2017

Unisys Security Index™

BELGIUM

Supplemental Research

Belgians Largely Support Sharing Personal Data with Police and Healthcare Providers but not if it Means Losing Control of Personal Data

Belgian consumers support Internet of Things technology to promote safety and convenience but do not want to be monitored continuously

UNISYS | Securing Your Tomorrow™

Executive Summary

As part of the Unisys Security Index™, Unisys has surveyed Belgian consumers on topical security issues and trends. This time the company asked them about their views on sharing, collecting and analysing personal data via a range of technologies and circumstances common in today's highly connected world.

The Internet of Things (IoT) phenomenon features "smart" devices, sensors and computer systems that can connect and exchange information with one another using the internet. Greater affordability and less cumbersome or intrusive designs have helped IoT become mainstream: from fitness trackers and smartwatches to smart medical devices and location tracking tags. As a result, Belgians are becoming increasingly connected.

This study examines Belgian consumer reaction to the trend. Within that context, the Unisys Security Index seeks to balance commercial and government organisations' appetite for harnessing the data available via IoT with the Belgian public's willingness to share such data. The findings reveal that Belgians' support for IoT varies widely depending on what, why and by whom the data is collected, how it is used and whether individuals can control when and if their data is shared with external third parties.

Belgians support sharing personal data with police or healthcare providers via smart devices, but enthusiasm varies depending on why and by whom the data is collected and how it is to be used

The Unisys Security Index: 10 Years and Counting

Unisys has conducted the Unisys Security Index – the only recurring snapshot of security concerns conducted globally – since 2007 in order to provide an ongoing, statistically-robust measure of concern about security. The index is a calculated score out of 300 covering changing consumer attitudes over time across eight areas of security in four categories: national security and disaster/epidemic, in the National Security category; bankcard fraud and financial obligations, in the Financial Security category; viruses/hacking and online transactions, in the Internet Security category; and identity theft and personal safety, in the Personal Security category.

The 2017 Unisys Security Index is based on online surveys conducted between April 6-18, 2017 of nationally representative samples of at least 1,000 adults in each of the following countries: Argentina, Australia, Belgium, Brazil, Colombia, Germany, Malaysia, Mexico, Netherlands, New Zealand, Philippines, the U.S. and the U.K. The margin of error at a country level is +/-3.1 percent at 95 percent confidence level, and 0.9 percent at a global level.

The follow up findings looking at the IoT were gathered from a global supplementary question fielded in all countries. The question was:

Today many objects, devices and computer systems can connect and exchange information with each other using the Internet. This information may potentially be available to others.

For more information on the 2017 Unisys Security Index, visit: www.unisys.com/unisys-security-index.

Download the full report of Belgium results: http://www.unisys.com/unisys-security-index/belgium.

NATIONAL SECURITY	NATIONAL SECURITY	Your Country's national security in relation to war or terrorism
	DISASTER/ EPIDEMIC	A serious natural disaster occurring in your country
FINANCIAL SECURITY	BANKCARD FRAUD	Other people obtaining and using your credit or debit card details
	FINANCIAL OBLIGATIONS	Your ability to meet your essential financial obligations
INTERNET SECURITY	VIRUSES/ HACKING	Computer and Internet security in relation to viruses, unsolicited emails or hacking
	ONLINE TRANSACTIONS	The security of shopping or banking online
PERSONAL SECURITY	IDENTITY THEFT	Unauthorized access to, or misuse of your personal information
	PERSONAL SAFETY	Your overall personal safety over the next 6 months

Belgians Selective About Supporting IoT

Today, countless connected objects, devices and computer systems can interact with and exchange information with one another using the Internet. On the face of it, this brings many benefits to our increasingly busy lives. The important thing to remember, however, is that this information may be made available to others without one's consent, raising questions about data security and privacy.

Estimates from companies like Cisco and Ericsson predict 50 billion internet-connected devices by 2020. And analyst firm CCS Insight expects 185 million smart wearable devices – including wristbands, eyewear, footwear and more – worth $16.9 billion to be sold by 2021. Simultaneously, companies and government agencies are seeking ways to harness the increasing amount of data available to make more informed decisions, as well as improve customer experience, using insights gained from data analytics – including data collected from IoT-related technology.

