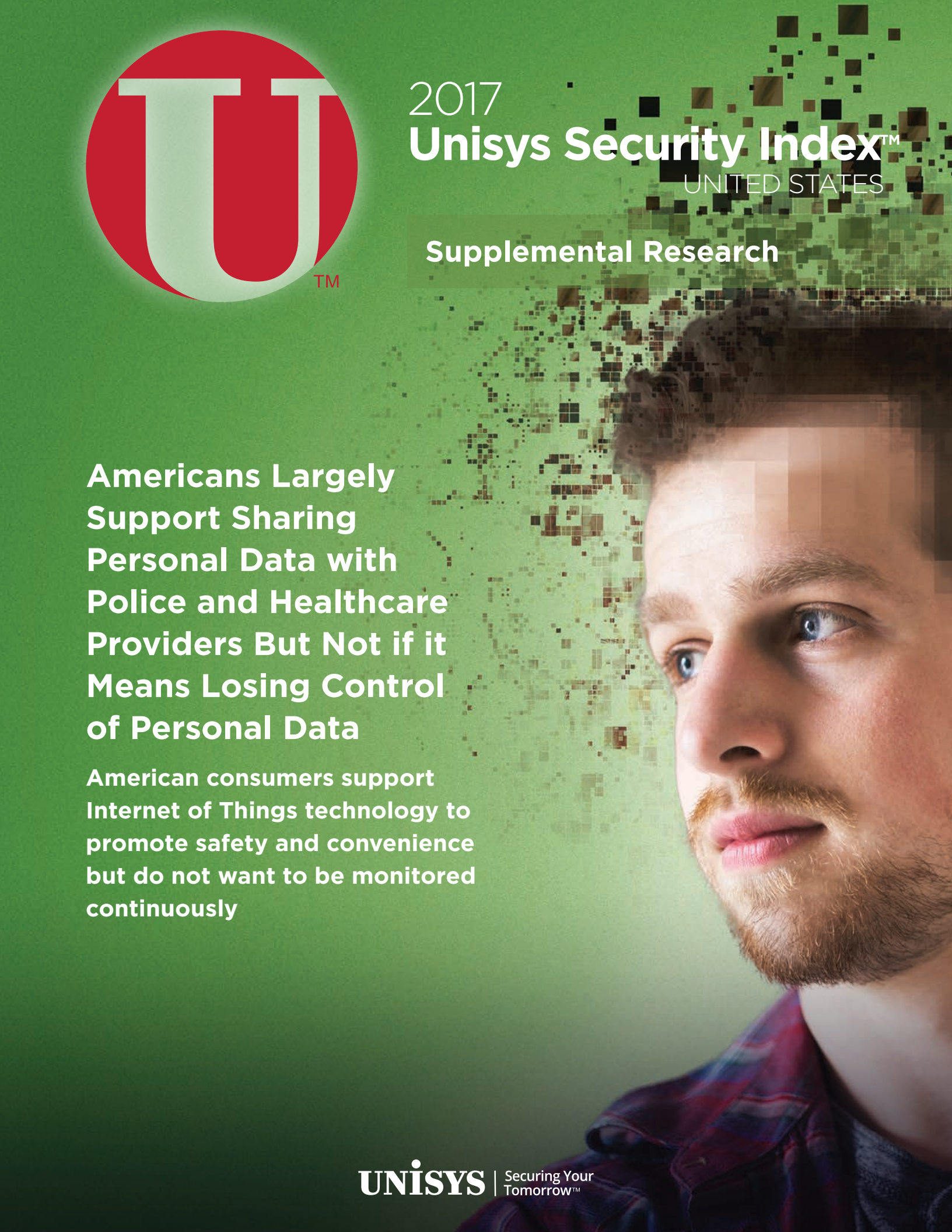
2017

Unisys Security Index™

UNITED STATES

Supplemental Research



Americans Largely Support Sharing Personal Data with Police and Healthcare Providers But Not if it Means Losing Control of Personal Data

American 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

The Unisys Security Index™ found divergent views among American consumers relative to the Internet of Things (IoT) phenomenon, in which smart devices, sensors or computer systems connect and exchange information with one another using the internet. The survey found general support for the security and convenience benefits of IoT, but also some wariness about how these applications will use their personal data, who will be able to access it and how it will be used.

