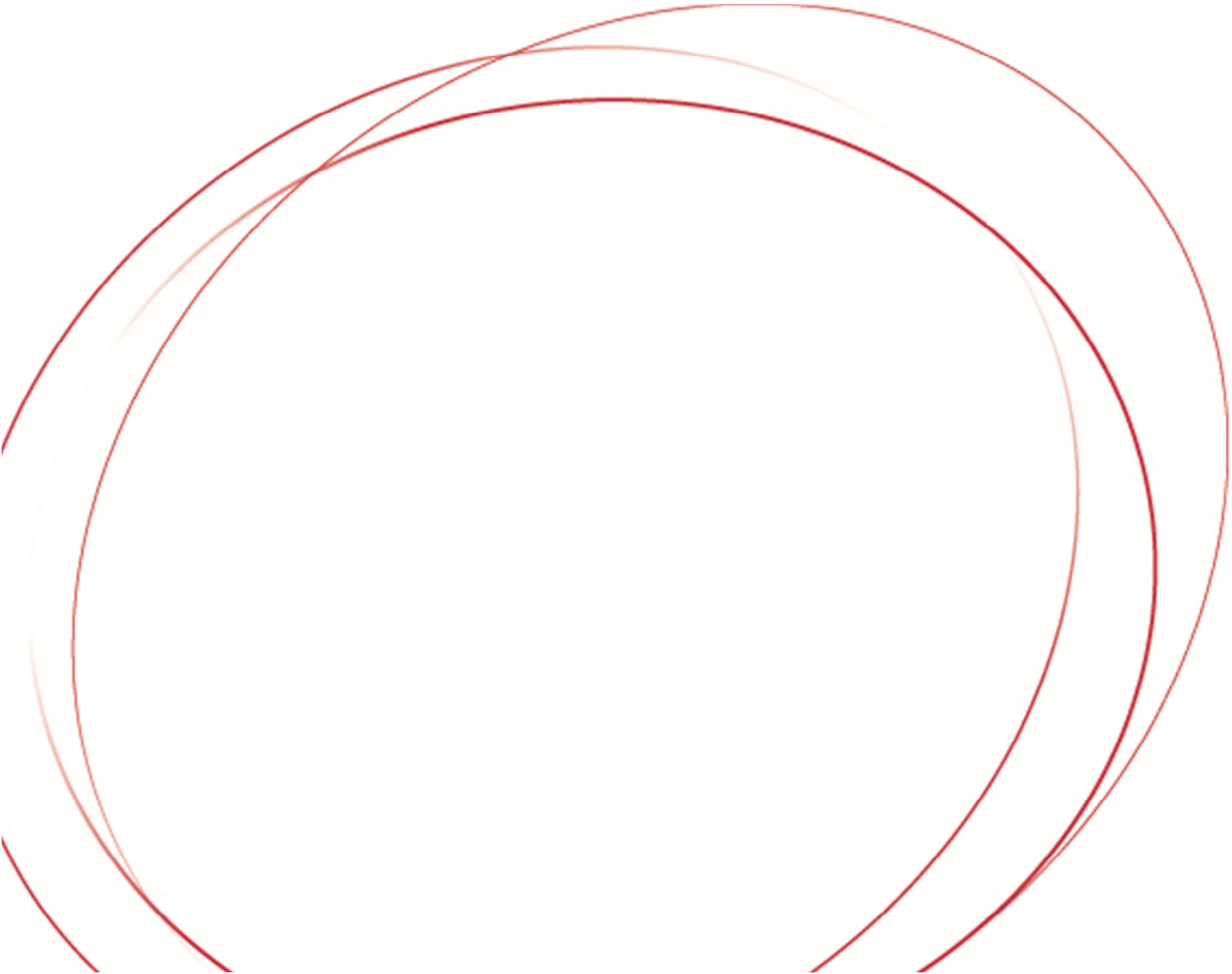
UNISYS

Unisys Security Index™: *US*

20 September 2011 (Wave 2H'11)

Lieberman Research Group



Contents

Executive summary 2
Survey questions 3
Polling methodology 6

Unisys on security

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 US. Unisys' commitments to public and financial safety and security are the reasons for the creation of this index to monitor progress in these areas.

The **Unisys Security Index** is the only regular snapshot of the nation's sense of security. Launched in 2H 2007 and conducted by leading marketing research company Lieberman Research Group, the Unisys Security Index provides a regular, statistically robust measure of concerns about eight areas of security in the areas of finance, personal safety, the Internet, and national security.

For this version of the Index, we instead are focusing on these two key questions:

1. What would you do if you discovered that your personal information being held by an organization you do business with had been accessed by unauthorized person(s); and
2. Would you be willing to provide personal biometric information (fingerprint, voice, iris scan, etc.) to enhance security on your cellphone, Blackberry or other mobile device when accessing any of the following?