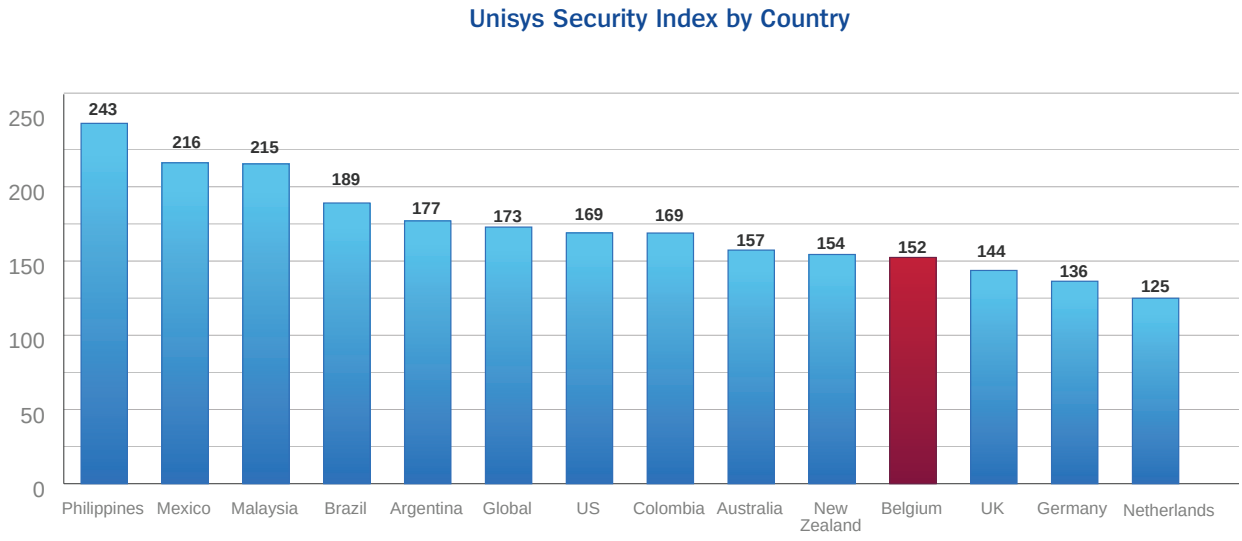
The 2017 Unisys Security Index findings revealed that, rather than having a homogenous response to the concept of IoT, Belgian consumers are selective about which instances of IoT they are comfortable with, highlighting a complex relationship between privacy, security and benefits such as convenience. Ultimately, consumers want control over what, where, when and with whom they share their data via IoT - and the right to decide if the reason is compelling enough or brings them any benefits.

The vast majority of Belgians, 8 out of 10, support using a button on their smartwatches to alert police to their location in case of emergency, whereas only 1 out of 4 support police being able to monitor fitness tracker data at any moment to determine their location at a certain time. There is also high support (73 percent of respondents) for medical devices such as pacemakers or blood sugar sensors being able to immediately transmit any significant changes to a patient's doctor and for sensors in luggage that communicate with an airport's baggage management system and an app on mobile phones to tell travelers if their luggage has been unloaded and what carousel it will be on (59 percent).

Yet only about one in five people support using a smartwatch app from a bank or credit card company to make payments (21 percent), or a health insurer accessing fitness tracker data to determine a premium or reward customers for good behaviour (19 percent).

