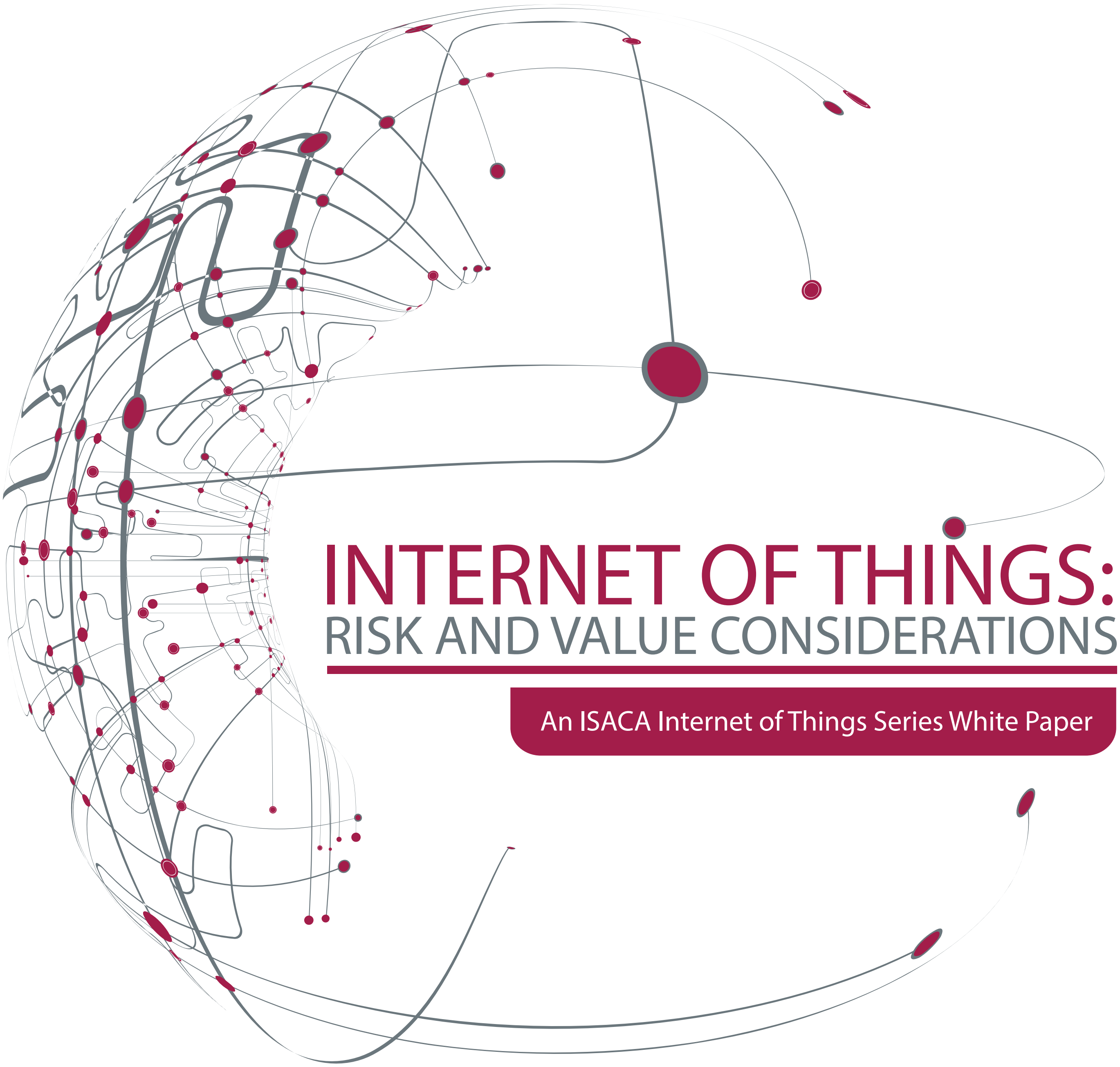


INTERNET OF THINGS:
RISK AND VALUE CONSIDERATIONS

An ISACA Internet of Things Series White Paper

The Internet of Things (IoT) revolution has the potential to be staggeringly transformational and, at the same time, highly disruptive to business. Business value and organizational competitiveness can be derived as enterprises capitalize on these new capabilities to gain more and better business value from IoT devices. With that additional value comes additional risk – or, at least, new avenues of risk. Devices with "always on" network connectivity are enabling new types of attacks that have not been seen in the past; these devices represent a new set of targets for potential data exposure and crime. It is imperative that assurance, security and governance professionals take notice of the IoT trend because it has the potential to redefine the risk equation within many enterprises.

