UNISYS

Unisys Security Insights: U.K.

A Consumer Viewpoint - 2015

How consumers in the U.K. feel about:

- Personal data security, ranked by industry
- Drones monitoring public places

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 its customers in the U.K. Unisys' commitment to public and financial safety and security are the reasons for our research in these areas.

The Unisys Security Insights survey is a snapshot of the nation's views on security in certain focus areas that provides a statistical measure of consumer concerns to enable organisations 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.K. were asked about their perceptions regarding

• Personal data security, ranked by industry

• Drones monitoring public places

The survey asked consumers about the likelihood that their personal data – held by organisations including airlines & transportation, banking & finance, government, healthcare, retail, telecoms and utilities – would be accessed by an unauthorised person within the next year.

The perceived threat to personal data security is highest for retailers, with 44 percent of those surveyed expecting a data breach within the next 12 months. Banking & Finance companies were perceived to be the least at risk with just 25 percent of respondents expecting consumer data to be compromised in some way.

Britons have varying opinions towards the usage of drones. Almost half of respondents see drones as helpful in combating anti-social behavior and a third expect improved personal safety from drones (49 percent and 36 percent respectively). On the other hand, 40 percent of respondents do fear the compromise of privacy, and 22 percent view them as a physical danger for the public.

These findings serve as a reminder for businesses and institutions in the U.K. 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 organisation's ability to effectively mitigate risk environment. The Unisys approach to security goes beyond bits and bytes, recognising 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

The U.K. public lack confidence in retailers and telecoms companies when it comes to protecting personal data

The results of Unisys' Security Insights 2015 indicates that consumers in the U.K. lack confidence in retailers and telecoms companies when it comes to protecting personal data with 44 and 43 per cent of respondents expecting a data breach there in the next 12 months, At the other end of the scale, the perceived threat of a data breach is lowest for airlines and banks (29 and 25 percent respectively).

The results indicate that consumers have relatively low expectations of organisations holding personal data on them and that they lack trust in security controls. Organisations should aim to safeguard consumer data by deploying solutions that not only enhance enterprise security, but also inspire consumer confidence.
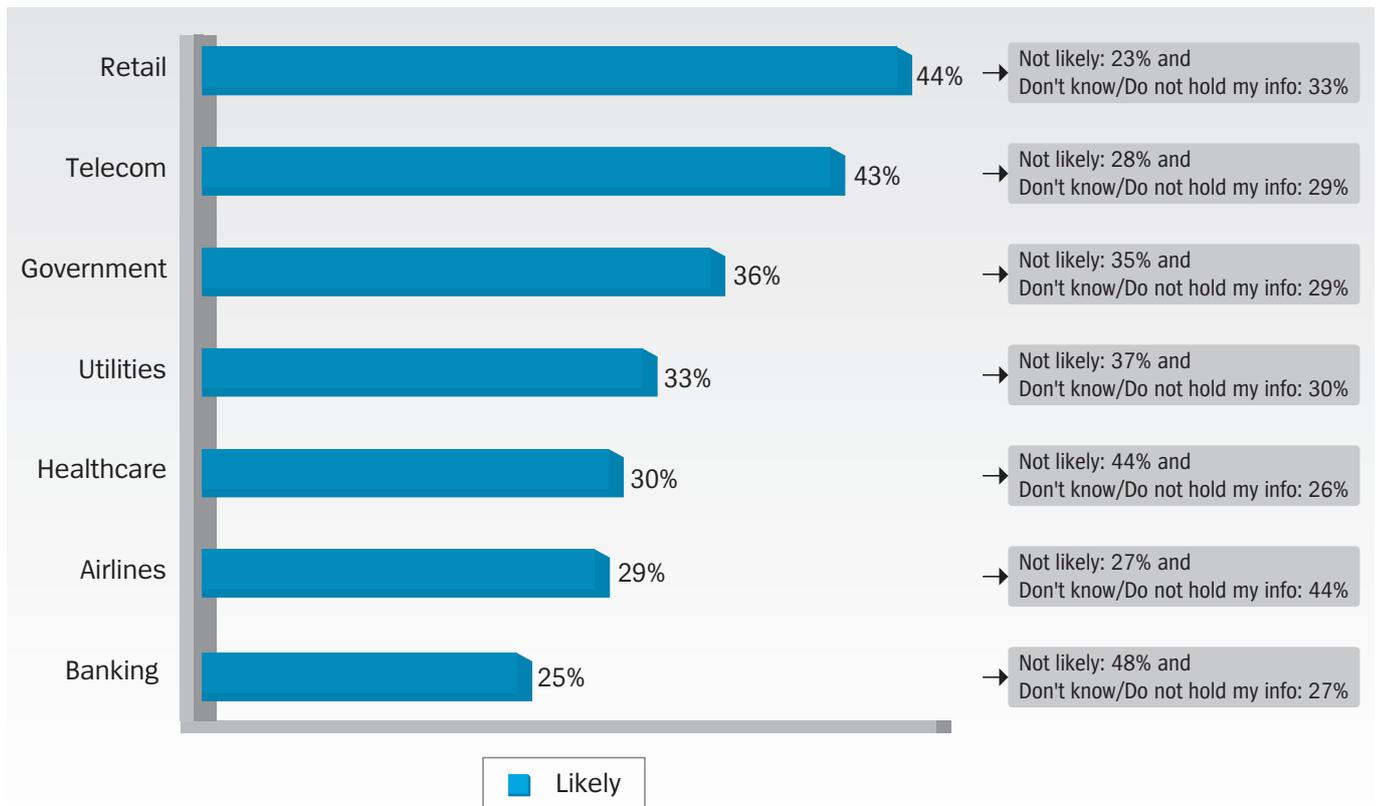
Use of video-equipped drones to monitor or police public spaces splits U.K. consumers

