

Uncovering the potential of the Internet of Things

How the right cybersecurity and privacy safeguards can help businesses realize the promises of the IoT

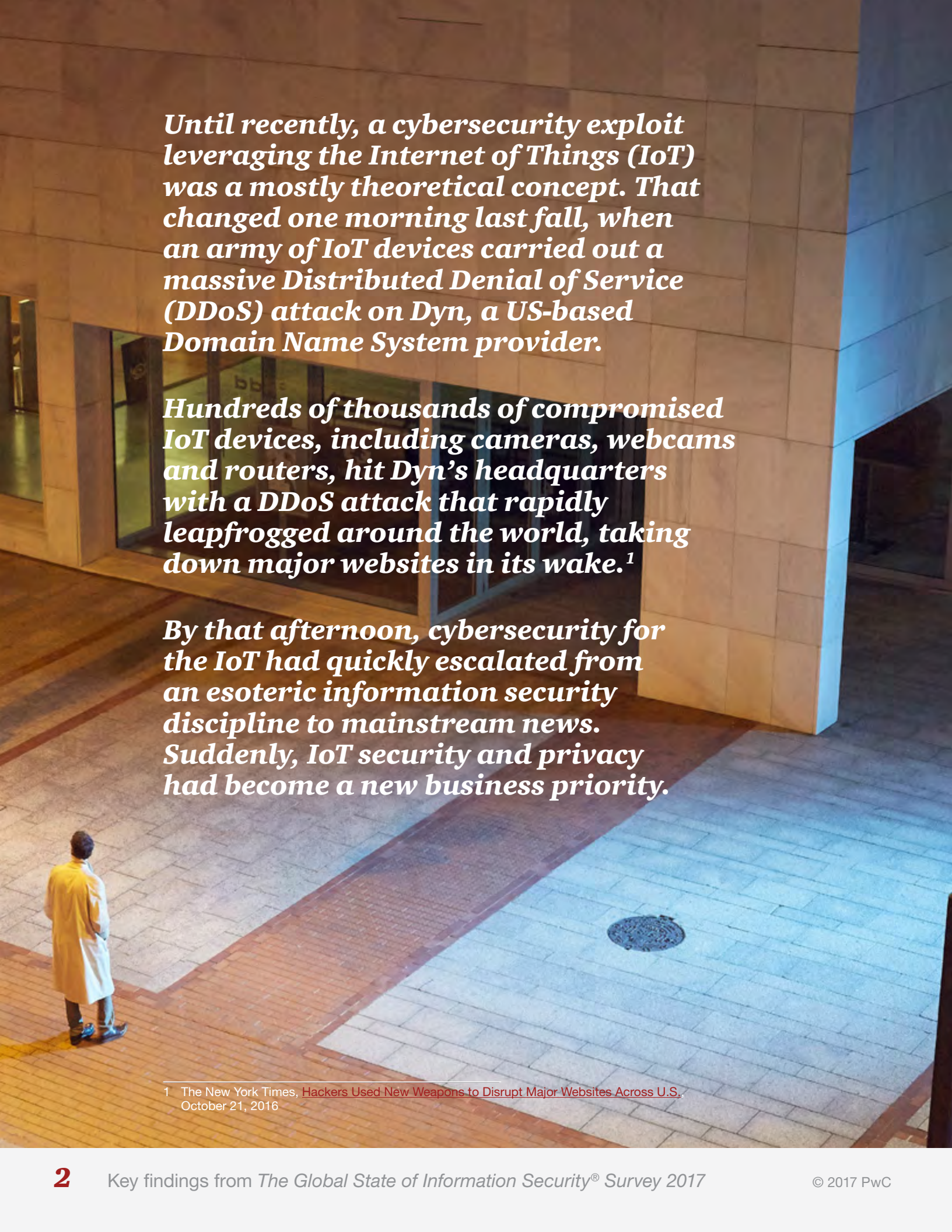


***Key findings from
The Global State of
Information Security®
Survey 2017***

A man in a dark jacket and blue jeans, carrying a brown bag, is walking from left to right in the foreground. He is walking past a large, modern building with a glass facade that reflects the sky and the surrounding environment. The building's structure is composed of many rectangular glass panels separated by dark frames. The overall scene is brightly lit, suggesting a sunny day.

Table of contents

Introduction	2
Competitive advantages of the IoT	7
It's complicated: Why security is a moving target	9
<i>Automakers are racing to secure the connected car</i>	<i>11</i>
<i>How devices are connecting patients to better healthcare.....</i>	<i>12</i>
The risks of too much information	13
Taking steps to build IoT cybersecurity.....	15
Leveraging existing technologies to integrate cybersecurity	19
People: The Achilles' heel of cybersecurity	21
Connecting the dots for the future	22
Methodology	23
Contacts	24



Until recently, a cybersecurity exploit leveraging the Internet of Things (IoT) was a mostly theoretical concept. That changed one morning last fall, when an army of IoT devices carried out a massive Distributed Denial of Service (DDoS) attack on Dyn, a US-based Domain Name System provider.

Hundreds of thousands of compromised IoT devices, including cameras, webcams and routers, hit Dyn's headquarters with a DDoS attack that rapidly leapfrogged around the world, taking down major websites in its wake.¹

By that afternoon, cybersecurity for the IoT had quickly escalated from an esoteric information security discipline to mainstream news. Suddenly, IoT security and privacy had become a new business priority.

