

Unisys Security Insights: Colombia

A Consumer Viewpoint - 2015



How Colombia consumers feel about:

- Personal data security, ranked by industry
- Vulnerability of various online transaction channels

Table of Contents

| | |
|--|----|
| Executive Summary | 3 |
| Unisys Outlook | 4 |
| Detailed Findings: (1) Likelihood of Data Breach | 5 |
| Key Demographic Differences by Industry | 6 |
| Detailed Findings: (2) Vulnerability to Cyberattacks | 7 |
| Key Demographic Differences | 7 |
| Unisys Perspective on Security | 8 |
| Polling Methodology | 9 |
| About Lieberman Research Group | 10 |
| About Unisys | 11 |

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 Colombia. 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 Colombia were asked about their perceptions regarding

- Personal data security, ranked by industry
- Vulnerability of various online transaction channels

Threat to personal data security is high across some industry sectors in Colombia. Depending on the type of organization, the expectation that a security breach is likely within the next 12 months ranges from 36 percent for airlines to 71 percent for telecommunications providers.

Colombia consumers also have security concerns related to online transactions. The vulnerability to cyberattacks is greatest for ATMs and online purchases using desktop or laptop computers, while smartphones and tablets are seen as least vulnerable.

These findings serve as a reminder for Colombia 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

High concern among Colombians about personal data security in telecom

The results of Unisys' Security Insights 2015 indicate that consumers in Colombia are most concerned about their personal data held by telecom companies, as around two thirds expect a data breach in the next 12 months (71 percent). The perceived vulnerability of telecom companies stand out, most likely due to the recent high profile cases of data breach. Consumers in Colombia are also apprehensive about cybersecurity threats in banks (57 percent), while threat of a data breach is relatively low across airlines and retailers in the next 12 months.

For a majority of industries, cybersecurity concerns are consistently low among seniors.

Consumers in Colombia have high levels of data security concern across some industry sectors, and organizations would do well to mitigate these perceptions by proactively implementing IT security solutions to improve confidence.

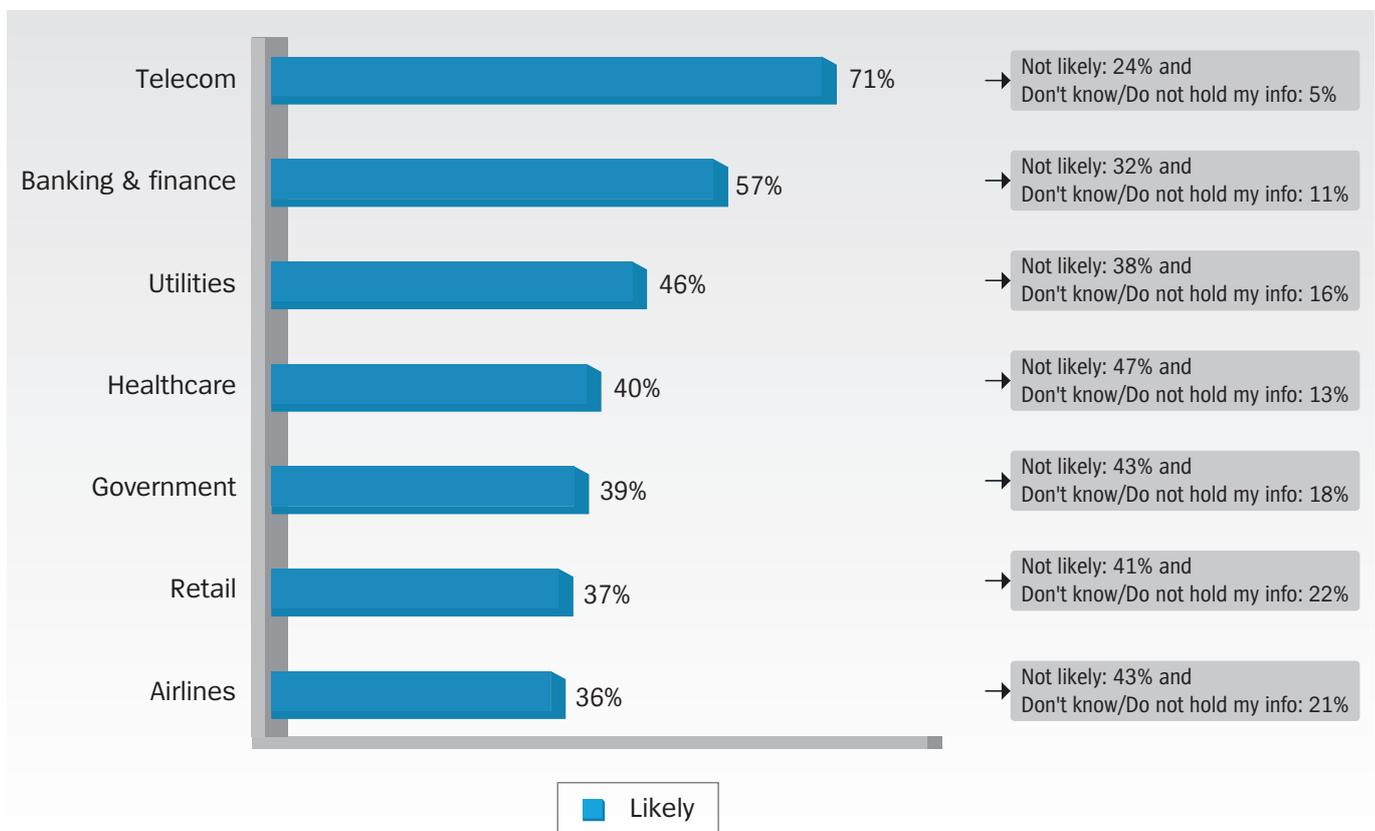
Security related concerns regarding online transactions