As part of the Unisys Security Insights research, consumers were also asked about their perceptions regarding the usage of drones as a security measure to monitor or police public spaces. The research revealed that perceptions are mixed, with positives outweighing the negatives by a narrow margin.

Usage of drone technology as a security measure to monitor public spaces is still in nascent stages, and is likely to have a profound impact in the years to come, as it is alluring yet alarming. Focus on stringent policy guidelines to allay fears, this should help improve adoption.
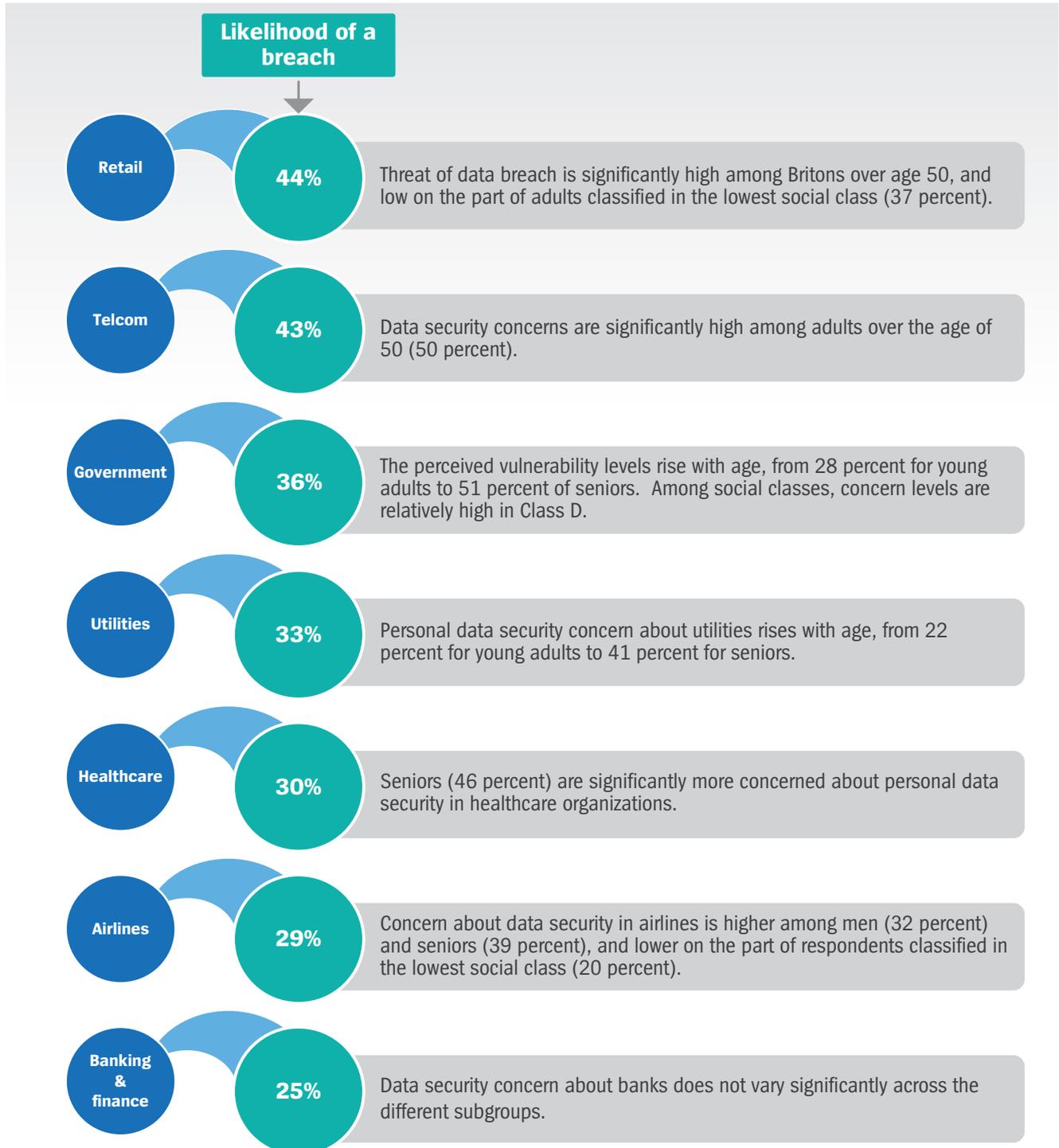
Detailed Findings: (1) For each of the following types of organizations that collect your personal information, how likely do you think it is that your personal information will be accessed by an unauthorized person either accidently or deliberately within the next 12 months?