ISACA®
Trust in, and value from, information systems

Trust in, and value from, information systems

ISACA®

With more than 115,000 constituents in 180 countries, ISACA (*www.isaca.org*) helps business and IT leaders build trust in, and value from, information and information systems. Established in 1969, ISACA is the trusted source of knowledge, standards, networking, and career development for information systems audit, assurance, security, risk, privacy and governance professionals. ISACA offers the Cybersecurity Nexus™, a comprehensive set of resources for cybersecurity professionals, and COBIT®, a business framework that helps enterprises govern and manage their information and technology. ISACA also advances and validates business-critical skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) credentials. The association has more than 200 chapters worldwide.

DISCLAIMER

ISACA has designed and created *Internet of Things: Risk and Value Considerations white paper* (the "Work") primarily as an educational resource for assurance, governance, risk and security professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, assurance, governance, risk and security professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

Phone: +1.847.253.1545

Fax: +1.847.253.1443

Email: info@isaca.org

Web site: www.isaca.org

Provide feedback:
www.isaca.org/internet-of-things

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

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

ACKNOWLEDGMENTS

Expert Reviewers

Hans Henrik Berthing
CISA, CGEIT, CRISC, CIA, CPA,
Aalborg University, Denmark

Dan Blum
CISSP,
Security Architects LLC, USA

Allan Boardman
CISA, CISM, CGEIT, CRISC, ACA, CA(SA), CISSP,
UK

Robert Hanson
CISA, CISM, CRISC,
Australian Government, Australia

Rebecca Herold
CISA, CISM, CIPM, CIPP/US, CIPT, CISSP, FLMI,
The Privacy Professor® and SIMBUS®, USA

Phil J. Lageschulte
CGEIT, CPA, KPMG LLP,
USA

Norman Marks
CPA, CRMA

Aureo Monteiro Tavares Da Silva
CISM, CGEIT,
Brazil

Dave Newell
CISSP,
Loptr LLC, USA

Jotham Nyamari
CISA, CISSP, PwC,
USA

Gurvinder Singh
CISA, CISM, CRISC,
Australia

ISACA Board of Directors

Robert E Stroud
CGEIT, CRISC,
CA, USA, International President

Steven A. Babb
CGEIT, CRISC, ITIL,
Vodafone, UK, Vice President

Garry J. Barnes
CISA, CISM, CGEIT, CRISC,
BAE Systems Detica, Australia, Vice President

Robert A. Clyde
CISM,
Adaptive Computing, USA, Vice President

Ramses Gallego
CISM, CGEIT, CCSK, CISSP, SCPM,
Six Sigma Black Belt,
Dell, Spain, Vice President

Theresa Grafenstine
CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA,
US House of Representatives, USA, Vice President

Vittal R. Raj
CISA, CISM, CGEIT, CRISC, CFE, CIA, CISSP, FCA,
Kumar & Raj, India, Vice President

Tony Hayes
CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA,
Queensland Government, Australia, Past International President

Gregory T. Grocholski
CISA,
SABIC, Saudi Arabia, Past International President

Debbie A. Lew
CISA, CRISC,
Ernst & Young LLP, USA, Director

Frank K.M. Yam
CISA, CIA, FHKCS, FHKIoD,
Focus Strategic Group Inc., Hong Kong, Director

Alexander Zapata Lenis
CISA, CGEIT, CRISC, ITIL, PMP,
Grupo Cynthus S.A. de C.V., Mexico, Director

Knowledge Board

Steven A. Babb
CGEIT, CRISC, ITIL
Vodafone, UK, Chairman

Rosemary M. Amato
CISA, CMA, CPA,
Deloitte Touche Tohmatsu Ltd., The Netherlands

Neil Patrick Barlow
CISA, CISM, CRISC, CISSP,
Capital One, UK

Charlie Blanchard
CISA, CISM, CRISC, CIPP/US, CIPP/E, CISSP, FBCS, ACA,
Amgen Inc., USA