Support for IoT was most apparent when consumers were presented with a number of "Safe Cities" scenarios, in which IoT technology is introduced into urban environments to promote safety and security. Consumers registered strong support for applications such as sensors in cities to detect the presence of harmful chemicals or radiation as well as surveillance systems that can automatically detect suspicious behavior and notify the police.

Likewise, the survey found significant support for the use of internet-connected medical devices that can detect health issues and automatically notify care providers of potential emergencies.

But this enthusiasm was tempered by substantial concerns about privacy and security – especially where issues like financial applications involving banks and personal data involving medical records are concerned. The Unisys Security Index results make it clear that public and private sector organizations must takes steps to address these concerns by assuring the privacy and security of personal data that traverses the IoT.

Americans 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

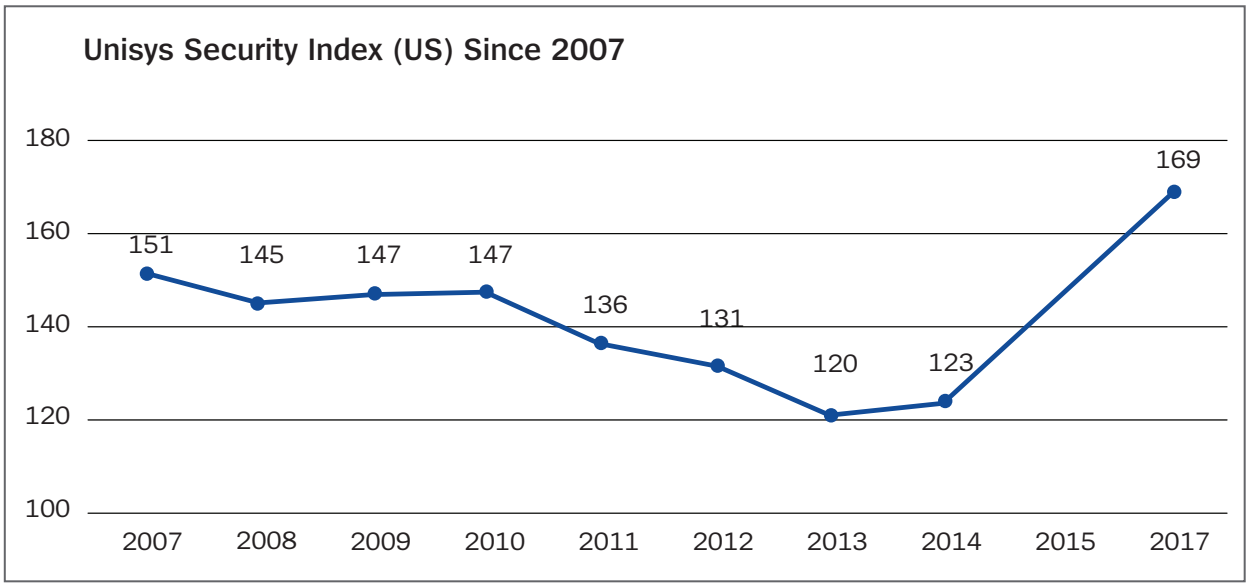
Unisys Corporation (NYSE: UIS) launched the Unisys Security Index – the only recurring snapshot of security concerns conducted globally – in 2007 to provide an ongoing, statistically-robust measure of concern about a nation's sense of security. The index is a calculated score out of 300 covering changing consumer attitudes over time across eight areas of security in four categories:

NATIONAL SECURITY	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
	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

Unisys Security Index (US) Since 2007

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 UK and the U.S. In all countries, the sample is weighted with respect to national demographic characteristics such as gender, age and region. The margin of error (with a 95 percent confidence level) is +/-3.1 percent at a country level and 0.9 percent at a global level. The 2017 Unisys Security Index was conducted by research firm Reputation Leaders.