Organizations and governments today confront potential security threats that didn't exist a generation ago. The community's sense of security is a critical determinant of public confidence in how governments and private organizations respond. Security threats are global and can impact any individual. 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.unisyssecurityindex.com. For more information on Unisys security offerings, visit www.unisys.com/security.

Executive summary

Americans take exception to the notion of security breaches in organizations with which they do business, and are willing in many cases to provide personal biometric data to enhance security.

Practically all Americans say they would take action of some kind after learning of a security breach, with a large majority saying they would close their account and half saying they would take legal action.

Roughly half would be willing to provide personal biometric data to enhance security for activities such as airport screening and banking transactions.

Survey questions

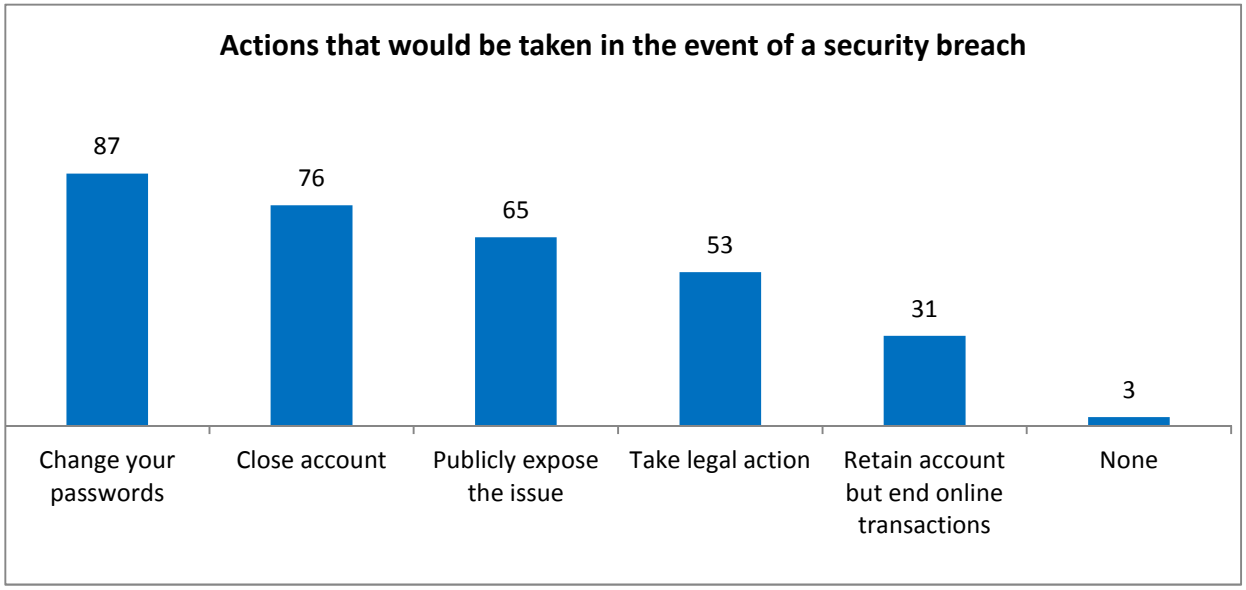
IF YOU BECAME AWARE THAT PERSONAL INFORMATION THAT WAS BEING HELD BY AN ORGANIZATION YOU DEALT WITH HAD BEEN ACCESSED BY AN UNAUTHORIZED PERSON, WHAT WOULD YOU DO?

Practically all Americans say they would take action in the event that they learned of a security breach suffered by an organization with which they were dealing. The most common actions are:

1. Changing passwords on that organization's website and any other sites they would be concerned about (87%)
2. Stop dealing with that organization, such as closing their account (76%)

Half or more say they would publicly expose the issue (65%), or take legal action (53%)