¹ The New York Times, [Hackers Used New Weapons to Disrupt Major Websites Across U.S.](#), October 21, 2016

Risks of future compromises will very likely increase as connected devices proliferate. “Gartner, Inc. forecasts that 8.4 billion connected things will be in use worldwide in 2017, up 31 percent from 2016, and will reach 20.4 billion by 2020”.² Approximately one-quarter of respondents to The Global State of Information Security® Survey 2017 report exploits of IoT components like operational technologies (OT), embedded systems and consumer devices.

46%



Plan to invest in security for the Internet of Things this year

PwC, CIO and CSO, *The Global State of Information Security® Survey 2017*, October 5, 2016

As the IoT moves toward the core of digital business, the integration of security domains—IT, OT and consumer technologies—will likely introduce game-changing hazards. These potential risks include disruption in the information flow among connected

² Gartner Press Release, [Gartner Says 8.4 Billion Connected “Things” Will Be in Use in 2017, Up 31 Percent From 2016](#), February 7, 2017



devices, physical interference with equipment, impacts on business operations, theft of sensitive information, compromise of personal data, damage to critical infrastructure and even loss of human life.

Yet few organizations have executed an integrated IoT cybersecurity program, largely because implementation standards or frameworks have been slow to emerge for the platform. We're starting to see some guidance, however: The U.S. Department of Homeland Security³ and Department of Commerce⁴ recently released white papers on IoT guidelines.

Beyond security, many privacy issues surround IoT implementation, particularly related to the collection, storage and use of data flows of information acquired through the use of IoT devices. When the collection and use of IoT data includes personal information, or if the information collected can be used to paint a detailed picture of an individual's activities, businesses must then consider the privacy risks associated with processing this data. And since IoT security and privacy is a nascent discipline, most businesses lack the expertise and resources to design, deploy and operate a program on their own.

Nonetheless, many are starting to take action on both the security and privacy fronts. This year, 35% of GSISS respondents said they have an IoT security strategy in place, and an additional 28% are implementing one. Additionally, 46% of respondents said they will invest in security for the Internet of Things over the next 12 months. They plan to fund initiatives such as development of new data-governance policies, device and system interconnectivity and vulnerability, employee training and uniform cybersecurity standards and policies.

35%

*Have implemented
a security strategy for
the Internet of Things*



PwC, CIO and CSO, *The Global State of Information Security*® Survey 2017, October 5, 2016

³ US Department of Homeland Security, [Strategic Principles for Securing the Internet of Things](#), November 2016

⁴ Department of Commerce, [Fostering the Advancement of the Internet of Things](#), January 2017

Implementation of IoT policies, technologies & people skills in the next 12 months



New data collection, retention and destruction policies

37%



Assess device and system interconnectivity and vulnerability across the business ecosystem

35%



Employee training on IoT security practices

35%



Policies and technologies to safeguard against consumer privacy violations

34%



Uniform cybersecurity standards and policies for IoT devices and systems

32%

Source: PwC, CIO and CSO, *The Global State of Information Security® Survey 2017*, October 5, 2016

In addition to these programs, organizations will need to develop procedures to build in cybersecurity and privacy from the outset when designing new software and devices. Already, some businesses are reconsidering their software-development strategy for connected devices, with an emphasis on more flexible cybersecurity capabilities. *“Forward-thinking businesses are re-architecting the way that they write the code that goes into IoT devices,”* said David Burg, PwC’s Global Cybersecurity and Privacy Advisory Leader. *“Our clients are asking us to create development environments in which it’s very easy to continuously increase the cybersecurity capability of the product itself.”*

Beyond devices, business leaders should be prepared to proactively monitor and assess the entire continuum of conditions and threats across domains—including OT, which has often been back-burnered, for decades, in some cases, as organizations focus on securing their IT systems. *“We’re working with businesses to help them gain visibility into what’s happening across all three IoT domains,”* said PwC’s Burg. *“Companies should be able to see the fissures in the seams across those three layers before there is a crack.”*

It’s good news that organizations are beginning to address cybersecurity and privacy for converged technologies, but much remains to be done. Those that take proactive steps to implement an integrated IoT cybersecurity and privacy program will be better prepared to manage inevitable future risks and create new products and services that can transform business models. Following is a look at how organizations are taking steps to secure the IoT and prepare for future opportunities.

This is the third in a four-part series on key findings from The Global State of Information Security® Survey 2017. The first two installments, Moving forward with cybersecurity and privacy and Toward new possibilities in threat management, explored how digital businesses are adopting new cybersecurity technologies and processes and how they are addressing threats. Our fourth and final paper is about how organizations are managing rising geopolitical threats.



Take a look at our interactive timeline.

Connecting the dots: A timeline of technologies, threats and regulations that redefined cybersecurity and privacy

Competitive advantages of the IoT

It seems all but certain that the IoT will be this decade's great disruptor. Most prognosticators believe the interconnected platform will generate expansive economic growth by transforming business models and unleashing innovative products and services that will make consumers' lives easier and safer.

The potential advantages are almost limitless. In a digital-first world, the IoT promises to help companies improve operations, redefine consumer relationships and create entirely new revenue streams. Among consumers, digital convergence will bring unprecedented lifestyle conveniences, improve healthcare and offer new control over homes and automobiles. And governments and municipalities will leverage IoT technologies to create "smart cities" in which digitally connected infrastructure—such as street lighting, traffic monitoring and intelligent buildings—employs data to improve citizens' quality of life and save money.

