UNISYS

Unisys Security Insights: U.S.

A Consumer Viewpoint - 2015

How US consumers feel about

- Personal data security, ranked by industry
- Biometrics as a security measure

Research by

LIEBERMAN

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) Biometrics for Smartphone Data Security	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 the U.S. 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 U.S. were asked about their perceptions regarding

- Personal data security, ranked by industry
- Biometrics as a security measure

Levels of concern about cybersecurity are high in some U.S. industry sectors. Depending upon the type of organization, the expectation that a security breach is likely within the next 12 months ranges from 21 percent for utilities to nearly half (44 percent) for retailers.

Perceptions concerning the effectiveness of biometrics are mixed in the U.S. About one third view biometrics as effective, while a similar proportion is unsure.

These findings serve as a reminder for businesses and institutions in the U.S. 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 Americans about personal data security in retailers and government agencies

The results of Unisys' Security Insights 2015 indicate retail and government agencies are the top two industries that concern consumers the most that their personal data might be compromised (44 and 39 percent respectively). Concern about unauthorized access in retail is high, as consumers seem to be less trusting of retailers owing to recent high profile data breaches at several retail chains, including the likes of a leading general merchandiser and a dominant home improvement specialist. The perceived threat of a data breach in the next 12 months is also relatively high among government agencies, most likely a result of recently reported cyberattacks.

Interestingly, despite the recent targeting of high profile banks by hackers, the perceived threat of data breach is low among banks (24 percent), possibly reflecting traditional high levels of trust in the security of these organizations.

Among demographic profiles, concerns of data breach are most evident across older middle-aged respondents (age group 50-64).

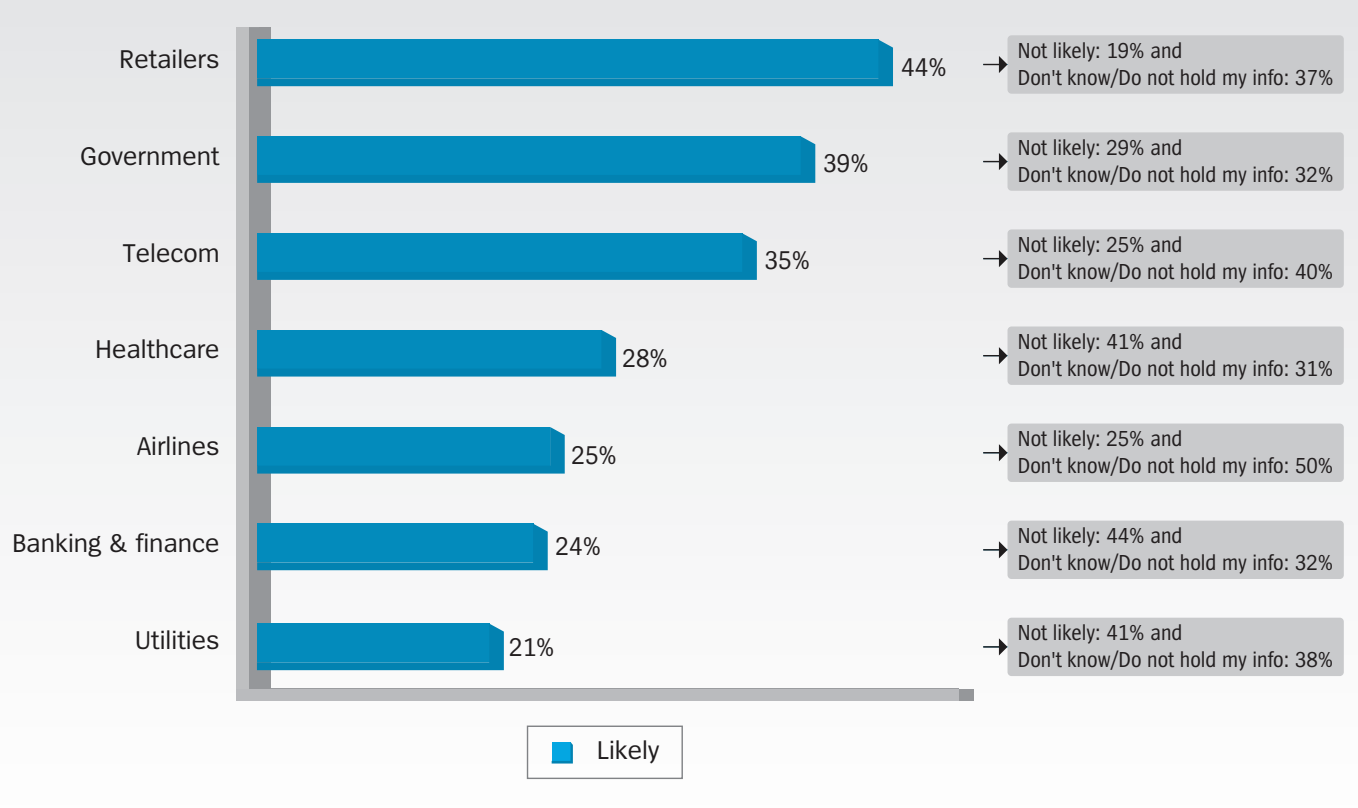
Perceptions concerning the effectiveness of biometrics for smartphone protection are split in the U.S.