The perceived vulnerability of different organizations ranges from a quarter to a half, with 25 percent (lowest proportion) of British adults expecting a data breach in banks and 44 percent seeing retailers as vulnerable (highest proportion).

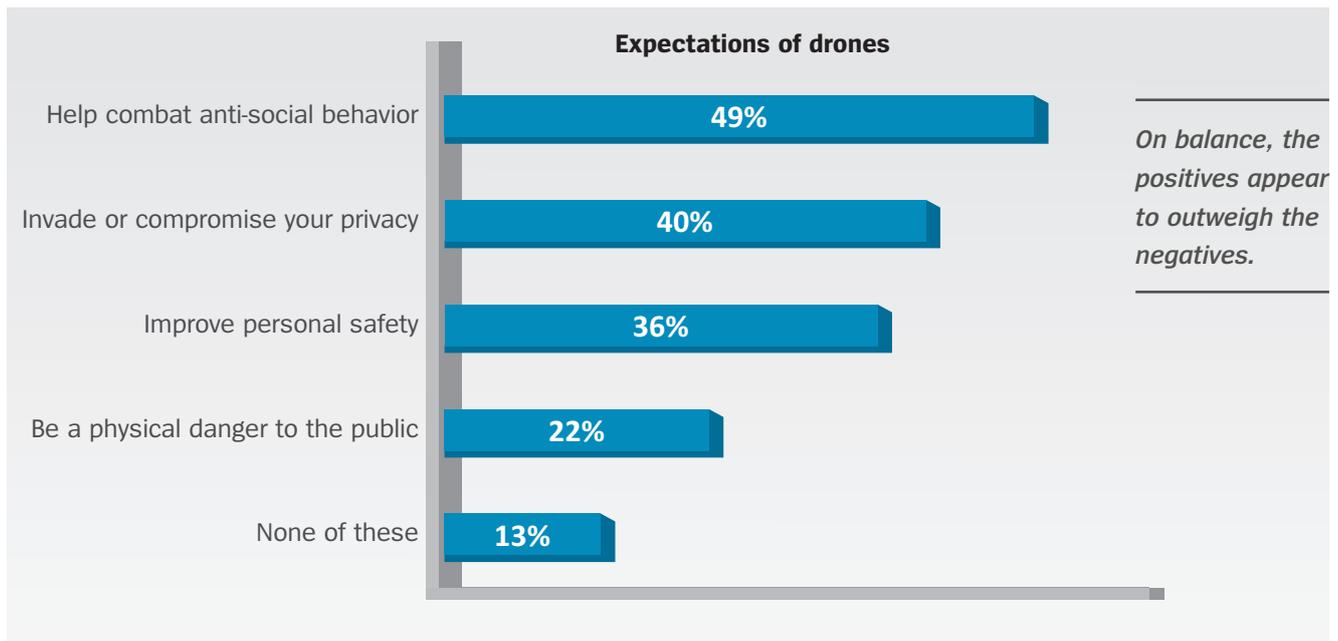| Organization	Likely	Additional info
Retail	44%	Not likely: 23% and Don't know/Do not hold my info: 33%
Telecom	43%	Not likely: 28% and Don't know/Do not hold my info: 29%
Government	36%	Not likely: 35% and Don't know/Do not hold my info: 29%
Utilities	33%	Not likely: 37% and Don't know/Do not hold my info: 30%
Healthcare	30%	Not likely: 44% and Don't know/Do not hold my info: 26%
Airlines	29%	Not likely: 27% and Don't know/Do not hold my info: 44%
Banking	25%	Not likely: 48% and Don't know/Do not hold my info: 27%