As part of the Unisys Security Insights, consumers were also asked about their perceptions regarding the transaction channel most vulnerable to suffer cyberattack. The research revealed that concern regarding cyberattacks on ATMs are the highest (34 percent). The consumers also cite online purchases with desktops/laptops as a transaction channel highly vulnerable to cyberattacks (30 percent), while payments through mobile devices are considered the safest.

It appears that Colombians are skeptical about the safety of their transaction channels. It would be prudent for businesses and public agencies to review and enhance existing security measures across various transaction platforms to gain consumer trust.

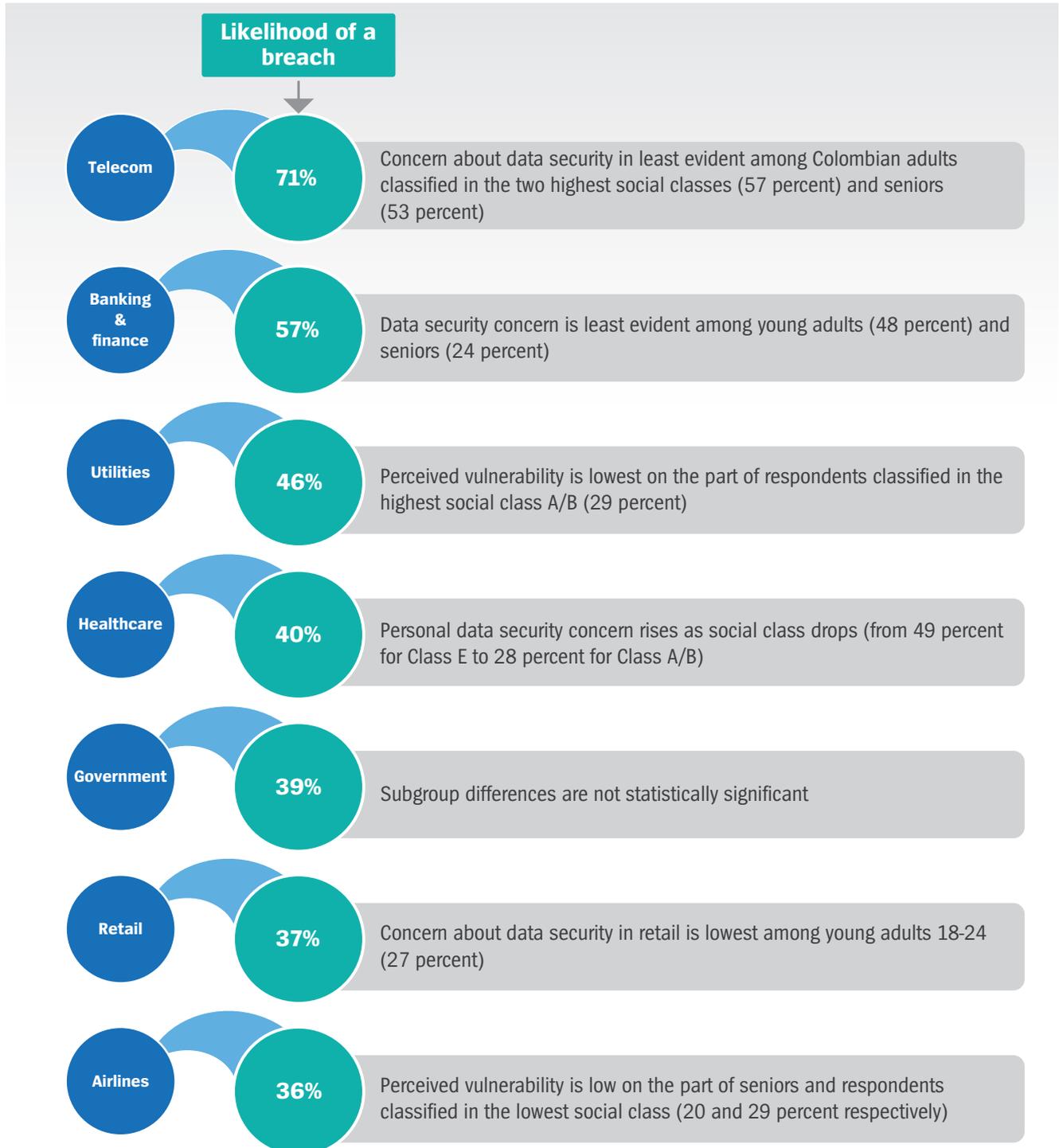
Detailed Findings: (1) For each of the following types of organizations that collect your personal information, how likely do you think it is that your personal information will be accessed by an unauthorized person either accidentally or deliberately within the next 12 months?

