

RISKS AND REWARDS OF CONNECTED DEVICES

THE HIDDEN INTERNET OF THINGS
ISACA 2015 IT RISK / REWARD BAROMETER



The Internet of Things paints a vision of a carefree, seamlessly connected world—where interconnected devices collect and share our most practical data to improve the functionality of products, the efficiency of homes and workplaces, the infrastructures of cities, and, fundamentally, the overall integration of our lives. But there are also hidden, or lesser-known, risks. These risks stand between consumers and the utopia where devices talk to each other in reliable and meaningful ways. ISACA’s 2015 IT Risk/Reward Barometer explores tradeoffs and recommendations that consumers and organizations must consider for their cyber lives.

THE INTERNET OF THINGS CYBER LANDSCAPE TODAY

Conversations about the Internet of Things (IoT) typically involve large figures: the estimated number of connected devices in use by the year 2020 (30 billion¹), connected vehicles projected to reach roadways in the next five years (one in five cars²), and the potential global economic impact the IoT could create by 2025 (up to US \$11 trillion³). These totals are indeed remarkable, and they offer consumers and organizations a sense of the tremendous scale at which connected devices are operating and growing.

Unlike many tech fads that fall out of public consciousness, the IoT is an evolution that deserves attention. By measuring, evaluating and sharing big data intelligently, these devices have an unprecedented potential to improve the way things work at an awe-inspiring level.

But there is much more to the IoT landscape than this broad, macro view. Within these large numbers live individual people, and to most users of such devices, it isn’t the billions or the trillions that matter—it’s the handful of connected items they carry with them and have in their homes and offices. They care about what these devices can do for them on a practical level: the information they collect, the aspects of their lives they can improve and the complicated tasks they can simplify. The job for manufacturers is to deliver on these promises while addressing privacy and security concerns.

30 BILLION

THE ESTIMATED NUMBER
OF CONNECTED DEVICES
IN USE BY THE YEAR 2020



And perhaps, in the worthy pursuit of making the IoT a ubiquitous reality, many manufacturers have left their connected devices vulnerable to hidden, or unexpected, risks. The rush for mass adoption may have come at the expense of thorough safeguards. And with so many devices collecting such vast amounts of data in such new ways, it's nearly impossible to fully prepare or account for every possible threat.

In the past few years, we have seen technology experts, white and black hat hackers, and security researchers point out weaknesses in all sorts of connected devices: thermostats, refrigerators, fitness trackers, insulin pumps, and most recently, automobiles. For a piece in *WIRED* magazine, two hackers went through the process of remotely taking over a Jeep while a journalist was driving it—controlling everything from the air conditioning and onscreen video to cutting the brakes and killing the engine—all while sitting comfortably in a living room miles away.

These are real threats, and compromised devices open the door to the much more serious problem of compromised personal information. Do consumers and IT professionals see eye to eye on the severity of these threats? And if so, are they doing their part to ensure that their data is as safe as it can be?

WITH SO MANY DEVICES COLLECTING SUCH VAST AMOUNTS OF DATA IN SUCH NEW WAYS, IT'S NEARLY IMPOSSIBLE TO FULLY PREPARE OR ACCOUNT FOR EVERY POSSIBLE THREAT.

EXPLORING RISKS AND REWARDS OF THE IoT EVOLUTION

The IT Risk/Reward Barometer examines attitudes and behaviors related to the risks and rewards of key technology trends, including the IoT and cybersecurity. The 2015 Barometer consists of two survey audiences:

- 7,016 ISACA members from 140 countries
- 5,396 consumers in five countries: Australia, India, Mexico, the United Kingdom and the United States.

HIGH AWARENESS AND OWNERSHIP OF IoT DEVICES

The vast majority of consumers say they are somewhat or very knowledgeable in identifying devices considered part of the IoT. This number ranges from 76 percent of UK consumers to 95 percent of consumers in India [UK: 76 percent, AU: 81 percent, US: 83 percent, MX: 91 percent; IN: 95 percent].