In 2017 the overall Unisys Security Index for the U.S. is 169 out of 300, a substantial increase from 123 recorded in the last survey in 2014, and the highest level of concern since the research was first conducted in 2007. For more details refer to: www.unisys.com/unisys-security-index/us.



Divergent Views on IoT

As part of the Unisys Security Index, Unisys regularly surveys Americans on topical security issues and trends. This time the company asked American consumers about their views on sharing, collecting and analyzing personal data via a range of technologies and circumstances common in today's highly-connected world.

The IoT phenomenon features "smart" devices, sensors or 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 sensors deployed in U.S. cities to make citizens safer. This study examines American consumer reaction to this trend.

Estimates from companies like Cisco and Ericsson predict 50 billion internet-connected devices by 2020. And analyst firm CSS Insight expects 185 million smart wearable devices 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.

Analysts expect "smart cities" initiatives – and their law enforcement equivalents known as "safe cities" – to drive IoT growth. These initiatives use IoT devices such as connected sensors to collect and analyze data to enable local governments to improve infrastructure and public services. For example, New York City has tested sensors that detect gunshots in police precincts in Brooklyn and the Bronx, and has experimented with a connected car program designed to improve roads by using sensors to detect locations where drivers make frequent hard brakes or sharp turns because of traffic. And the City of San Diego uses cameras and connected streetlights to monitor pedestrian traffic and reroute automobile traffic to avoid pedestrian accidents.

Americans Generally Support IoT

The Unisys Security Index findings reveal that U.S. consumers' support for sharing personal data via smart devices varies widely depending on why and by whom the data is collected, how it is to be used and whether the individual can control when and if the data is shared.

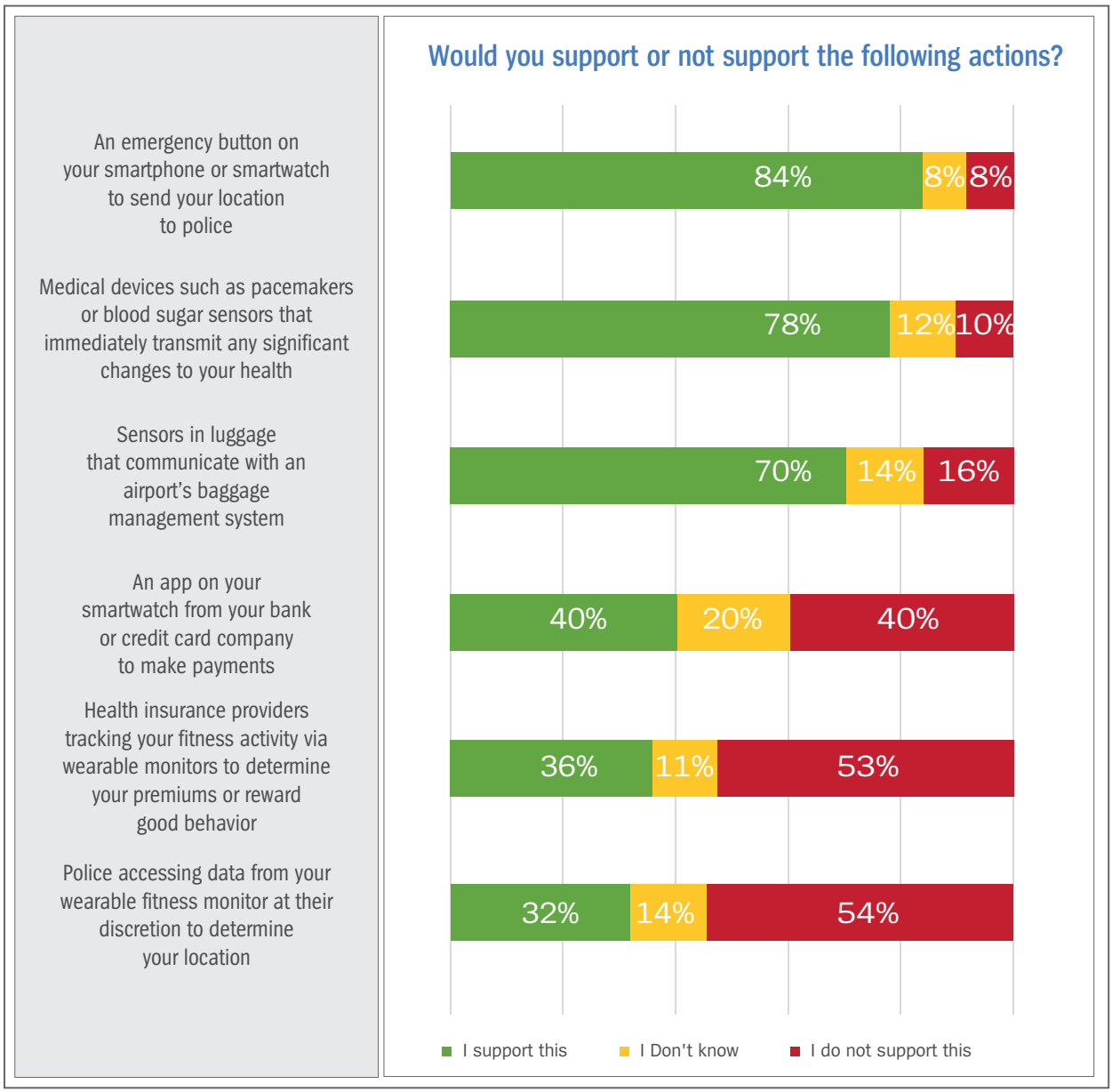
The survey highlights a complex relationship between privacy, security and benefits such as convenience. Ultimately, consumers want control over what, where, when and with whom they share their data via IoT – and the right to decide if the reason for the data to be shared is compelling enough.