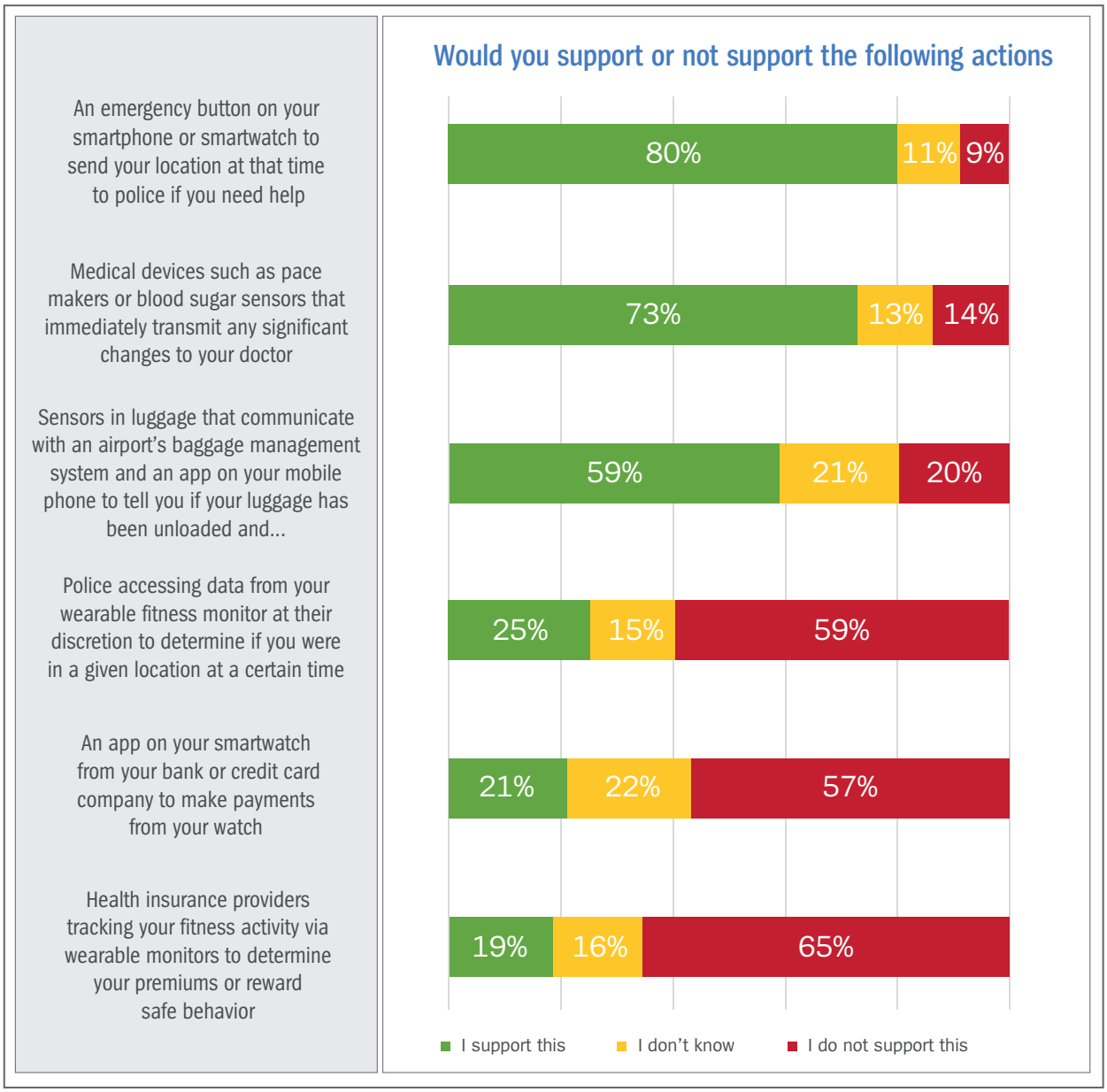
Households with lower incomes are generally more concerned about their security and safety. People aged 18-34 years have higher support for all scenarios than those aged 35 years or older.

Security concerns highest in developing markets



Key Barriers to Belgian IoT Usage

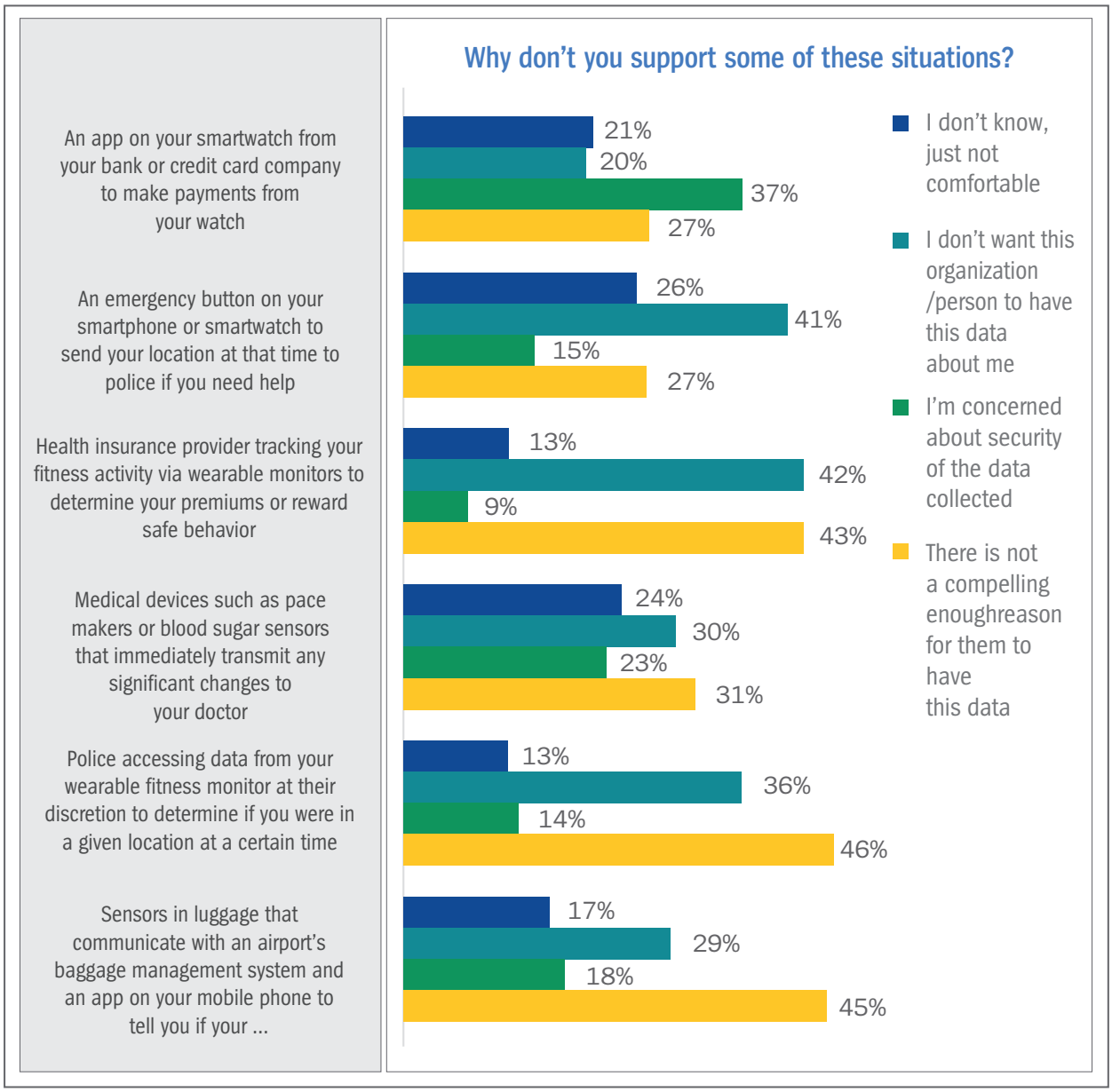
More appetite for emergency help apps that are triggered manually or automatically by the userLess support for tracking and monitoring apps.