But perhaps consumers overestimate their knowledge about the state of connected devices. When asked how many IoT devices they thought were currently found in a typical household in their country, respondents, on average, indicated six to 14 [IN: 14, US: 9, MX: 8, AU: 7, UK: 6]. But when asked how many IoT devices they currently had in their own homes, the average answer was five to seven [IN: 7, MX: 7, AU: 6, UK: 5, US: 5]. Contrasting these two responses, many might see themselves as behind in their ownership of connected devices compared to their neighbors, as they don't appear to know how many connected devices are actually surrounding them.

Whatever their perception of the IoT, most consumers want more of it. The majority of consumers in countries surveyed now own some type of IoT device [MX: 93 percent, AU: 86 percent, IN: 84 percent, UK: 78 percent, US: 76 percent], with smart TVs, Internet-enabled cameras, connected cars and wireless fitness trackers leading the way across markets surveyed. Further, the vast majority in most countries surveyed would like to get some type of IoT device in the next 12 months, if they do not already have one [IN: 91 percent, MX: 88 percent, UK: 62 percent, US: 60 percent, AU: 59 percent]. Smart TVs, smart watches and wireless fitness trackers are among the most popular.

CONSUMERS WORRY ABOUT DATA SECURITY, BUT ALSO FEEL PREPARED TO PROTECT THEMSELVES

With increased ownership of connected devices comes increased vulnerability, a reality that most consumers realize—most are afraid that their IoT device[s] may be hacked [MX: 80 percent, IN: 76 percent, US: 65 percent, AU: 63 percent, UK: 63 percent]. These consumers are also well aware of the kinds of information that hackers may steal. Across all countries, credit card numbers, national identification numbers such as a social security numbers, passwords and personal emails were among the highest concerns.

<i>Top 5 Things Consumers Fear Will be Misused by a Cybercriminal</i>					
	Australia	India	Mexico	UK	US
1	Credit/debit card information [76%]	Credit/debit card information [80%]	Credit/debit card information [91%]	Credit/debit card information [71%]	Credit/debit card information [76%]
2	Passwords [70%]	Passwords [77%]	Passwords [88%]	Passwords [67%]	National ID number [72%]
3	Personal emails [51%]	Personal emails [70%]	National ID number [78%]	National ID number [54%]	Passwords [68%]
4	National ID number [51%]	National ID number [69%]	Personal photographs [76%]	Personal emails [52%]	Personal emails [52%]
5	Social media usage [49%]	Personal photographs [69%]	Personal emails [74%]	Social media usage [42%]	Health records [51%]

However, the results also show that nearly the exact same percentage who fear hacking are confident that they can control the security on IoT devices they own, specifically who has access to their information [MX: 82 percent, IN: 81 percent, UK: 66 percent, AU: 65 percent, US: 64 percent]. Despite the slew of very public data breaches over the past few years, consumers appear to find themselves in a tension between healthy fear and stubborn optimism: aware of the risks, yet capable of dealing with them.

Globally, 94 percent of consumers believe that hacking into an Internet of Things device is burglary.

GLOBAL IT PROFESSIONALS LESS OPTIMISTIC ABOUT CONSUMER CYBER PREPAREDNESS

However, according to IT professionals, consumer confidence in the security of their connected devices is misguided. In ISACA's member survey, 63 percent of IT professionals are not confident that they can control who has access to their information collected by IoT devices at home — nearly the same percentage of consumers in the US, UK and Australia who say they are confident that they can.

What's more, rather than saying consumers have the power to protect themselves through proactive measures such as changing their passwords, 45 percent of IT professionals say the most important thing to do to keep their IoT data secure is simply to not store any sensitive or classified data on the devices at all, hardly a comforting thought for those who already do, or for those who own such devices that require personal information to fully function.

IT professionals also say that the device manufacturers should have a stronger role. Nearly three-quarters of IT professionals (72 percent) don't believe that device manufacturers are implementing sufficient security measures in IoT devices. Further, they feel that these manufacturers are failing to let people know what they are at risk to lose: 84 percent of IT professionals don't believe that device manufacturers make consumers sufficiently aware of the type of information the devices can/do collect.