These tectonic transitions are shaking up businesses across virtually all industries, often with great fanfare and oversize consumer expectations. Consider the connected automobile. While the commercial availability of the fully autonomous car is

a few years down the pike, today's new vehicles come fully loaded with self-driving features made possible by in-vehicle computers, sensors, cameras and software. These technologies enable Internet connectivity, blind-spot monitoring, real-time navigation and lane-departure warnings, and vehicle diagnostics. Motorists believe tomorrow's autonomous automobile will deliver practically Jetsonian conveniences, money-saving predictive maintenance and improved driving safety. (See sidebar on page 11.)

46%



Plan to invest in new security needs related to evolving business models

PwC, CIO and CSO, *The Global State of Information Security® Survey 2017*, October 5, 2016

Industries most likely to have/are implementing an IoT security strategy



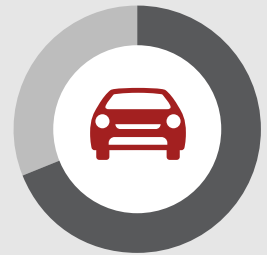
78%

Telecommunications



73%

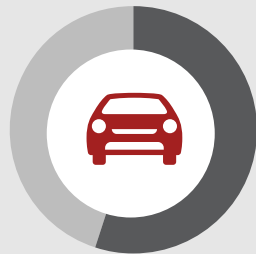
Technology



69%

Automotive

Planning to invest in IoT security in the coming year



55%

Automotive



55%

Industrial products



53%

Technology

Source: PwC, CIO and CSO, *The Global State of Information Security® Survey 2017*, October 5, 2016

The IoT also promises to redefine how healthcare providers monitor, interact with and treat medical patients. Today, the healthcare ecosystem includes connected equipment such as health monitors, “smart” hospital beds, telemedicine capabilities and connected medical devices like pacemakers and glucose monitors. These connected devices and medical equipment promise to advance patient care, promote wellness and even help predict future disease trends. (See sidebar on page 12.)

It's complicated: Why security is a moving target

The IoT is the Wild West of cybersecurity and privacy, an ungoverned frontier without laws and norms. In fact, there is no global agreement as to which entities own the platform and are ultimately responsible for its security.

“As the Internet of Things rapidly expands, it is introducing new risks that are not well understood and could have sweeping implications,” said Sean Joyce, PwC’s US Cybersecurity and Privacy Leader. *“The management of risks to cybersecurity and privacy must not be an afterthought in development and adoption of connected devices — it needs to be a greater priority.”*

Doing so will be a Herculean effort. The IoT juggernaut comprises billions of devices and equipment that employ disparate operating systems, communications protocols and hardware specifications. The massive footprint and complexity of the platform precludes most businesses from drafting an IoT cybersecurity and privacy framework—they simply lack the in-house technical expertise. And while third-party vendors have developed a slew of custom frameworks and bolt-on modules, they typically are not interoperable.

Similarly, no standards exist for the multitude of devices that are already part of the ecosystem. Unlike IT equipment, connected devices were not designed with security in mind—and risks are rampant. HP Fortify on Demand reviewed 10 of the most

35%

Plan to assess device and system interconnectivity and vulnerabilities across the business ecosystem



PwC, CIO and CSO, *The Global State of Information Security*® Survey 2017, October 5, 2016

commonly used connected devices and found that 70% contain serious vulnerabilities.⁵ Addressing these shortcomings will be a hurdle because many devices lack the computing power to handle essential technologies like encryption, authentication and automated patching. In addition, many of these devices were developed and designed without regard for security.

At the other end of the spectrum, operational technologies and infrastructure systems have lifetimes that can stretch into decades. These once-powerful legacy systems are often a burden to update—if they even can be updated, given that many may be at the end of their life cycle. They also may be incapable of interoperation with disparate new systems, software and communications protocols.

Another issue: The IoT presents an entirely new class of risks. Connected equipment often interacts with physical systems and can execute operational changes that could potentially damage property and harm people. Consider, for instance, that researchers have proved that IoT components used in power grids, medical devices and manufacturing plants, to name a few, can be compromised with potentially catastrophic physical results, even including loss of human life.

“As IoT devices continue to permeate our environment, the associated risks increase exponentially,” said Chris Hall, Principal, PwC. *“Organizations and individual consumers need to be far more educated on how to address these risks: from the simplistic, such as changing default passwords, to the more complex, such as network segmentation or device management. Failure to do so can truly be a matter of life or death. That isn’t hyperbole any longer.”*

5 HPE Fortify on Demand, [Internet of Things State of the Union Study](#), July 2014

Automakers are racing to secure the connected car

Nothing about the IoT has captured the public's imagination with the same pedal-to-the-metal enthusiasm as the autonomous vehicle. Auto aficionados envision a future in which driverless cars will alleviate the daily chore of commuting by reducing traffic accidents, easing congestion, improving fuel efficiency and simplifying auto maintenance.

Thanks to highly publicized studies, they are also well aware of the risks of hacking.

Researchers have proved that skilled hackers can remotely hijack today's connected cars to apply the brakes, kill the engine and control steering. Cybercriminals can also gain access to in-vehicle telematics to pilfer sensitive data about the automobile and its driver. At this point, no such hacks have been reported in the wild. But that hasn't muted the buzz.

Automakers, meanwhile, are racing toward autonomy, and many are following a road map that emphasizes security and privacy. More than half (54%) of automotive respondents to this year's survey said they produce or sell products or services that enable in-vehicle telematics. Among those that do, 81% said they are confident that

they can securely provide these services. Most entrust their traditional IT function to develop the security framework and architecture for telematics.