Likely

Key Demographic Differences by Industry

Consumer responses were analyzed based on demographic segments gender, age and social class. Age categories were 18-34, 35-49, 50-64 and 65+ and social classes are classified as Class A (highest), Class B, Class C, Class D and Class E (lowest).

Likelihood of a breach

Retail — **44%** — Threat of data breach is significantly high among Britons over age 50, and low on the part of adults classified in the lowest social class (37 percent).

Telcom — **43%** — Data security concerns are significantly high among adults over the age of 50 (50 percent).

Government — **36%** — The perceived vulnerability levels rise with age, from 28 percent for young adults to 51 percent of seniors. Among social classes, concern levels are relatively high in Class D.

Utilities — **33%** — Personal data security concern about utilities rises with age, from 22 percent for young adults to 41 percent for seniors.

Healthcare — **30%** — Seniors (46 percent) are significantly more concerned about personal data security in healthcare organizations.

Airlines — **29%** — Concern about data security in airlines is higher among men (32 percent) and seniors (39 percent), and lower on the part of respondents classified in the lowest social class (20 percent).

Banking & finance — **25%** — Data security concern about banks does not vary significantly across the different subgroups.

Detailed Findings: (2) Which do you think the use of video-equipped drones to monitor or police public spaces would do?

British respondents have mixed feelings – positive and negative – about drones. While 49 percent see them as helpful in combating antisocial behavior, 40 percent worry about their privacy being compromised. Improving personal safety (36 percent) is cited more often than drones putting the public in physical danger.

Expectations of drones

Help combat anti-social behavior	49%
Invade or compromise your privacy	40%
Improve personal safety	36%
Be a physical danger to the public	22%
None of these	13%

On balance, the positives appear to outweigh the negatives.

Key Demographic Differences

Help combat anti-social behavior	Expectations of drones helping to combat anti-social behavior rise with age, from 33 percent of young adults to 61 percent of seniors
Compromise of Privacy	Seniors (34 percent) have lowest levels of concern about drones compromising privacy
Improve personal safety	Seniors are more likely to expect drones to improve personal safety (42 percent)
Physical danger to public	Concern over physical danger is higher among men (24 percent), Britons age 50-64 (26 percent) and respondents in social classes A and B (29 and 26 percent respectively)

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 U.K. is based on online surveys carried out over April 22-23, 2015. The survey has been conducted as follows:

- 2,006 completed interviews among nationally representative adults, 18 and above.

- The survey is conducted in English.

- The data from this survey are weighted to ensure projectability of the data to British adults.

Percentages are based on the full sample of 2,006. 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