The perceived vulnerability of telecommunications companies stands out in the minds of Colombian adults, with more than two thirds (71 percent) of consumers expecting a data breach in the telecom industry in the next 12 months. Concern about banking is also on the high side (57 percent), and from one third to one half of Colombians worry about other organizations as well.



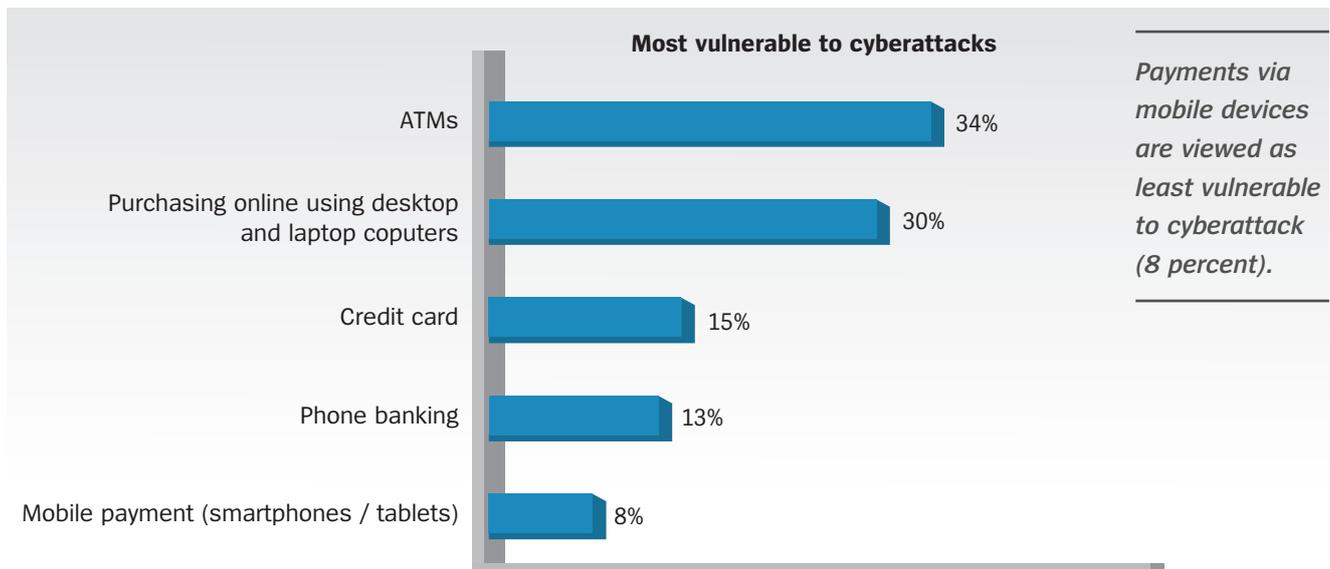
Key Demographic Differences by Industry

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 Class A/B (highest), Class C, Class D and Class E (lowest).



Detailed Findings: (2) In your opinion, which of these transaction channels is MOST vulnerable to suffer cyberattacks?

Colombian respondents cite ATMs (34 percent) and online purchases with desktops / laptops (30 percent) as the channels most vulnerable to suffering a cyberattack.



Key Demographic Differences

| | |
|--------------------------------------|---|
| ATMs | Adults classified in the lowest social class are more likely to cite ATMs as most vulnerable (41 percent), while young adults are least likely (25 percent) |
| Online purchases via computer | Concern about online transactions via computers is significantly high among adults classified in Class C and Class A/B (46 and 39 respectively) |
| Credit Cards | Adults in Class C (6 percent) are less likely to cite credit card transactions as most vulnerable |
| Phone Banking | Subgroup differences are not statistically significant |
| Mobile Payments | Subgroup differences are not statistically significant |

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 Colombia is based on personal interviews carried out in April 14-21 2015. The survey has been conducted as follows:

- 510 completed interviews among nationally representative adults, 18 and above.
- The survey is conducted in Spanish.
- The data from this survey are weighted to ensure projectability of the data to adults in Colombia.

Percentages are based on the full sample of 510. 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

© 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.