Sushil Chatterji
CGEIT,
Edutech Enterprises, Singapore

Phil J. Lageschulte
CGEIT, CPA,
KPMG LLP, USA

Anthony P. Noble
CISA,
Viacom, USA

Jamie Pasfield
CGEIT, ITIL V3, MSP, PRINCE2,
Pfizer, UK

Ivan Sanchez Lopez
CISA, CISM, ISO 27001 LA, CISSP,
DHL Global Forwarding & Freight, Germany

Guidance and Practices Committee

Phil J. Lageschulte
CGEIT, CPA,
KPMG LLP, USA, Chairman

John Jasinski
CISA, CGEIT,
ISO 20K, ITIL Exp, SSBB, ITSMBP,
USA

Yves Marcel Le Roux
CISM, CISSP,
CA Technologies, France

Aureo Monteiro Tavares Da Silva
CISM, CGEIT, Brazil

Jotham Nyamari
CISA, CISSP, PwC, USA

James Seaman
CISM, CRISC, A. Inst. IISP, CCP, CLAS, QSA,
Sysnet Global Solutions, UK

Gurvinder Singh
CISA, CISM, CRISC, Australia

Siang Jun Julia Yeo
CISA, CRISC, CPA (Australia),
MasterCard Asia/Pacific Pte. Ltd., Singapore

Nikolaos Zacharopoulos
CISA, CRISC, CISSP,
Merck KGaA, Germany

Emerging Business and Technology Committee

Jamie Pasfield
CGEIT, ITIL V3 Expert, MSP, PRINCE2,
Pfizer, UK, Chairman

James Ambrosini
CISA, CRISC, CFE, CISSP,
CohnReznick Advisory Group, USA

Bhavesh C. Bhagat
CISM, CGEIT,
ConfidentGovernance.com, EnCrisp, USA

Dan Blum
CISSP,
Security Architects LLC, USA

Victor Chapela
CRISC,
Sm4rt Corp., Mexico

Usha Devarajah
CISSP

William S.W. Gee
CISA, CRISC, FCA, FHKICPA,
PwC, China

Norman Marks
CPA, CRMA

INTERNET OF THINGS: RISK AND VALUE CONSIDERATIONS

A revolution is underway that has the potential to be staggeringly transformational and, at the same time, highly disruptive—the Internet of Things (IoT) trend. IoT (also referred to as "Internet of Everything") devices have embedded network, computing and other information processing capabilities, which allow these devices to be interconnected. The number and types of devices that are being manufactured with these built-in IoT features are increasing rapidly. It is imperative that assurance, security and governance professionals take notice of the IoT trend because it has the potential to redefine the risk equation within many enterprises.

This growing internetwork of "things" is comprised of physical objects with the capability to communicate in new ways—with each other, with their owners or operators, with their manufacturers or with others—to make people's lives easier and enterprises more efficient and competitive. Possible use cases for IoT are extensive. Already, automobiles, household appliances, biomedical devices and other purpose-built devices are processing data, communicating with each other and performing other automated tasks, such as keeping themselves updated, notifying users of potential repair issues and tracking (and potentially scheduling automatically) routine service calls. Less predictable use cases include smart utensils that help to monitor eating habits[1], smart socks that measure pressure to help improve running performance[2] and a "smart diaper" that notifies parents when it needs to be changed[3].

The IoT trend is transformative from a business standpoint. Business value and organizational competitiveness can be derived as enterprises capitalize on these new capabilities to gain more and better business value from devices that they purchase. Additionally, businesses can compete more effectively in the marketplace as they provide these features in products that they sell and incorporate them into service offerings that they provide.

However, with that additional value comes additional risk—or, at least, new avenues of risk. Devices with "always on" network connectivity are enabling new types of attacks that have not been seen in the past; these devices represent a new set of targets for potential data exposure and crime. Moreover, without appropriate planning and forethought, these devices could have privacy impacts that are beyond the customer comfort level.

For practitioners who hold a stake in the trust and value of information and information systems, the ramification of IoT is a changed risk/value equation, which means that risk decisions may need to be revisited. Holistic risk management, ideally, should account for the upside potential of the technology use (i.e., new value enabled through the use of the technology) and possible new risk that is introduced by using the technology. Thinking these areas through ahead of time—before the technology is actively proliferating throughout the enterprise—helps enterprises to be more strategic by accounting for potential areas of adoption in their enterprise risk planning. Practitioners can plan ahead because they can start to invest now in areas to help them to maximize investment—and decrease risk—as IoT use increases.

