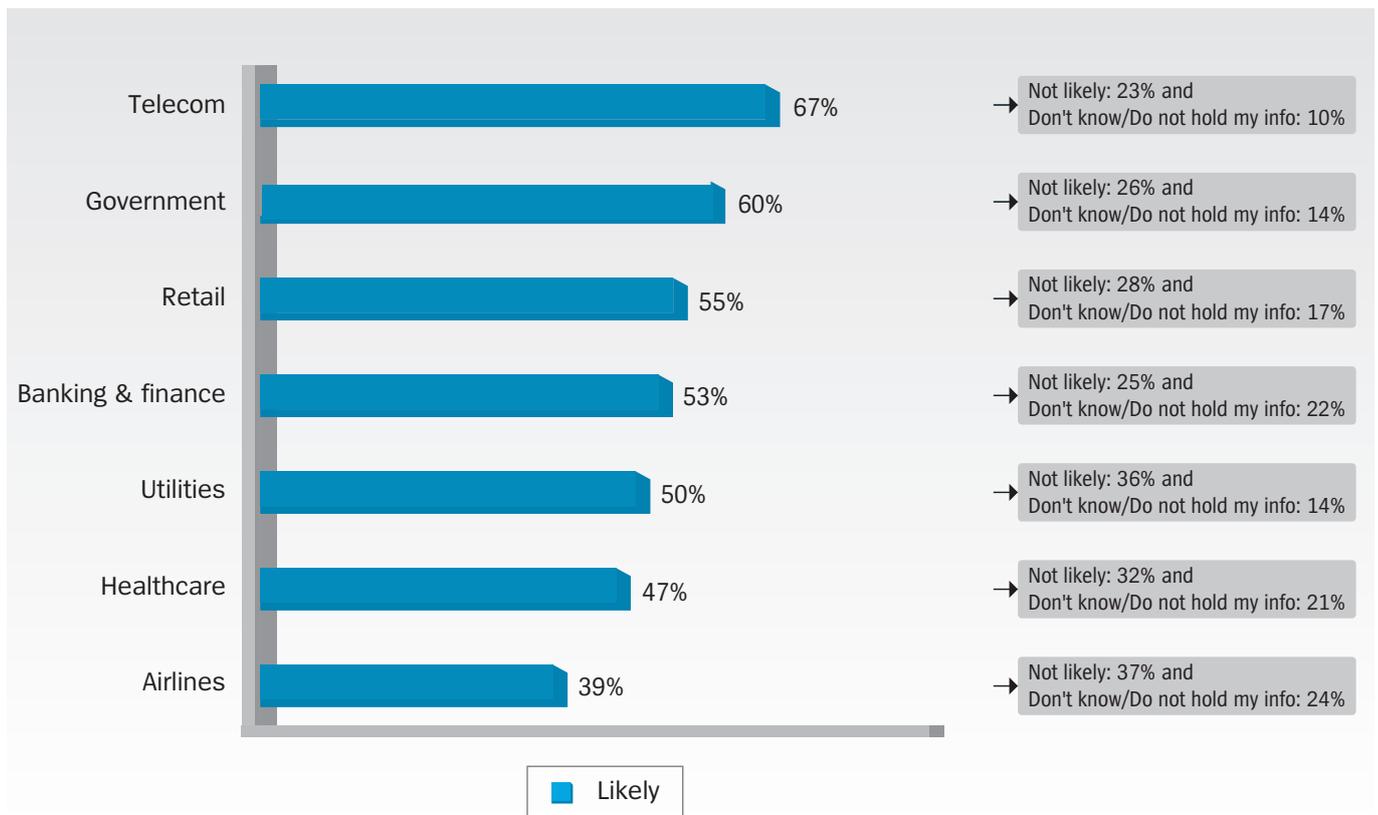
Security related concerns regarding the 2016 Olympic Games are high

As part of the Unisys Security Insights, consumers were also asked about the biggest security concern regarding the 2016 Olympic Games in Brazil. The research revealed that concerns regarding the event are high, as 77 percent of those surveyed have at least one apprehension. Among concerns, urban violence is by far the biggest worry (57 percent), followed by security in public transportation (11 percent) and attacks by terrorist groups (9 percent).