Carmakers and OEMs are also equipped to ingest and use real-time vehicle diagnostics data. Among those that are investing in remote-vehicle diagnostics, half already have already deployed diagnostic-monitoring capabilities—and 74% have implemented a security plan for telematics data.

Telematics data can reveal a great deal about an individual vehicle and its driver, including sensitive information that could impact consumer data privacy. Consider that almost two-thirds (65%) of respondents said they currently collect information on vehicle location from telematics systems and 44% gather driver data.

And they're not just compiling data. More than one-quarter (28%) said they currently market telematics information, and an additional 25% plan to do so over the next 24 months. There will be no shortage of buyers: Insurance companies, attorneys and law enforcement agencies, and after-market automotive OEMs, among others, are eager to capture telematics data.

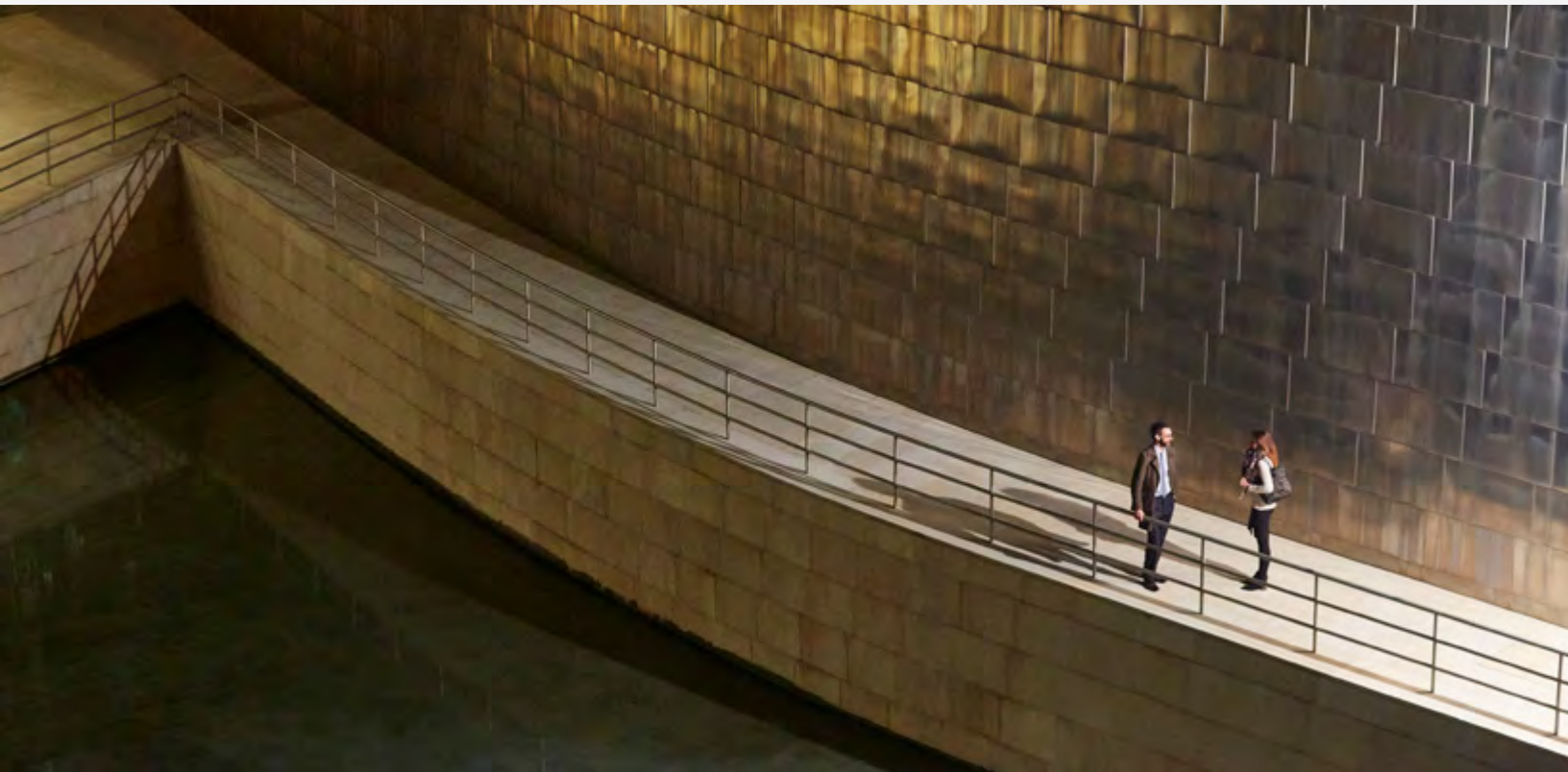
How devices are connecting patients to better healthcare

By now, you've probably overheard at least one conversation about the daily grail of 10,000 steps. Millions of fitness fanatics, and those who would be buff, are attempting to achieve this activity metric set by makers of wearable monitoring devices.

While fitness trackers are the most visible of connected health devices, businesses and consumers alike have adopted an array of more sophisticated IoT equipment that includes implanted glucose monitors and pacemakers, monitoring systems for eldercare, in-hospital surgical systems and telemedicine capabilities, to name a few.

Among respondents to this year's security survey, 44% of healthcare payer and provider respondents said they have integrated operational systems and wearable devices with their IT infrastructure, effectively converging the three domains that comprise the IoT. Among these respondents, 68% said their organization gathers data from wearable devices.