As embedded network and computing capabilities become more and more commonplace, practitioners need to rebalance related risk/reward decisions. Practitioners also need to adjust how these devices fit into their overall governance approach and ensure that the security of these devices is addressed. Not only should the potential value to the enterprise be understood and evaluated, but also the potential new risk that is introduced should be understood and evaluated so that a holistic risk decision can be made.

This paper is the first in a series that will explore considerations related to IoT. Future papers will discuss risk and security considerations, privacy and regulatory compliance, and assurance topics.

[1] HAPI.com, "HAPIfork: Eat Slowly, Lose Weight, Feel Great!", *www.hapi.com/product/hapifork*

[2] Ramashandran, Vignesh; "Smart Socks Act as Your Running Coach", Mashable, 13 June 2013, *www.mashable.com/2013/06/13/sensoria-smart-socks/*

[3] Pepitone, Julianne; "7 Craziest Things Connected to the Internet", CNN Money, 18 September 2012, *www.money.cnn.com/gallery/technology/2012/09/18/internet-of-things/7.html*

WHAT IS THE INTERNET OF THINGS?

The "Internet of Things" refers to physical objects that have embedded network and computing elements and communicate with other objects over a network. Definitions of IoT vary about the pathway of communication. Some definitions state that IoT devices communicate over the Internet; others state that IoT devices communicate via a network, which may or may not be the Internet. For example, an IEEE special report states the following:

> *"The Internet of Things, or IoT, which you probably have heard about with increasing frequency, is not a second Internet. Rather, it is a network of items—each embedded with sensors—which are connected to the Internet."*[4]

TechTarget describes IoT as follows:

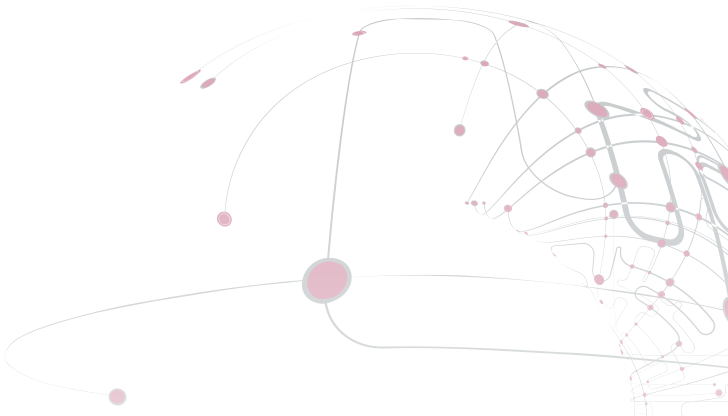
> *"The Internet of Things (IoT) is a scenario in which objects, animals or people are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction."*[5]

The embedded computing elements in IoT objects control how the physical objects behave, the utility that the objects provide to the end user and the manner in which users interact with the objects. For example, household appliances are now available that can automatically schedule repairs or routine service with minimal (or no) user intervention, wearable devices can track their wearers' physical activity (to let them know whether they are leading a healthy lifestyle) and automobiles have computerized navigation, accident prevention and fuel efficiency features.

Research conducted by Pew Internet in association with Elon University suggests that this technology is emerging at a fairly rapid rate and that significant change will transpire. The researchers surveyed a population of "technology experts and/or industry stakeholders"; 83 percent of those they surveyed envisioned widespread, transformative and beneficial impacts on the technology ecosystem due to the emergence of IoT by the year 2025.[6]

Although this widespread transformative change may take a few years to be fully realized, the beginning changes are taking place now. For example, the healthcare vertical has used embedded connectivity and computing components for many years. Biomedical devices (including implantable devices), such as pacemakers and insulin pumps, and diagnostic equipment, such as imaging equipment, not only have the capability to communicate with each other and the outside world, but also have built-in computing elements to automate certain tasks. An implantable defibrillator can have the capability to share diagnostic information wirelessly with medical personnel and also have computing elements that help to make the determination about when defibrillation is necessary.