As part of the Unisys Security Insights, American respondents were also asked about their perceptions regarding the usage of biometrics as a security measure. The research revealed that perceptions are split, and 38 percent of the total respondents endorse biometrics to increase their smartphone cybersecurity. This apprehension seems to be consistent across all demographic subgroups.

Biometric techniques like voice, signature and facial recognition allow for advanced authentication, and leverage built-in capabilities of next generation devices. The awareness about benefits of biometrics as a security measure seem to be low among consumers, and organizations need to educate them to improve adoption.

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?

Americans are most concerned about cybersecurity risks from retailers, with nearly half (44 percent) describing the chance of a retailer data breach in the next 12 months as "likely". Concern is also high in government agencies (39 percent) and telecommunications providers (35 percent).



Key Demographic Differences by Industry

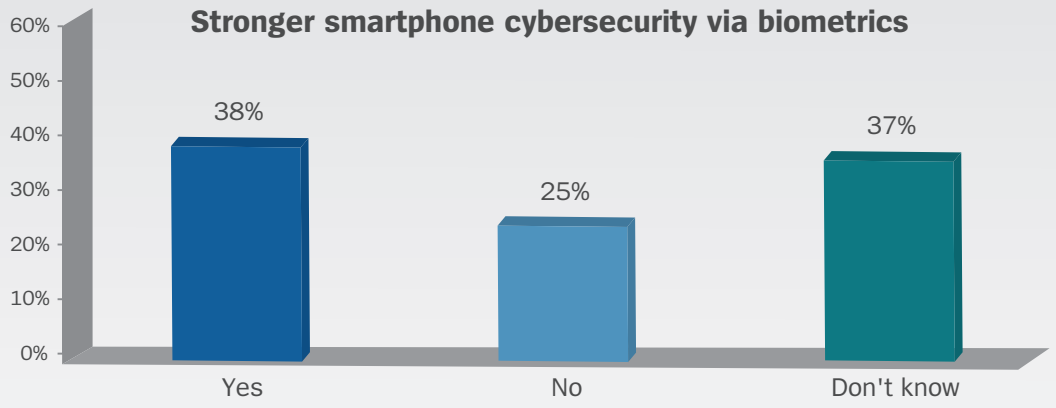
Consumer responses were analyzed based on demographic segments gender, age, income and region. Age categories were 18-34, 35-49, 50-64 and 65+, income groups Under $50K and Over $50K and regions segmented by Northeast, Midwest, South and West.

Likelihood of a breach

Retail	44%	Data security concerns are significantly high on the part of men (46 percent), older middle aged respondents (49 percent), and Americans with incomes of $50,000 or more (48 percent).
Government	39%	Middle aged (41 percent) and older (45 percent) respondents have significantly high data security concerns
Telecom	35%	Threat of data breach is significantly high among men (38 percent) and older middle aged (40 percent) respondents
Healthcare	28%	The perceived vulnerability levels are significantly high among older middle aged respondents (33 percent) and Americans living in the western region (32 percent)
Airlines	25%	Concerns about personal data security are significantly high among men (28 percent), older middle aged respondents (28 percent), seniors (27 percent) and Americans with incomes of $50,000 or more (28 percent)
Banking & finance	24%	Older middle aged respondents (29 percent) have significantly high concern levels about personal data security
Utilities	21%	Americans over the age of 35 have significantly higher data security concerns than younger respondents

Detailed Findings: (2) Do you feel that the use of biometrics such as fingerprint readers on smartphones strengthens the security of your information?

Perceptions concerning the effectiveness of biometrics for smartphone protection are split in the U.S. Over one third (38 percent) feel that the use of biometrics on smartphones strengthens cybersecurity, but one quarter (25 percent) are skeptical.



Among demographic profiles, the possibility of using biometrics to increase smartphone security is significantly higher among men.

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 for the U.S. is based on online surveys carried out in April 17-19, 2015. The survey has been conducted as follows:

- 1,016 completed interviews among nationally representative adults, 18 and above.
- Respondents are from an online probability panel, recruited through address-based sampling of landlines and cellphone-only households. Non-Internet households are provided with Internet access and a laptop for completion of the survey. Therefore, the sample is not limited to Internet households.
- The survey is conducted in English and representative of English-speaking households; and,
- The data from this study are weighted according to the most recent estimates published by the U.S. Census Bureau to ensure projectability of the data to U.S. adults.

Percentages are based on the full sample of 1,016. Subgroup differences 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.

Advancing the Business of Research
CASRO®
COUNCIL OF AMERICAN SURVEY RESEARCH ORGANIZATIONS®

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.

06/15 15-0227