The survey also identified differences in attitudes among consumers based on whether organizations that collect data via the IoT are sharing, retaining or simply using their personal data.

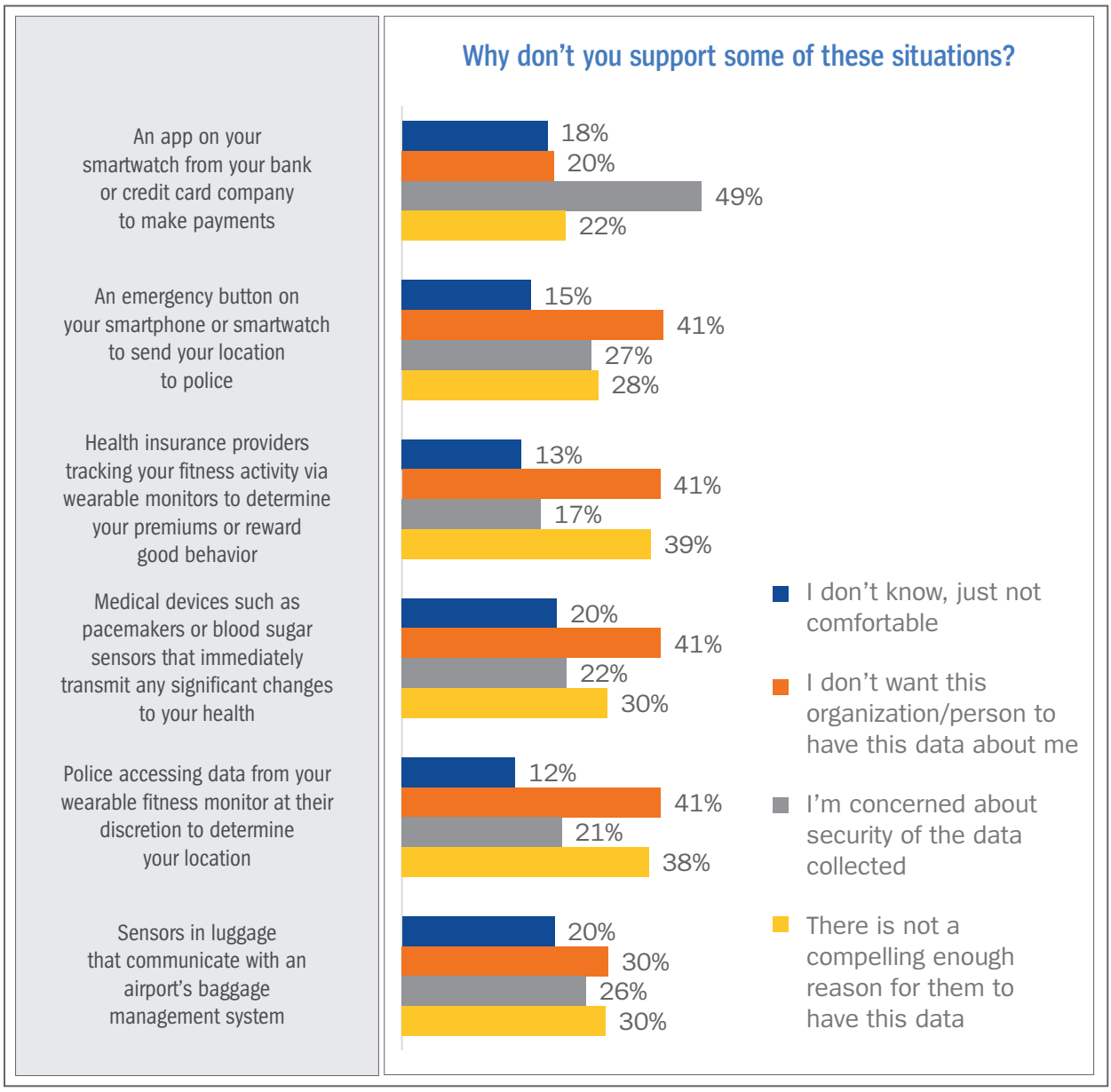
When it comes to data usage, the Unisys Security Index shows that consumers generally accept use cases in which their personal data may help to increase their personal safety or health or those that promote general convenience. But they are uneasy about sharing personal data via the IoT that is used in relation to money matters such as banking and qualifying for different insurance rates.