Security concerns about 2016 Olympic Games calls for proactive measures to be taken, in order to improve the safety perceptions about the event among Brazilians.
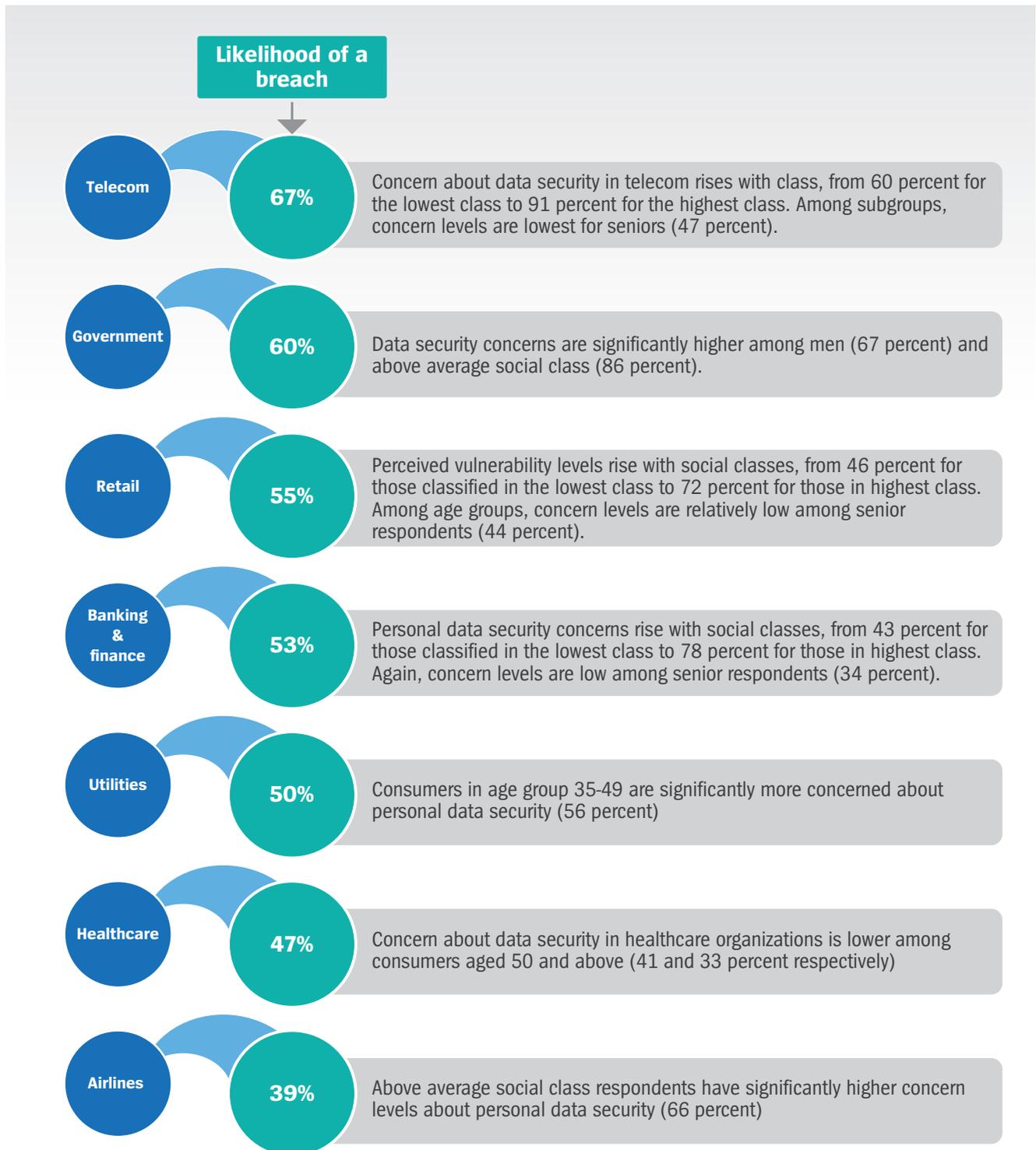
Detailed Findings: (1) For each of the following types of organizations that collect your personal information, how likely do you think it is that your personal information will be accessed by an unauthorized person either accidently or deliberately within the next 12 months?

The perceived vulnerability of different organizations is highest for telecommunications companies, as two thirds (67 percent) of Brazilian adults expect a data breach in the next 12 months.