ORGANIZATIONS ALSO VULNERABLE TO THE RISKS OF CONNECTED DEVICES

In the workplace, IoT devices can be a great boon for businesses. Seventy-seven percent of IT professionals say that the IoT has benefited their company, bringing things like greater accessibility to information (44 percent), greater efficiency (35 percent), improved services (34 percent), and increased productivity (25 percent).

But where the rewards are the greatest, so are the risks. Sixty-three percent of IT professionals believe that the IoT will result in decreased employee privacy. Also, 73 percent do not believe that security standards in the IT industry sufficiently address the IoT (and that updates are needed), and roughly half (49 percent) do not believe that their IT department is even aware of all of its organizations connected devices.

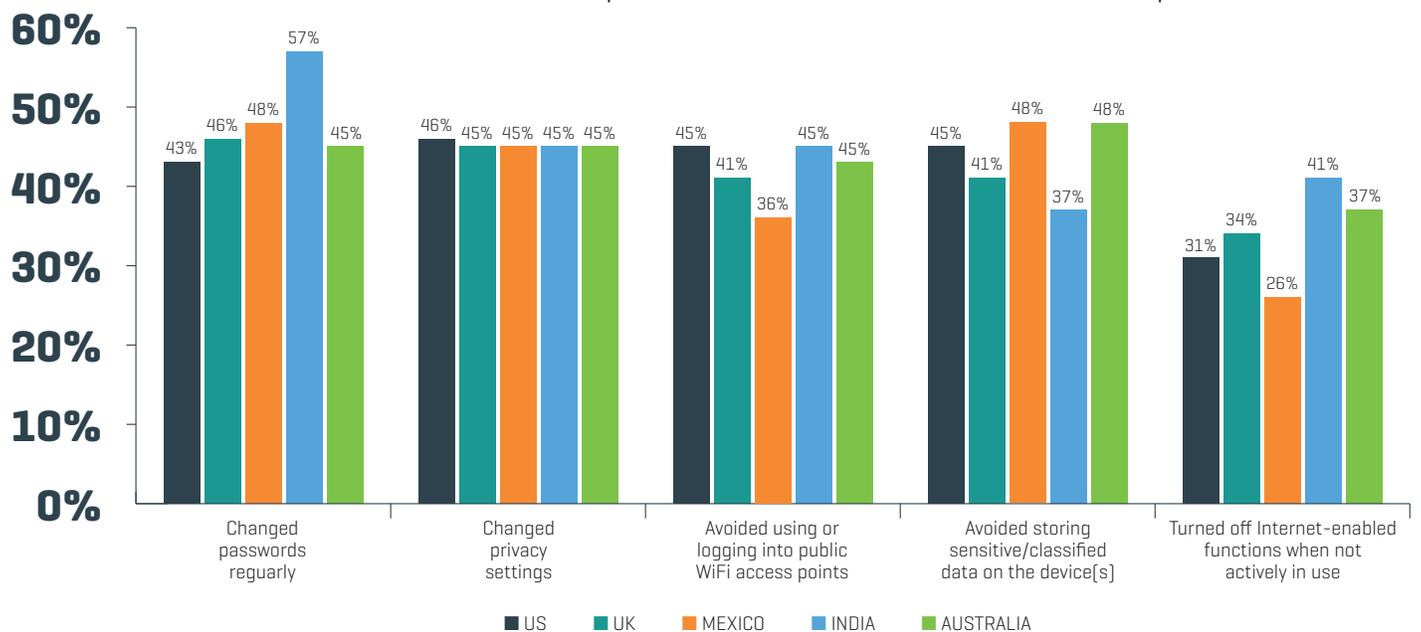
Further, 73 percent consider it a medium to high likelihood that a company will be hacked through an IoT device, and 61 percent say that enterprises of all sizes are equally vulnerable, from small businesses with 1-49 workers to large corporations with 500 employees or more. Data leakage is seen as the most significant enterprise security concern related to the IoT. But ultimately, organizations should not avoid new technology. The business risk of not embracing the Internet of Things — and falling behind competitors — may well outweigh any potential cost of a cyberattack.