For IoT applications that involve data retention and sharing, consumers express even greater levels of concern about sharing personal information, especially when it comes to their financial lives.

When do Americans support data collected via IoT?



Reasons Americans Don't Support IoT



Broad Support for IoT Related to Personal Safety

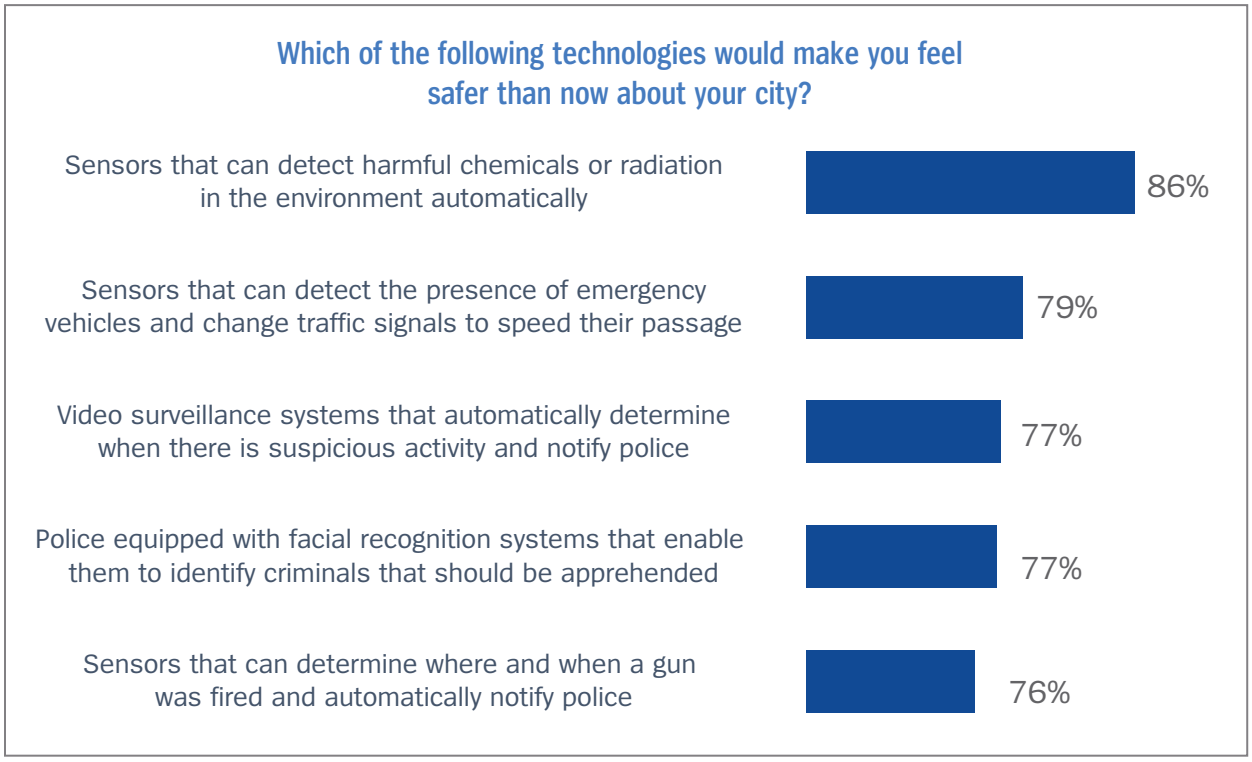
Americans largely support IoT applications that promote public safety, as long as they do not impact their sense of privacy. For example, the vast majority of Americans (84 percent) said they support using a button on their smartwatches to alert police to their location in an emergency, whereas only 32 percent support police being able to monitor fitness tracker data anytime to determine if someone was in a given location at a certain time.