It's encouraging that many respondents said they are addressing security and privacy risks. In fact, 64% said they have performed a risk assessment of connected devices and technologies to evaluate potential security vulnerabilities, and more than half (55%) said they have implemented security controls for these devices.



The risks of too much information

Today, much of the data generated by the IoT is anonymous and often meaningless messaging between machines. Increasingly, however, data compiled in the IoT ecosystem can yield sensitive personal information about consumers who use connected devices.

Already, smartphones, fitness trackers, in-vehicle telematics and home-monitoring systems generate an incredible amount of data that digitally track the specific locations and behaviors of individuals. Use of such data to provide insight about consumer behavior or to personalize services based on customer preferences can create numerous business opportunities. However, businesses that mine personal data for purposes that are not transparent to the user, or that share personal data with third parties without adequate notice, run the risk of engaging in practices that violate consumer protection and safety regulations. These regulations include those enforced by the Federal Trade Commission (FTC), which plays a primary role in regulating information privacy and security using its broad authority to protect consumers from unfair or deceptive trade practices.

“At the outset, businesses should be considering the privacy implications of acquiring, storing and using data collected through IoT devices and develop data-use governance practices that address the security and privacy of personal information stored online,” said Jocelyn Aqua, Principal, PwC.

And then there’s ethical use of data, a new discipline for many businesses that may not be governed by existing privacy regulations. As companies collect and analyze a broader range of information, they may unwittingly create situations that could blur the lines of acceptable data use. Consider the following scenario: A business includes employee addresses in hiring algorithms to determine how close candidates live to the workplace. That’s all well and good, but this information could also be used unethically,

allowing a company to disqualify individuals based on race, sexual orientation or religion since neighborhoods often have unique demographic compositions that correspond to these categories.

It's not surprising, then, that IoT-generated data is already in the crosshairs of regulatory bodies that are prepared to levy steep fines and remediation obligations. In the EU, the landmark General Data Protection Regulation (GDPR) will bring far-reaching data-privacy requirements for any business that is established in the EU and processes personal data, offers goods or services, or monitors the behavior of European residents. The regulation also extends the commonly accepted definition of personal data to include elements such as geolocation and online identifiers like an IP address. GDPR violations could incur fines of up to 4% of annual global turnover when the regulation takes effect in May 2018.

“At the outset, businesses should be considering the privacy implications of acquiring, storing and using data collected through IoT devices and develop data-use governance practices that address the security and privacy of personal information stored online,” said Jocelyn Aqua, Principal, PwC.

In the United States, the FTC recently reached a settlement with a mobile advertising company that had tracked consumers' geolocation data without permission.⁶ The FTC fined the business \$950,000 and prohibited it from collecting consumers' location information without their express consent. The Commission also required that the mobile ad firm implement a comprehensive data-privacy program that must be independently audited every two years—for the next 20 years.

⁶ Federal Trade Commission, [Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission](#), June 22, 2016

Taking steps to build IoT cybersecurity

Many businesses are deciding that the opportunities of the IoT are simply too compelling to ignore. They see the emerging platform as a catalyst of change, a vehicle to boost competitive advantages, increase operational efficiencies and create new revenue streams.

Trouble is, many are jumping into the IoT before they implement cybersecurity safeguards. Granted, the lack of IoT standards is a significant hurdle, but it is not insurmountable. Businesses can follow existing best practices that will help build a strong foundation for IoT cybersecurity, said Shawn Connors, Principal, PwC.

“Given the sprawl of cybersecurity technologies deployed across organizational ecosystems, we would advocate that enterprises begin the dialogue now with their technology product partners regarding the path forward to identifying, securing and managing data produced or transacted on by an IoT capability,” Connors said. *“We believe that many organizations will find that existing enterprise-class technologies are going to be quickly extended to manage and protect the flow of data within and across IoT networks. Keeping a sharp eye on the niche vendor landscape will also be important, but given that IoT presents another wrinkle in the enterprise data-management conversation, initiating a solution conversation with those that know your organization best seems like a good place to start.”*



An IoT cybersecurity initiative should begin with a careful assessment of all data across the business ecosystem — including the extended IoT platform, third-party partners and communications networks. Organizations will need a solid understanding of the value of data, the number and type of data assets, where data is located and transmitted, who has access to this information and the potential impacts of compromise. Use of personal information should be limited to the specific purposes for which it was collected.

“Given the sprawl of cybersecurity technologies deployed across organizational ecosystems, we would advocate that enterprises begin the dialogue now with their technology product partners regarding the path forward to identifying, securing and managing data produced or transacted on by an IoT capability,” said Shawn Connors, Principal, PwC.

The notion of “privacy by design” is viewed as a best practice, but is now mandatory under GDPR. This approach requires product and service developers to consider which personal information is really needed from the start, and to implement mechanisms that minimize, anonymize or otherwise obfuscate identifying data. Organizations will need to instill this discipline and allow designers to challenge the personal information that is truly necessary for a product or service to work as intended.

Multinational businesses will need to implement processes and controls to help ensure that transfer of personally identifiable information across borders does not violate regulatory mandates. Doing so will require an up-to-the-minute understanding of data-privacy regulations across geographies and knowledge of emerging interpretations on the ethical use of information. Going

beyond GDPR, businesses should work carefully with legal and compliance stakeholders to ensure they implement appropriate privacy safeguards.