Other industries have similar special-purpose devices that have embedded computational and/or networking capability. Examples include retail point of sale (PoS) systems, energy and manufacturing industrial control systems (ICS), and communications company switching and routing equipment. One difference between these "purpose-built" embedded systems that are already in use and the IoT concept described in this paper is the ubiquity of the technology and the scale of such endeavors. As the cost of IoT technology decreases, the number of possible use cases that integrate embedded components increases to the point where IoT technology can be economically incorporated into more large appliances and vehicles, and, ultimately, into smaller, lower-cost items, such as wearable objects.



[4] IEEE, "Special Report: The Internet of Things", March 2014, *www.theinstitute.ieee.org/static/special-report-the-internet-of-things*

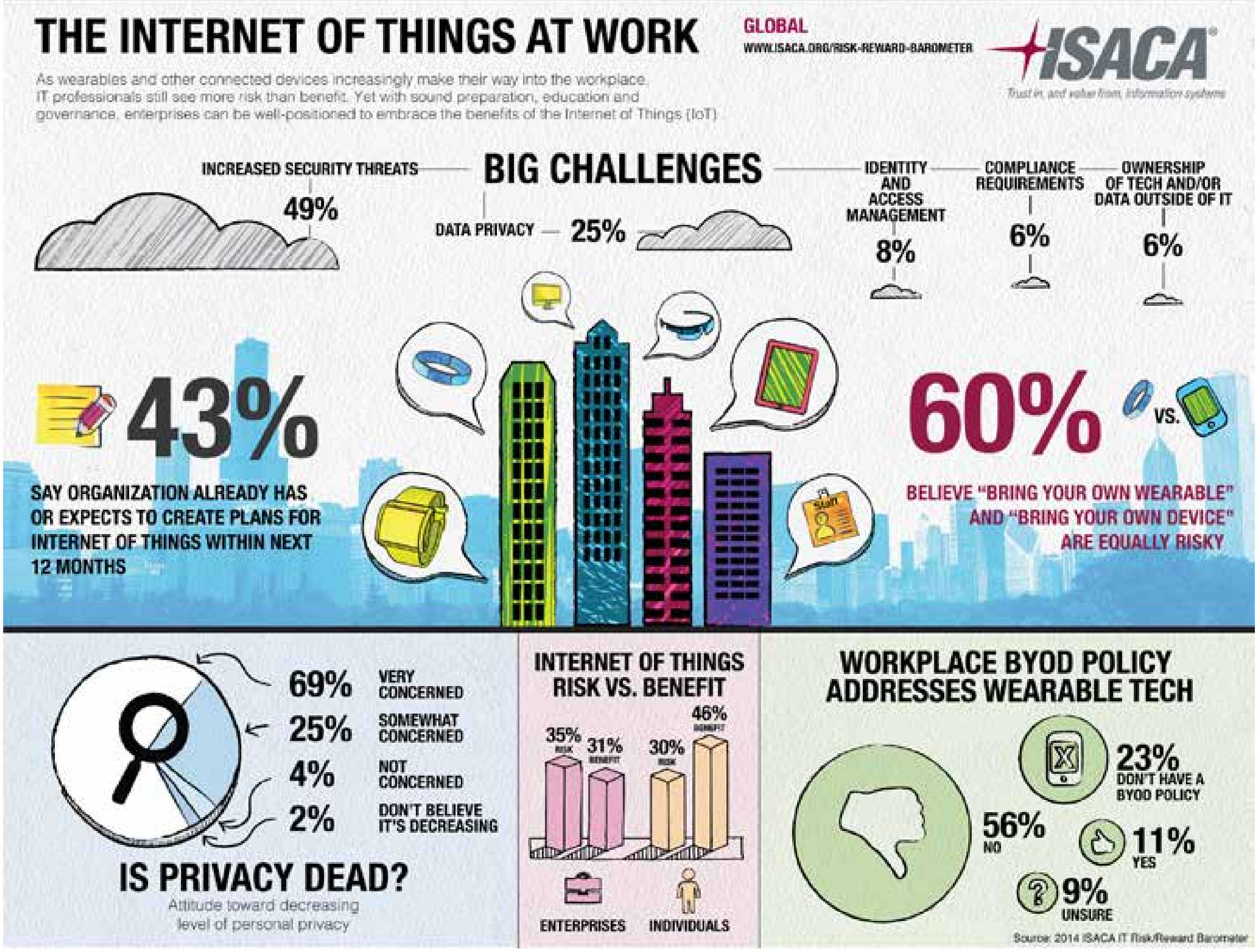
[5] TechTarget, "Internet of Things (IoT)", June 2014, *www.whatis.techtarget.com/definition/Internet-of-Things*