The study also looked at the levels of support among consumers for IoT technologies used by law enforcement – deployed under the auspices of Safe Cities initiatives – to promote safety and security in U.S. urban environments. The results showed a broad support for a variety of Safe Cities use cases.

The Unisys Security Index presented five Safe Cities scenarios to respondents and asked if deployment of IoT technology in each instance would make them feel safer. Scenarios included deployment of: sensors to detect harmful chemicals or radiation in the urban environment; sensors to detect the presence of emergency vehicles and automatically change traffic signals accordingly; video surveillance systems to detect suspicious behavior and automatically notify police; police equipped with facial recognition systems to help identify criminals who should be apprehended; and sensors that can detect gun shots and automatically notify police.

In all five cases, more than three-quarters of respondents said the technology would make them feel safer (see graph below).

"When it comes to ensuring their physical safety, the survey shows that Americans largely support the use of Internet of Things technology in their public and personal lives," said Bill Searcy, vice president, Justice, Law Enforcement and Border Security at Unisys and a former deputy assistant director at the FBI. "Law enforcement agencies may view these findings as a green light to proceed with Internet of Things projects that will enhance the safety of their constituents, but they should do so with an eye on protecting the privacy and the data of those they serve."

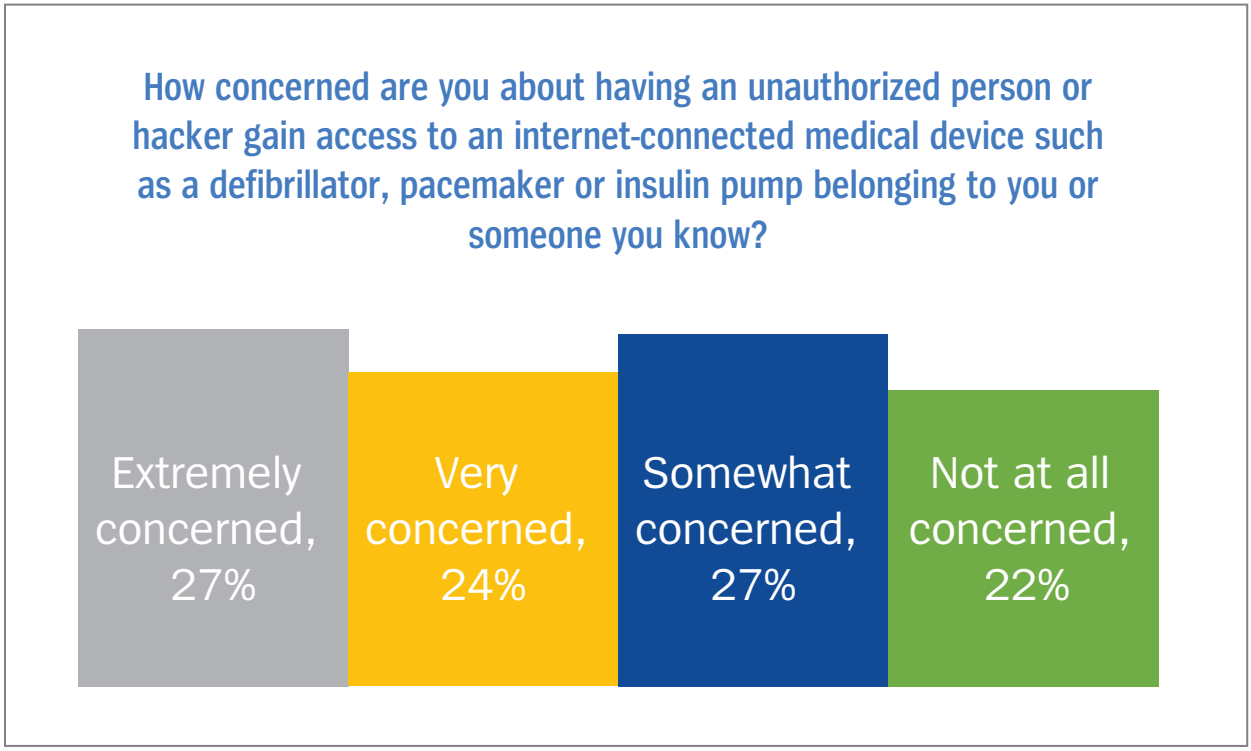


Strong Support for IoT Related to Personal Health – Within Limits

As with IoT applications related to personal safety, Americans generally support applications related to personal health – but also within limits. The survey found that U.S. consumers registered high support (78 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. But only about one in three Americans (36 percent) support technology to allow health insurance providers to access fitness tracker data to determine a premium or reward customers for good behavior.

The survey indicated that consumers' reluctance to share their medical data may reflect general concern about maintaining the safety and security of not only personal data, but personal medical devices as well. Asked about their level of concern about someone gaining unauthorized access to an internet-connected medical device such as a defibrillator, pacemaker or insulin pump belonging to them or someone they know, more than half of Americans (51 percent) said they were extremely or very concerned. An additional 27 percent said they were somewhat concerned.

Jeff R. Livingstone, PhD, Vice President and Global Head, Life Sciences and Healthcare, Unisys, sees issues playing out in the healthcare industry similar to those already present in public safety organizations. "There is great potential for the healthcare industry to benefit from IoT, but consumers have reason to remain wary," Livingstone said. "For example, there is a major risk contrast between a health insurance company collecting information about member behavior and a doctor monitoring a patient's critical medical data. This remains true despite any direct or indirect advantage to the member or patient. As the number of smart medical devices grows – including those that are worn or even embedded in patient's bodies – healthcare providers will be challenged with efficiently tracking and managing devices away from their medical facilities and ensuring those devices are secure."