Beyond data, an assessment of the security capabilities of connected devices will be integral. As the IoT platform matures and connected things proliferate, it's unlikely that businesses will be able to evaluate all connected equipment—but they should identify, inventory and evaluate the security capabilities of critical at-risk equipment. This assessment should be performed at the network, application, data and physical layers, and include ethical hacking and vulnerability testing to understand the weaknesses of connected devices and how hackers might exploit them.

Businesses should also carefully assess potential vulnerabilities in entry points between services and devices. Cybercriminals often take advantage of weaknesses in API interfaces between mobile devices, web interfaces and cloud systems to gain a foothold into the network and systems.



As noted above, the longevity of operational systems presents a particular concern. OT equipment is often not managed with the same discipline as IT systems, and may go years without patches or updates. At the other end of the spectrum, new bare-bones connected devices are often incapable of automated patching. Nonetheless, businesses should implement processes to update critical equipment whenever possible and include software patches for IoT devices in their vulnerability-management policies. If systems are too old for this type of automatic update, organizations could segment them onto their own subnet, thereby reducing the risk. Also, active monitoring of these devices must be put in place for alerting on anomalous behavior as well as system health.

“We believe that many organizations will find that existing enterprise-class technologies are going to be quickly extended to manage and protect the flow of data within and across IoT networks. Keeping a sharp eye on the niche vendor landscape will also be important, but given that IoT presents another wrinkle in the enterprise data-management conversation, initiating a solution conversation with those that know your organization best seems like a good place to start,” said Shawn Connors, Principal, PwC.

As with IT and OT infrastructure, IoT components are vulnerable to exploits of privileged user accounts, which can provide a fast lane to compromise of sensitive data, systems and digital assets. Many organizations overlook the risks of privileged accounts—even in their IT environment—and may unwittingly assign an IoT device to a privileged account that lacks adequate cybersecurity safeguards. Basic precautions include using strong passwords for devices associated with a privileged account and limiting the sharing of privileged account credentials among IT administrators.

Leveraging existing technologies to integrate cybersecurity

A cybersecurity program for the IoT does not necessarily require wholesale purchase of new technologies and solutions. Instead, organizations can start by integrating core IT cybersecurity safeguards with their IoT infrastructure.

As identity shifts from people and applications to connected devices, identity and access management (IAM) will become an increasingly critical capability. The vast number of identities across the IoT ecosystem will require a unified approach to authorizing and de-authorizing access to data, as well as the ability to seamlessly apply security policies across all domains.

It's more essential than ever that IAM solutions integrate strong user authentication to protect connected devices that store or transmit sensitive data. Authentication should employ the principle of least privilege and segregate user roles in multiple environments. While multi-factor authentication and biometrics will work only with human identities, these technologies can still play a role in better securing the infrastructure.

Encryption is another critical technology for safeguarding private data.

As noted, however, rudimentary connected devices may not have the computing horsepower to manage cryptographic keys. Nonetheless, businesses should implement strong data-encryption algorithms when possible and ensure that encryption keys are not

43%
of respondents plan to invest in biometrics and advanced authentication in the coming year



PwC, CIO and CSO, *The Global State of Information Security® Survey 2017*, October 5, 2016

displayed in clear text. To the best extent possible, all personal data should be encrypted at rest and in transit. The challenge will be to do so without increasing costs and complexity, or creating data-processing slowdowns.

Some forward-thinking businesses are employing Enterprise Security Architecture (ESA) to build IoT security that is baked into architectural components across domains. ESA can be particularly useful in helping businesses integrate and secure new layers—sensors, additional networking and computing platforms and service platforms—that the IoT will add to the enterprise security stack. ESA can enable organizations to apply appropriate security controls to these additional layers and integrate them with enterprise stacks by leveraging common denominators such as network layers and communication channels.



People: The Achilles' heel of cybersecurity

A cybersecurity program is only as strong as its weakest link—and that's often employees who are undertrained in cybersecurity and privacy procedures. Employees have traditionally been the leading source of security incidents, and while some act with malicious intent, many unwittingly trigger incidents through simple carelessness or unawareness of basic precautions.

By now, most business leaders know that employee training is a foundational element of any cybersecurity program—yet just over half (53%) of this year's survey respondents have an employee security awareness program in place. Training for IoT security practices is not yet a matter of course for most organizations, but it's promising that 35% of respondents said they plan to invest in employee training on IoT cybersecurity practices this year.

35%
of respondents plan to invest in employee training for the IoT in the next 12 months



To be most effective, training should be tailored to the individual company's threats, response-readiness and

processes. Fostering a culture of security will be most effective when executive leaders proactively articulate the importance of a secure business environment. *“Organizations need to set the tone from the top, making security training really about enabling the company's digital future,”* said Grant Waterfall, PwC's Global Cybersecurity and Privacy Assurance Leader. *“They then need to tie training to the purpose of the company and design awareness programs around that.”*

PwC, CIO and CSO, *The Global State of Information Security*® Survey 2017, October 5, 2016

Aside from training for employees, IoT cybersecurity will require staff expertise in new competencies that extend beyond traditional IT security. For instance, security practitioners will need hands-on knowledge of embedded devices, sensors and machine-to-machine communications. They should have experience integrating disparate protocols for data transmission, communications and networking — both within the on-premises infrastructure as well as across cloud environments. Algorithmic expertise will be needed to enhance the quality of collected data across systems and domains, as well as the ability to discern between insight and noise generated by massive volumes of data.

Managing the dynamic risks of the IoT will represent a challenge of the first order for organizations that lack the caliber of talent necessary to create, implement and manage IoT security. Rather than using internal resources to develop an end-to-end cybersecurity program, some businesses are turning to managed security service providers that specialize in the IoT. In addition to providing expertise specific to IoT security and infrastructure, managed service providers can also help address the global shortage of skilled cybersecurity workers and ease security budget constraints.