[6] Elon University, "The Internet of Things Will Thrive by 2025", 14 May 2014, *www.elon.edu/docs/e-web/imagining/surveys/2014_survey/Elon%20Pew%20Future%20of%20the%20Internet%20of%20Things%20Report%205-14-14.pdf*

MATURITY AND ADOPTION

In many respects, IoT is less “emerging” than it is “emerged” and already building traction. Meaning, by many indicators, IoT has already arrived in force. Analyst firm International Data Corporation (IDC) estimates that the current (2014) install base is approximately 190.1 billion unique devices, with a market size of just under $6 trillion in total revenue ($5,942.4 billion USD). IDC expects those numbers to increase to 211.9 billion installed end points and about $9 trillion ($8,852 billion USD) by 2020, which is an anticipated growth rate of 7.9 percent, year over year.[7] According to the *2014 ISACA Risk/Reward Barometer*, a survey of global ISACA members in 110 countries, 43 percent of businesses are already addressing IoT: 28 percent already have plans in place to leverage IoT, while another 15 percent will be creating those plans in the next 12 months (see **figure 1**).[8]

Figure 1—The Internet of Things at Work



Source: “ISACA 2014 IT Risk/Reward Barometer”, ISACA, 2014, *www.isaca.org/pages/2014-risk-reward-barometer.aspx*

[7] Lund, Denise; Carrie MacGillivray; Vernon Turner; Mario Morales; “Worldwide Internet of Things (IoT) 2013–2020 Forecast: Billions of Things, Trillions of Dollars”, IDC, May 2014, *www.idc.com/getdoc.jsp?containerId=243661*

[8] ISACA, “ISACA 2014 IT Risk/Reward Barometer”, 2014, *www.isaca.org/pages/2014-risk-reward-barometer.aspx*

Although market size and install base (number of devices) is projected to be quite high, signs of change may be paradoxically somewhat harder for risk practitioners to see within their enterprises. The change may impact the enterprise, but be subtle and occur in a way that is not obvious immediately. The reasons that the IoT change may be difficult to see are lack of familiarity with the concept, the dynamics of adoption, and context. The term Internet of Things is not familiar to many business leaders. For example, the findings from the ISACA 2013 Risk/Reward Barometer survey[9] found that even those individuals who were active users of IoT technologies were unaware of the term:

> *"In the US, where Internet of Things devices are readily available, fewer than one in five Americans (16%) were aware of the term "Internet of Things." Yet, many have used Internet of Things devices, such as a GPS system (62%), electronic toll devices on their cars (28%), and smart TVs (20%)."*[10]

The technology may be in use in physical objects throughout the enterprise, but because the additional network computing function is not visible and most people are not familiar with IoT, business partners or others in the enterprise are less likely to inform practitioners that anything has changed.

The dynamics of how IoT adoption occurs also affects the ability of practitioners to see IoT-related change. Enterprises that do not yet have industry-specific embedded computing use cases (e.g., biomed, point of sale and ICS,) may not have formulated an overarching strategy to address IoT. Enterprises may acquire embedded networking and computing capability as additive features in replacements for items that they purchased in the past—unless enterprises already have an overarching strategy to address IoT, they may not realize that these features are even there.

Practitioner ability to detect IoT change also depends on context because scale may be small. For example, a new, large-scale inventory management system that leverages IoT is probably not going to be undetected, but incorporation of network-enabled smoke detectors into a building could be undetected by risk managers. Chances are good that risk management personnel will evaluate the inventory management system from a due diligence standpoint. For example, they will likely evaluate the technical, operational, compliance and other risk scenarios as that system moves through the procurement process. In contrast, commonplace purchases (smoke alarms, new vehicles for an automobile fleet, temperature sensors, etc.) may not trigger risk manager attention in the same way—although the items can contain computing and network capabilities, they are less likely to be evaluated in a thorough manner (unless the scenarios are evaluated ahead of time). Risk can exist in the seemingly innocuous purchases. For example, competitors can get possession of delivery route information because of a problem with a networked navigation system, or attackers can subvert a smoke alarm. Enterprises can be using IoT without even realizing that they are doing so, or under conditions by which the risk management stakeholders are not informed.