Cautious Support for IoT Related to Personal Finances

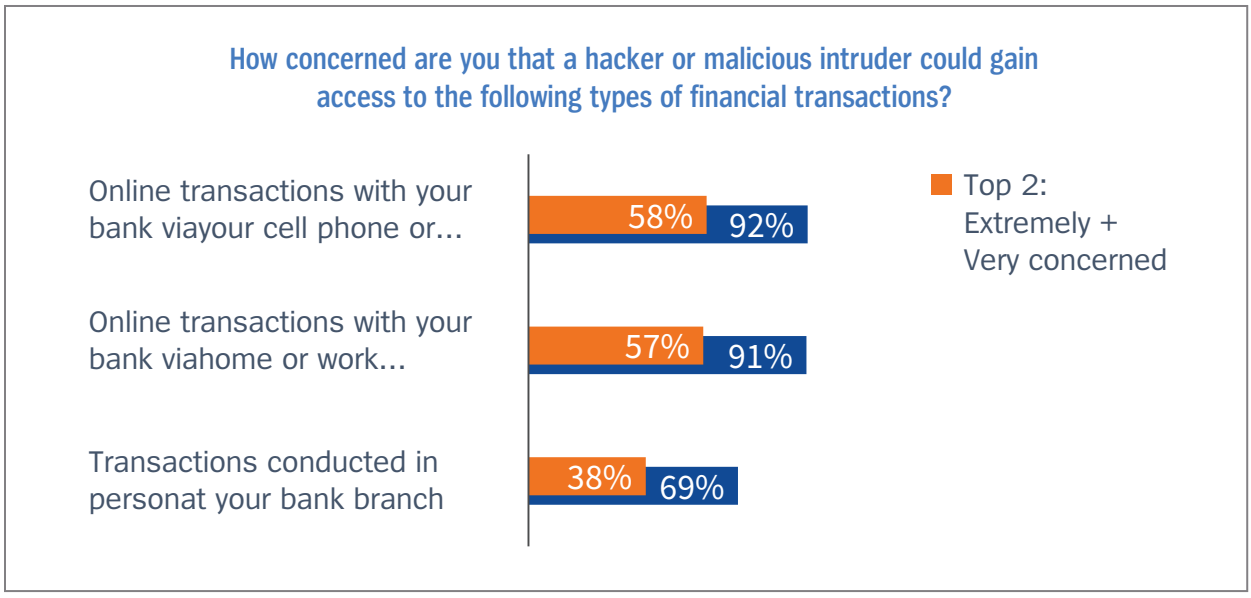
American consumers appeared somewhat more concerned about financial transaction using the IoT. For example, American respondents were divided on support for using a smartwatch app from a bank or credit card company to make payments, with 40 percent supportive and 40 percent against.

Concern about sharing financial data over the IoT was to a great extent driven by consumers' security concerns. Nearly half (49 percent) of those who did not support using a smartwatch app from a bank or credit card company to make payments said they were most worried about the security of those transactions.

When asked specifically about their concerns about hackers or malicious intruders gaining access to financial transactions made via internet-connected devices, more than 90 percent of U.S. respondents registered some level of concern about the security of transactions using a mobile device or computer – with nearly 60 percent reporting they are "very" or "extremely" concerned about the security of those transactions.

In contrast, 69 percent of Americans expressed some concern about the security of in-person transactions at their banks, with 38 percent "very" or "extremely" concerned.

"The Unisys Security Index results clearly tell us that consumers remained concerned about the security and privacy of banking via channels such as smartphones and smartwatches," said Eric Crabtree, global head of Unisys Financial Services. "Banks and other financial institutions can address consumer concerns around data security of smartwatch payment channels through a multi-pronged approach that addresses both policies and technology – such as the use of biometrics. These types of technological advances can more quickly and accurately determine whether a transaction is fraudulent, giving customers a greatest sense of security."



Enthusiasm for IoT Related to Personal Convenience

In addition to safety and health issues, Americans voiced support for IoT applications that promote convenience. For example, 70 percent of Americans registered support for sensors in luggage that communicate with an airport's baggage management system along with an app on their mobile phones to tell them if their luggage has been unloaded and what carousel it will be on.

Enterprises and government organizations looking to reach out to consumers via the IoT should emphasize these benefits with an eye on reasons consumers may be wary.

The Unisys Security Index found that most U.S. respondents who did not support some IoT applications reported that they simply did not want various organizations to obtain information about them. Also, many said they did not see a compelling need for the organizations to obtain the data.

"The Unisys Security Index survey results tell us that Americans want to obtain the convenience and security benefits of the Internet of Things, but not at the expense of losing control of their personal data," said Searcy. "For the IoT to succeed, governments, healthcare organizations, 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."

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. Communicate that your organization is in compliance with data privacy regulations such as PCI DSS for card payment information and HIPAA for medical records.
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 disclosed 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/us.

For more information visit www.unisys.com