How consumers in the Netherlands feel about:

- Personal data security, ranked by industry
- Safety and effectiveness of username and password on online platforms
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) Adequacy of Password Protection 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 its customers in Netherlands. 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 to make more informed security decisions. The research is conducted by leading market research company Lieberman Research Group.

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

- Personal data security, ranked by industry
- Safety and effectiveness of username and password on online platforms

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 the government, with 69 percent of those surveyed expecting a data breach within the next 12 months. Airline and transportation companies were perceived to be the least at risk with just 41 percent of respondents expecting consumer data to be compromised in some way.

Username and password security as a safety measure for online platforms are seen as inadequate by 22 percent of respondents. A third (34 percent), view it as an adequate approach to safety for social media with a majority considering it as sufficient protection for accessing government services (71 percent).

These findings serve as a reminder for businesses and institutions in the Netherlands 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 Dutch public lack confidence in the government and telecommunications companies when it comes to protecting personal data

The results of Unisys’ Security Insights 2015 indicates that consumers in the Netherlands lack confidence in the government and telecoms companies when it comes to protecting personal data, with 69 and 68 percent of respondents expecting a data breach in these sectors in the next 12 months. At the other end of the scale, the perceived threat of a data breach is at its lowest for airlines and retailers (41 and 50 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.

Dutch skeptical about adequacy of username/password approach to protecting data

As part of the Unisys Security Insights research, consumers were also asked about their concerns in relation to passwords and usernames for online platforms. The research revealed that the majority view it as sufficient protection when accessing government services and performing online or banking transactions (71 and 50 percent), consumers are not confident of this approach for social media access and email protection (34 and 23 percent respectively).

In today’s hyper-connected world, people are wary of losing valuable data and assets to cybercrimes and want assurances that their personal data is safe. Organisations must look to innovate and evaluate advanced security measures to help consumers migrate to stronger authentication techniques.
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 Dutch adults, with more than two thirds expecting a data breach in government agencies and telecommunications companies in the next 12 months (69 & 68 percent respectively).

<table>
<thead>
<tr>
<th>Organization</th>
<th>Likely</th>
<th>Not likely</th>
<th>Don't know/Do not hold my info</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government</td>
<td>69%</td>
<td>28%</td>
<td>3%</td>
</tr>
<tr>
<td>Telecom</td>
<td>68%</td>
<td>25%</td>
<td>7%</td>
</tr>
<tr>
<td>Banking &amp; finance</td>
<td>63%</td>
<td>32%</td>
<td>5%</td>
</tr>
<tr>
<td>Utilities</td>
<td>62%</td>
<td>32%</td>
<td>6%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>59%</td>
<td>36%</td>
<td>5%</td>
</tr>
<tr>
<td>Retail</td>
<td>50%</td>
<td>38%</td>
<td>12%</td>
</tr>
<tr>
<td>Airlines</td>
<td>41%</td>
<td>45%</td>
<td>14%</td>
</tr>
</tbody>
</table>
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 income groups segmented as high, medium and low.

- **Government**: 69% - Concern about data breach is significantly high among Dutch adults aged 25-34 (81 percent) and lowest among young adults 18-24 (58 percent)
- **Telecom**: 68% - Data security concern in telecom companies does not vary significantly across the different subgroups
- **Banking & finance**: 63% - Data security concern in banks does not vary significantly across the different subgroups
- **Utilities**: 62% - Data security concern in utilities does not vary significantly across the different subgroups
- **Healthcare**: 59% - Perceived vulnerability is low among Dutch adults in the age group 35-49 (51 percent)
- **Retail**: 50% - Data security concern in retail does not vary significantly across the different subgroups
- **Airlines**: 41% - Data security concern in airlines does not vary significantly across the different subgroups
Detailed Findings: (2) Access to online services is usually protected with a username and a password. Are a username and password sufficient protection for the following?

A majority of Dutch adults view the standard username/password approach to be sufficient in protecting information on online platforms, with only a quarter skeptical about it.

<table>
<thead>
<tr>
<th>Access Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government services for which you have to log in, such as DigiD</td>
<td>71%</td>
</tr>
<tr>
<td>Online or mobile banking</td>
<td>50%</td>
</tr>
<tr>
<td>Social media</td>
<td>34%</td>
</tr>
<tr>
<td>Your email</td>
<td>23%</td>
</tr>
<tr>
<td>None of these</td>
<td>22%</td>
</tr>
</tbody>
</table>

**Key Demographic Differences**

<table>
<thead>
<tr>
<th>Access Type</th>
<th>Observation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government services</td>
<td>Concerns do not vary significantly across the different subgroups</td>
</tr>
<tr>
<td>Online or mobile banking</td>
<td>Concerns do not vary significantly across the different subgroups</td>
</tr>
<tr>
<td>Social media</td>
<td>Confidence in username/password protection for social media drops with age, from 45 percent for young adults to 28 percent for seniors</td>
</tr>
<tr>
<td>Personal email</td>
<td>Confidence drops with age, from 34 percent for young adults to 17 percent for seniors</td>
</tr>
<tr>
<td>No application sufficient</td>
<td>Skepticism is lowest among young adults (8 percent)</td>
</tr>
</tbody>
</table>
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](http://www.unisys.com/security)
Polling Methodology

The Unisys Security Insights research in the Netherlands is based on telephonic interviews carried out in May 11-22, 2015. The survey has been conducted as follows:

• 509 completed interviews among nationally representative adults, 18 and above.
• The survey was conducted in Dutch
• The data from this survey are weighted to ensure projectability of the data to Dutch adults.

Percentages are based on the full sample of 509. 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.