Risk/assurance/security mechanisms can be very difficult to apply after deployment of a new technology. Enterprises experienced this difficulty acutely with the cloud. Although specific risk and privacy concerns are different between IoT and the cloud, a similar adoption dynamic should be anticipated. In many cases, enterprises adopted cloud usage in piecemeal and absent of central oversight and governance; the same potential exists for IoT.

The cloud was (and often still is) challenging to practitioners from a risk management standpoint. Practitioners should take notice that IoT is demonstrating similar adoption dynamics, because, looking forward, IoT appears to be on the cusp of a major wave of large-scale adoption (see **figure 1**). According to the *2014 ISACA Risk/Reward Barometer*, 64 percent of respondents believe that the benefits of IoT, as it relates to enterprises, outweigh the risk or that the risk and the benefits are appropriately balanced. Seventy percent of these same respondents believe that the benefits of IoT, as it relates to individuals, outweigh the risk or that the risk and the benefits are appropriately balanced.[11] The implications are that IoT should be an area of focus for practitioners.

[9] ISACA, "Risks and Rewards of the Internet of Things", 2013, *www.isaca.org/SiteCollectionDocuments/2013-Risk-Reward-Survey/2013-Global-Survey-Report.pdf*

[10] *Ibid.*

[11] ISACA, "ISACA 2014 IT Risk/Reward Barometer", 2014, *www.isaca.org/pages/2014-risk-reward-barometer.aspx*

VALUE PROPOSITION

For practitioners to be able to accurately and objectively evaluate an enterprise risk profile and make informed decisions about appropriate countermeasures, it is important for practitioners to understand the potential new risk that the enterprise may incur because of IoT devices and the new business value that IoT devices can potentially generate. Many business teams that are outside of assurance, security and risk management are likely to focus almost exclusively on the value side of IoT. This paper presents an overview of the value side of IoT first, and then addresses the risk areas of IoT.

The business value that strategic use of IoT can potentially generate can be shown in actual use cases of network-enabled devices and the value that they brought to the enterprise.

One of the better-known large-scale examples of business value is from government, specifically, the city of Santander, Spain. Since 2009, Santander has been working to become the "world's first smart city," by deploying 1,300 sensors throughout the city and another 325 sensors under street asphalt, to measure parking availability, traffic, air quality and numerous other aspects of city life.[12] The city government expects immediate benefits to residents and city management/operations. It envisions better/easier parking for residents, improved and more timely information to tourists about attractions, and improved city management through better intelligence about issues, such as traffic congestion and road safety. Longer term, the city government expects usage to expand and envisions additive and complementary functionality, such as automated payments for city services (including parking and municipal services). Additionally, as existing municipal systems (e.g., library systems) are integrated, new use cases and areas of benefit will continue to emerge.

A commercial example of IoT value is a published case study about the QuanU Furniture (China's largest furniture manufacturer) implementation of a product tracking system that integrates with its enterprise resource planning (ERP) platform. The purpose of the system is to streamline the production and delivery processes through the use of smart sensors (RFID, barcodes and portable terminals) and to integrate the sensors into existing systems and processes. Efficiency within the QuanU Furniture production and delivery process improved, resulting in an increase in delivery speed of 25 percent, a reduction in error rate of 95 percent, and numerous other efficiency and accuracy gains.[13]

Another example of IoT value is the experience of UK motoring firm RAC, which is headquartered in Birmingham. One of the services that RAC provides is a fleet of vehicle-breakdown specialists that responds to stranded motorists and lends roadside assistance. According to an article in *M2M Magazine*, RAC implemented a program that leverages sensors in the diagnostics port of its breakdown-support fleet vehicles. The sensors allow remote monitoring of driver performance and behavior. Through wireless communications, the data that sensors gather about driver adherence to traffic laws, fuel consumption, braking habits and other aspects of vehicle operation are sent to a central system for analysis. This analysis helps to drive efficiency improvements and (potentially, if required) remedial action to address drivers who are operating in an unsafe or illegal manner. Use of these devices led to a 17-percent reduction in fuel costs and to a potential new business opportunity—making the technology available to corporate customers.[14]

The previous use cases are economically focused returns (mostly financial), but IoT also provides important health and safety benefits and quality-of-life benefits. An example is the European Union's plans for eCall—a system that will be built into every vehicle and, in the case of a vehicle crash, will inform emergency personnel to assist.[15] This initiative is expected to shave 50 to 60 percent off of the response time for emergency services, leading to potentially lifesaving consequences.