**73
PERCENT
OF PEOPLE CONSIDER
IT A MEDIUM TO HIGH
RISK A COMPANY
WILL BE HACKED
VIA IoT DEVICE**

HOW CONSUMERS ARE PROTECTING THEMSELVES

Thankfully, consumers seem to be heeding some of these warnings. Nearly all have taken some type of proactive actions to keep their information private on the IoT devices they own. Approaches to protecting themselves include changing privacy settings, changing passwords regularly, avoiding public WiFi access points, and not storing sensitive data on their device. Fewer than 10 percent of consumers say they have not taken any proactive measures at all.

Actions taken to keep information on connected devices private



WHAT CONSUMERS WANT

The findings also suggest that consumers are likely to value businesses that can demonstrate their expertise in and commitment to cyber security best practices. The vast majority of consumers in countries surveyed say it is important that data security professionals hold a cyber security certification if they work at organizations with access to the consumers' personal information [MX: 98 percent, IN: 96 percent, AU: 93 percent, UK: 90 percent, US: 89 percent].

IMPLICATIONS FOR BUSINESS AND IT

Organizations and their IT departments need to adapt their strategies to account for the risk and reward represented by the Internet of Things. ISACA experts offer the following recommendations.

Ways for enterprises to maintain a cyber-secure workplace

- Safely embrace Internet of Things devices in the workplace to keep competitive advantage
- Ensure all workplace devices owned by organization are updated regularly with security upgrades.
- Require all devices be wirelessly connected through the workplace guest network, rather than internal network
- Provide cybersecurity training for all employees to demonstrate their awareness of best practices of cybersecurity and the different types of cyberattacks
- Ensure that IT and security professionals are CSX-certified

Manufacturers of IoT devices specifically should:

- Require all developers who build software to have appropriate performance-based cybersecurity certification, to ensure safe coding practices are being followed
- Insist all social media sharing be opt-in
- Encrypt all sensitive information, especially when connecting to Bluetooth-enabled devices
- Build Internet of Things devices that can be updated automatically with new security upgrades

RELATED RESOURCES

For full survey results, including related infographics, visit www.isaca.org/risk-reward-barometer.

Cybersecurity Nexus [CSX]: <https://cybersecurity.isaca.org>

COBIT framework for governance and management of enterprise IT: www.isaca.org/cobit

ISACA Knowledge Center: www.isaca.org/knowledge-center

ABOUT THE 2015 IT RISK/REWARD BAROMETER

The annual IT Risk/Reward Barometer is a global indicator of trust in information. Conducted by ISACA, a global association of more than 140,000 IT security, assurance, risk and governance professionals, the Barometer polls thousands of business and IT professionals and consumers worldwide to uncover attitudes and behaviors about essential technologies and information, and the trade-offs people make to balance risk and reward.

The study is based on online polling of 7,016 ISACA members among 140 countries from 27 August to 8 September 2015. Additional online surveys were fielded by M/A/R/C Research among 1,227 consumers in the US, 1,025 consumers in the UK, 1,060 consumers in Australia, 1,027 consumers in India and 1,057 consumers in Mexico. The US survey ran 17-20 August 2015, and the UK, Australia, India and Mexico surveys ran 21-30 August 2015. At a 95 percent confidence level, the margin of error for each individual country sample is +/- 3.1 percent. To see the full results, visit www.isaca.org/risk-reward-barometer.



ABOUT ISACA

ISACA® (isaca.org) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus™ [CSX], a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

 Follow ISACA on Twitter: <https://twitter.com/ISACANews>

 Join ISACA on LinkedIn: ISACA [Official], <http://linkd.in/ISACAOfficial>

 Like ISACA on Facebook: www.facebook.com/ISACAHQ

Contact: news@isaca.org

Additional Sources

- 1) McKinsey & Company, The Internet of Things: Sizing up the Opportunity, 2014
http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things_sizing_up_the_opportunity
- 2) McKinsey, The road to 2020 and beyond: What's driving the global automotive industry?, 2013
http://www.mckinsey.com/~media/mckinsey/dotcom/client_service/automotive%20and%20assembly/pdfs/mck_the_road_to_2020_and_beyond.ashx
- 3) McKinsey, Unlocking the Potential of the Internet of Things, 2015
http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world