Connecting the dots for the future

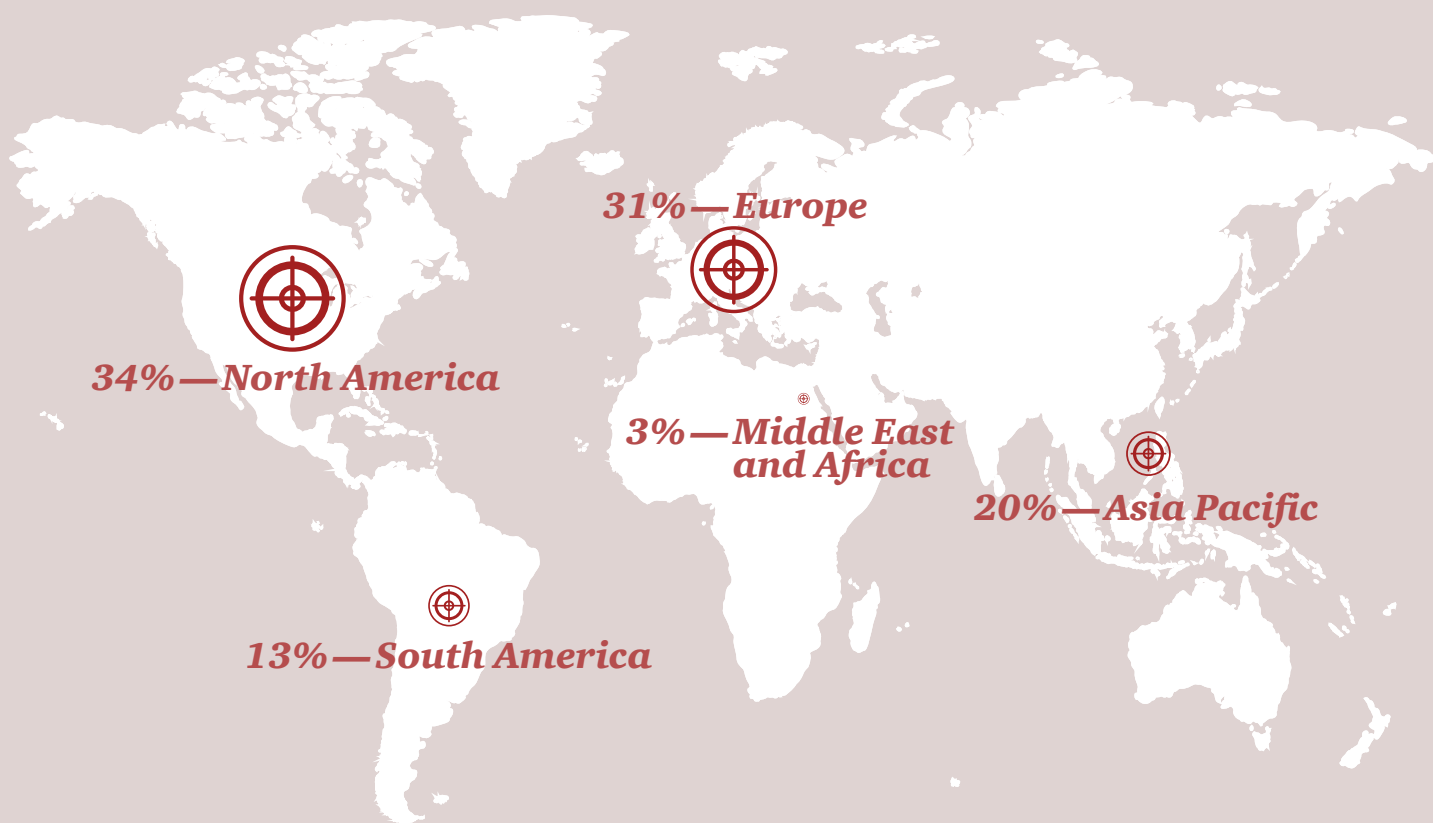
The IoT is poised to upend business models, disrupt economies around the world, and deliver unprecedented conveniences to society. An integrated cybersecurity and privacy program is key to realizing potential advantages as the Internet of Things unfolds. At the end of the day, businesses that align IoT product and systems development with emerging cybersecurity standards and existing safeguards will have a head start realizing advantages on the interconnected platform of tomorrow.

Methodology

The Global State of Information Security® Survey 2017 is a worldwide study by PwC, CIO and CSO. It was conducted online from April 4, 2016 to June 3, 2016. Readers of CIO and CSO and clients of PwC from around the globe were invited via email to participate in the survey.

The results discussed in this report are based on responses of more than 10,000 CEOs, CFOs, CIOs, CISOs, CSOs, VPs and directors of IT and security practices from more than 133 countries.

Thirty-four percent (34%) of survey respondents are from North America, 31% from Europe, 20% from Asia Pacific, 13% from South America and 3% from the Middle East and Africa.



The margin of error is less than 1%; numbers may not add to 100% due to rounding. All figures and graphics in this report were sourced from survey results.