The most common reasons given by Belgians for not supporting these IoT scenarios are that there is not a compelling enough reason to share their data or that they do not want organisations to have such data about them. However, the biggest barrier cited for not supporting a smartwatch payment app is concern about the security of data collected.

"Belgians welcome the smart help and support of the Internet of Things but not at the expense of losing control. Belgians want to decide on their own whether to share personal data or not," explains Rudolf de Schipper, Senior Project Manager at Unisys Belgium. "For the IoT to succeed, governments, healthcare organisations, financial institutions and other enterprises must take steps to assure the public that personal data collected from IoT devices will be secure and that privacy will be protected."

Sharing personal data with third parties is a main security concern, particularly if there is no compelling reason to share dataAlthough if money is involved, data security is the biggest concern.



Alleviating Consumer Concern through the General Data Protection Regulation

In recent years, the integration of social and economic elements and the overlapping of private, public and business domains have led to an increased flow of personal data. At the same time, the exchange of personal data between the public and private sector, rapid technological developments and globalization have brought new challenges to the protection of this data.

These challenges demanded a new data protection framework in the European Union. This framework, called General Data Protection Regulation (GDPR), was agreed to in April 2016 and will apply from 25 May 2018.

The GDPR focuses on strong enforcement of compliance requirements stressing the importance of creating trust to allow the digital economy to grow inside the European Community. The GDPR brings consistency to the current data protection laws across EU member states, and provides guidance on how customer data should be stored and how companies must respond in the event of a data breach.

The GDPR introduces new regulatory requirements for how institutions must manage the personal data they hold on their customers, including the segregation, obfuscation and encryption of data. GDPR requires businesses to implement security controls to address the risk presented by personal data processing, such as accidental or unlawful destruction, loss, alteration and unauthorized disclosure.

Organizations will be expected to demonstrate compliance at every stage of personal data processing, with potential heavy fines being levied by regulators on top of the high costs of dealing with data breaches. The GDPR imposes financial penalties on businesses for not protecting data, including fines of up to four percent of global revenue for the previous year, or €20 million – whichever is greater. Cloud providers and other data processors will be directly liable as the GDPR sets direct security obligations such as confidentiality, integrity, availability, resilience, business continuity and regular testing and evaluation.

In conjunction with the heavy fines, the GDPR has mandatory data breach reporting requirements. With the traditional challenges posed by data breaches and cybercrimes, businesses that collect, use and share data from European citizens must take adequate measures to ensure security of personal data and provide assurance that they meet the requirements set in the GDPR. As a result, there has been speculation about the struggle smaller cloud providers and other data processors will face in order to keep up with the financial burden and red tape associated with GDPR.