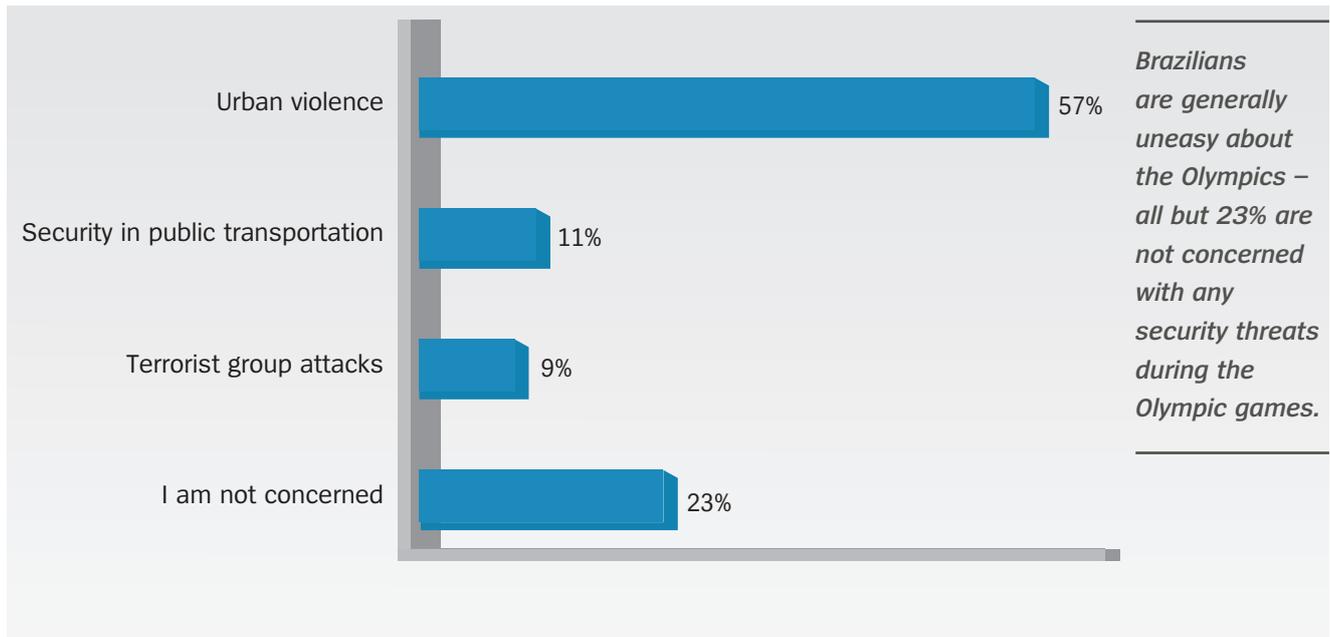| Organization	Likely	Details
Telecom	67%	Not likely: 23% and Don't know/Do not hold my info: 10%
Government	60%	Not likely: 26% and Don't know/Do not hold my info: 14%
Retail	55%	Not likely: 28% and Don't know/Do not hold my info: 17%
Banking & finance	53%	Not likely: 25% and Don't know/Do not hold my info: 22%
Utilities	50%	Not likely: 36% and Don't know/Do not hold my info: 14%
Healthcare	47%	Not likely: 32% and Don't know/Do not hold my info: 21%
Airlines	39%	Not likely: 37% and Don't know/Do not hold my info: 24%

Legend: ■ Likely

Key Demographic Differences by Industry

Consumer responses were analyzed based on demographic segments gender, age and social class. Age categories are 18-34, 35-49, 50-64 and 65+ and social classes are classified as above average, average and below average.

Likelihood of a breach

Telecom — **67%**
Concern about data security in telecom rises with class, from 60 percent for the lowest class to 91 percent for the highest class. Among subgroups, concern levels are lowest for seniors (47 percent).

Government — **60%**
Data security concerns are significantly higher among men (67 percent) and above average social class (86 percent).

Retail — **55%**
Perceived vulnerability levels rise with social classes, from 46 percent for those classified in the lowest class to 72 percent for those in highest class. Among age groups, concern levels are relatively low among senior respondents (44 percent).

Banking & finance — **53%**
Personal data security concerns rise with social classes, from 43 percent for those classified in the lowest class to 78 percent for those in highest class. Again, concern levels are low among senior respondents (34 percent).

Utilities — **50%**
Consumers in age group 35-49 are significantly more concerned about personal data security (56 percent)

Healthcare — **47%**
Concern about data security in healthcare organizations is lower among consumers aged 50 and above (41 and 33 percent respectively)

Airlines — **39%**
Above average social class respondents have significantly higher concern levels about personal data security (66 percent)

Detailed Findings: (2) What is your biggest security concern regarding the 2016 Olympic Games in Brazil?

Over half (57 percent) say that urban violence is their biggest Olympics-related security concern

Category	Percent
Urban violence	57%
Security in public transportation	11%
Terrorist group attacks	9%
I am not concerned	23%

Brazilians are generally uneasy about the Olympics – all but 23% are not concerned with any security threats during the Olympic games.

Key Demographic Differences

Urban Violence	Women are most likely to cite urban violence as the biggest concern (62 percent)
Public transit security	Young adults are most likely to cite public transit security as their biggest concern (16 percent)
Terrorism	Brazilians in the lowest social class are most likely to cite terrorist attacks as the biggest concern (14 percent)

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, 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

Polling Methodology

The Unisys Security Insights research in Brazil is based on a telephone survey carried out in April 22 - May 4, 2015. The survey has been conducted as follows:

• 1,026 completed interviews among nationally representative adults, 18 and above.

• The survey is conducted in Brazilian Portuguese.

• The data from this survey are weighted to ensure projectability of the data to Brazilian adults.

Percentages are based on the full sample of 1,026. Subgroup differences are noted if they are statistically significant at a 95 percent level of confidence.

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 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