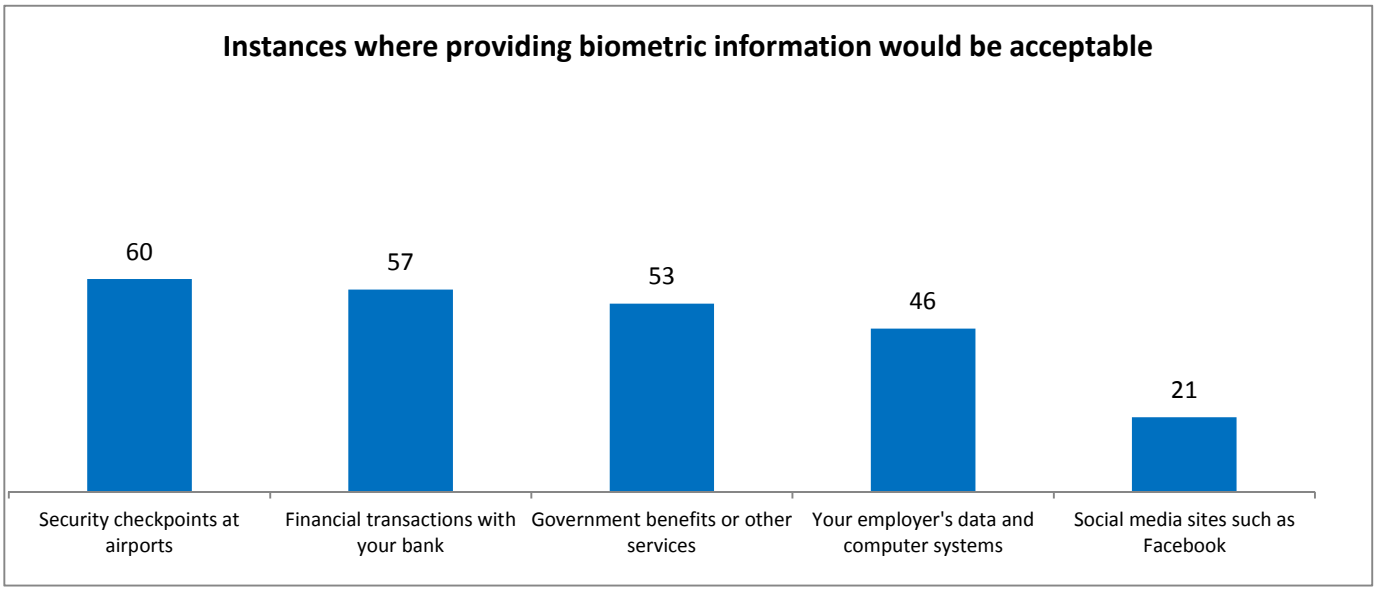
Those who say they would continue dealing with the organization (31%) would not do so online.



WOULD YOU BE WILLING TO PROVIDE PERSONAL BIOMETRIC INFORMATION (FINGERPRINT, VOICE, IRIS SCAN, ETC.) TO ENHANCE SECURITY ON YOUR CELLPHONE, BLACKBERRY OR OTHER MOBILE DEVICE WHEN ACCESSING ANY OF THE FOLLOWING?

Roughly half of Americans would be willing to provide personal biometric information to enhance security around everyday activities, including airport security (60%), banking transactions (57%), government benefits and services (53%) and employer computer systems (46%).

Even 21% would be willing to provide biometric information as part of logging onto social media sites like Facebook.



Variation by demographic group – Supplemental questions

Demographic	Actions taken after security breach	Use of personal biometric data to enhance security
Age	- Seniors are least likely to change their passwords (77%) and to retain their accounts but avoid online transactions (24%). - Americans age 25-34 are least likely to close their accounts (69%).	- Americans age 25-34 are most accepting of biometrics, and seniors least accepting, in connection with banking (68% vs. 50%), government benefits (62% vs. 46%) and employer computers (63% vs. 28%). - Americans age 25-34 and age 55-64 are most accepting of using biometrics for social media (30% and 27% respectively).
Gender	Men and women say they would respond similarly to a security breach.	Men and women have similar attitudes about personal biometric data.
Education	- In the event of a security breach, willingness to take legal action drops with level of education, from 60% of those with high school diplomas or less to 45% of those with college degrees. - College grads are most likely to retain their account but avoid online transactions (40%) while those with high school diplomas or less are least likely to change their passwords (79%).	Americans with differing levels of education have similar attitudes about personal biometric data.
Race	Blacks are most likely to say they would take legal action (69%).	Americans of different races have similar attitudes about personal biometric data.
Region	Americans in different regions say they would respond similarly to a security breach	Midwesterners are most comfortable with using biometrics to access employer computers (53%), while Northeasterners are least accepting (38%).

Polling methodology

The US Security Index is based on a telephone survey of 1006 persons aged 18 and over, September 9-14, 2011. This Wave 2H '11 survey does not include the traditional 8 security questions as first published in 2007 and subsequent studies. Instead, this wave includes a "Global" question – one asked in all countries in the survey – and a country-specific question. The US survey has been conducted as follows:

- 1006 completed interviews among nationally representative adults, 18+;
- Random digit dialing (RDD) sample of telephone households in the US;
- Random selection of household respondent to ensure greater representation;
- The survey is conducted in English and is representative of English-speaking households; and,
- The data from this study are weighted according to the most recent estimates published by the US Census Bureau to ensure projectability of the data to US adults.

Percentages are based on the full sample of 1006 unless otherwise noted. Subgroup variations in top-box percentages are noted if they are statistically significant at a 95% 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

For more information, please visit our web site at www.unisys.com

Printed in the United States of America.