The GDPR Articulates Four Key Requirements:

- Controllers and processors must know the locations of where personal data is stored. GDPR poses limits on the ability to transfer personal data outside the European Economic Area (EEA). When this is allowed, the transfer of personal data must comply with the data transfer rules of the GDPR.
- Companies whose core activities consist of processing personal data on a large scale must appoint a Data Protection Officer (DPO). The DPO's role is similar to that of a Compliance Officer and is expected to manage IT processes, data security (including dealing with cyber-attacks) and other critical business continuity issues relating to the holding and processing of personal and sensitive data.
- A Data Protection Impact Assessment to ensure overall compliance with the GDPR is required. This will involve identifying procedures, processes and technical controls such as encryption, network segmentation and data obfuscation.
- Personal data controllers and processors have to take adequate technical security measures to protect personal data from loss, alteration or unauthorized processing. GDPR requires protection by design as well as by default. This means that data protection safety measures must be considered from the earliest stage of development.

David Matthews, security industry director, Unisys EMEA, commented: "To meet these requirements, CISOs and CIOs should adopt new security paradigms, methods and technologies for the protection of personal data, because the GDPR will be the single most powerful force changing how businesses interact with their customers. For this reason, the GDPR is not only a compliance challenge but touches all aspects of an organization's value chain. Only if organizations plan their compliance strategies and review their personal data processing capabilities can the GDPR become an opportunity to streamline the value chain and identify new ways to provide customers with value-added services. To achieve these benefits, organizations need to heavily scrutinize their security postures and data protection policies as well as roles and responsibilities of key functions and the individuals within them."

"The Unisys Security Index shows how much value consumers put in their personal data and that they are selective about how and where they share it. Sometimes though, being selective isn't enough and the organisations that you choose to interact with can suffer data breaches as a result of the latest threats challenging outmoded security principles. The GDPR will provide such organisations with steps to take to safeguard themselves and their customers' data to ensure the risks are understood and that best practices in policy and technology use are being implemented."

- David Matthews,
Security industry director, Unisys EMEA

The Unisys Call to Action

When developing an IoT or data analytics strategy, Unisys believes that organizations need to consider the consumer's point of view on five key factors:

1. **Compelling purpose: What's in it for me?** – Is it a strong enough reason for consumers to want to give up some of their privacy?

2. **Trust: Do I want this organization to have this information about me?** – Will consumers be concerned that information will be used for a purpose other than that for which it was originally intended?

3. **Protection: Will my data be secure?** – Use technology, processes and policies to prevent security breaches, and minimize their impact should they happen. Then communicate these measures to reassure customers of the steps taken to protect them and their data.

4. **Control: Can I decide when and if I share my data?** – Consumers are more comfortable when they can choose if they share their data at a specific time, rather than granting unrestricted access.

5. **Just because you can, should you?** – Understand that public acceptance of IoT involves a complex mix of technology capability, human attitudes, cultural norms and ethics.

"Businesses and government agencies are striving to find new and innovative ways to stay in touch with their clients and constituents, and many are exploring the possibilities presented by the Internet of Things and particularly emerging technologies such as wearable devices," said Michelle Beistle, chief privacy officer at Unisys. "At the same time, consumers are getting more and more concerned about the privacy and security of their data. So any organization that wants to leverage these new channels must convince their clients or customers that they will keep their personal data private and secure. It is imperative that organizations openly disclose how they will use the data and assure clients that they will keep their data secure at all times, that it will not be used for any purposes other than those dis-closed and how that data will be secured. Organizations that can clearly address the points highlighted above will have a greater chance of connecting with their clients."

Conclusion

The IoT trend has only just begun. The wealth of data being generated by personal and workplace applications will only continue to grow. However, collecting and analyzing that data involves a complex relationship between technology and the human factors of trust, acceptable purpose and willingness to give up privacy. Commercial and government organizations looking to tap into IoT and data analytics must do so in the context of these human factors.

For more information on Unisys security offerings, visit: www.unisys.com/security

About Unisys

Unisys is a global information technology company that specializes in providing industry-focused solutions integrated with leading-edge security to clients in the government, financial services and commercial markets. Unisys offerings include security solutions, advanced data analytics, cloud and infrastructure services, application services and application and server software.

For more information, visit: www.unisys.com

About the Unisys Security Index

Unisys has conducted the Unisys Security Index – the only recurring snapshot of security concerns conducted globally – since 2007 in order to provide an ongoing, statistically-robust measure of concern about security. The index is a calculated score covering changing consumer attitudes over time across multiple areas of security in four categories: National Security, Financial Security, Internet Security and Personal Security.

For more information on the 2017 Unisys Security Index, visit: www.unisys.com/unisys-security-index/belgium

08/17 17-0453