PwC cybersecurity and privacy contacts by country

Australia

Richard Bergman

Partner

richard.bergman@au.pwc.com

Andrew Gordon

Partner

andrew.n.gordon@au.pwc.com

Steve Ingram

Partner

steve.ingram@au.pwc.com

Austria

Christian Kurz

Senior Manager

christian.kurz@at.pwc.com

Belgium

Filip De Wolf

Partner

filip.de.wolf@be.pwc.com

Brazil

Edgar D'Andrea

Partner

edgar.dandrea@br.pwc.com

Canada

David Craig

Partner

david.craig@ca.pwc.com

Sajith (Saj) Nair

Partner

s.nair@ca.pwc.com

Richard Wilson

Partner

richard.m.wilson@ca.pwc.com

China

Megan Haas

Partner

megan.l.haas@hk.pwc.com

Ramesh Moosa

Partner

ramesh.moosa@cn.pwc.com

Kenneth Wong

Partner

kenneth.ks.wong@hk.pwc.com

Denmark

Christian Kjær

Director

christian.x.kjaer@dk.pwc.com

Mads Nørgaard Madsen

Partner

mads.norgaard.madsen@dk.pwc.com

France

Philippe Trouchaud

Partner

philippe.trouchaud@fr.pwc.com

Germany

Derk Fischer

Partner

derk.fischer@de.pwc.com

India

Sivarama Krishnan

Partner

sivarama.krishnan@in.pwc.com

Israel

Rafael Maman

Partner

rafael.maman@il.pwc.com

Italy

Fabio Merello

Partner

fabio.merello@it.pwc.com

Japan

Yuji Hoshizawa

Partner

yuji.hoshizawa@pwc.com

Sean King

Partner

sean.c.king@pwc.com

Naoki Yamamoto

Partner

naoki.n.yamamoto@pwc.com

Korea

Soyoung Park

Partner

s.park@kr.pwc.com

Luxembourg

Vincent Villers

Partner

vincent.villers@lu.pwc.com

Mexico

Fernando Román Sandoval

Partner

fernando.roman@mx.pwc.com

Yonathan Parada

Partner

yonathan.parada@mx.pwc.com

Juan Carlos Carrillo

Director

carlos.carrillo@mx.pwc.com

Middle East

Mike Maddison

Partner

mike.maddison@ae.pwc.com

Netherlands

Gerwin Naber

Partner

gerwin.naber@nl.pwc.com

Otto Vermeulen

Partner

otto.vermeulen@nl.pwc.com

Bram van Tiel

Director

bram.van.tiel@nl.pwc.com

New Zealand

Adrian van Hest

Partner

adrian.p.van.hest@nz.pwc.com

Norway

Lars Erik Fjørtoft

Partner

lars.fjortoft@pwc.com

Poland

Rafal Jaczynski

Director

rafal.jaczynski@pl.pwc.com

Jacek Sygutowski

Director

jacek.sygutowski@pl.pwc.com

Piotr Urban

Partner

piotr.urban@pl.pwc.com

Russia

Tim Clough

Partner

tim.clough@ru.pwc.com

Singapore

Vincent Loy

Partner

vincent.j.loy@sg.pwc.com

Jimmy Sng

Partner

jimmy.sng@sg.pwc.com

South Africa

Sidriaan de Villiers

Partner

sidriaan.de.villiers@za.pwc.com

Elmo Hildebrand

Director/Partner

elmo.hildebrand@za.pwc.com

Busisiwe Mathe

Partner/Director

busisiwe.mathe@za.pwc.com

South East Asia

Jimmy Sng

Partner

jimmy.sng@sg.pwc.com

Spain

Javier Urtiaga Baonza

Partner

javier.urtiaga@es.pwc.com

Elena Maestre

Partner

elena.maestre@es.pwc.com

Sweden

Martin Allen

Director

martin.allen@se.pwc.com

Rolf Rosenvinge

Director

rolf.rosenvinge@se.pwc.com

Switzerland

Reto Haeni

Partner

reto.haeni@ch.pwc.com

Turkey

Burak Sadic

Director

burak.sadic@tr.pwc.com

United Kingdom

Neil Hampson

Partner

neil.r.hampson@uk.pwc.com

Richard Horne

Partner

richard.horne@uk.pwc.com

Alex Petsopoulos

Partner

alex.petsopoulos@uk.pwc.com

United States

Sean Joyce

Principal

sean.joyce@pwc.com

David Burg

Principal

david.b.burg@pwc.com

Grant Waterfall

Partner

grant.waterfall@pwc.com

Recommended reading

Framework for Cyber-Physical Systems Release 1.0: The US National Institute of Standards and Technology (NIST) guidelines for cyber-physical systems.

Careful Connections: Building Security in the Internet of Things: The US Federal Trade Commission advice on building security into Internet of Things devices.

Fostering the Advancement of the Internet of Things: An overview by the US Department of Commerce on the IoT landscape, infrastructure demands, and cybersecurity and privacy best practices.

Strategic Principles for Securing the Internet of Things: Guidance from the US Department of Homeland Security on principles and suggested best practices to build IoT security for devices and systems.

Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems (NIST Special Publication 800-160): The US National Institute of Standards and Technology (NIST) details an engineering-based approach for the entire life cycle of IoT devices and systems.

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 223,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

© 2017 PwC. All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

The Global State of Information Security® is a registered trademark of International Data Group, Inc.

PwC has exercised reasonable care in the collecting, processing, and reporting of this information but has not independently verified, validated, or audited the data to verify the accuracy or completeness of the information. PwC gives no express or implied warranties, including but not limited to any warranties of merchantability or fitness for a particular purpose or use and shall not be liable to any entity or person using this document, or have any liability with respect to this document. This report is for general purposes only, and is not a substitute for consultation with professional advisors.