The previous use cases illustrate that business value can be directly tied to employment of IoT.

[12] Gonzalez, Maria; "The Spanish City of Santander to Become a Global Smart City", Mobile World Capital, 11 November 2013, *www.mobileworldcapital.com/en/article/250*

[13] hp, "QuanU Furniture Co., Ltd. Improves Tracking Management System and Delivers Superior Products", ,August 2012, *h20195.www2.hp.com/v2/GetPDF.aspx%2F4AA4-1181EEW.pdf*

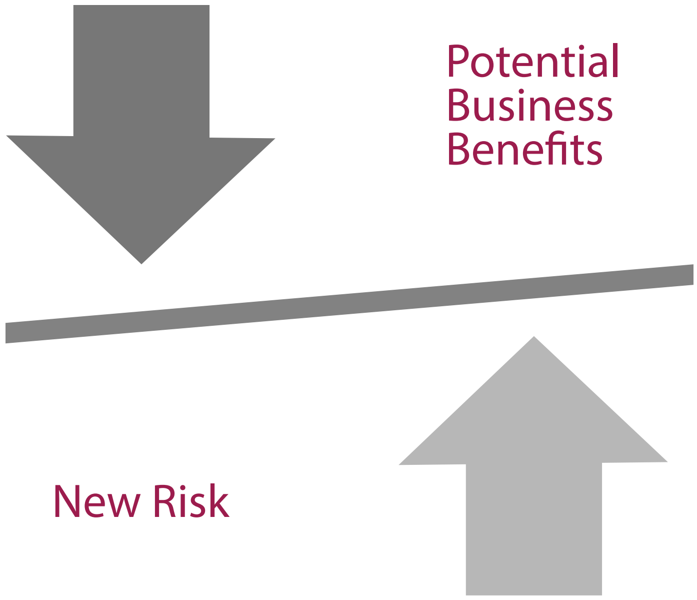
[14] M2M Magazine, "Case Study: RAC Using M2M to Cut Fuel Costs by 17%", 8 May 2014, *www.machinetomachinemagazine.com/2014/05/08/case-study-rac-using-m2m-to-cut-fuel-costs-by-17/*

RISK AND RISK MITIGATION

Although IoT can result in financial, health and safety, and quality-of-life benefits, IoT can also introduce new risk. Any new technology, process or business method can increase risk, but IoT, because of its pervasiveness, has the potential to increase risk significantly. Risk scenarios differ between enterprises that manufacture and sell communication-capable embedded systems and enterprises that are users of these devices. This paper focuses on the potential risk scenarios that are pertinent to users of IoT devices.

To evaluate risk holistically, numerous business, operational and technical risk areas must be considered to balance the business benefits described previously with new risk that is introduced through IoT adoption (see **figure 2**).

Figure 2—Holistic Risk Management: New Risk Compared With New Business Benefits



Although specific risk depends on usage, some of the IoT-usage risk areas that practitioners should consider follow.

Business risk:

- Health and safety
- Regulatory compliance
- User privacy
- Unexpected costs

Operational risk:

- Inappropriate access to functionality
- Shadow usage
- Performance

Technical risk:

- Device vulnerabilities
- Device updates
- Device management

The following sections outline each of these challenge areas in more detail.

Business Risk

Probably the most significant business risk is the potential health and safety impact if the operation of a device is subverted. Research shows that wireless, potentially lethal attacks are possible against implantable biomedical devices, such as a pacemaker or defibrillator. For example, a 2008 study concludes:

> *"Our investigation shows that an implantable cardioverter defibrillator (1) is potentially susceptible to malicious attacks that violate the privacy of patient information and medical telemetry, and (2) may experience malicious alteration to the integrity of information or state, including patient data and therapy settings for when and how shocks are administered."*[16]

[15] European Commission Digital Agenda for Europe, "eCall: Time Saved = Lives Saved", *www.ec.europa.eu/digital-agenda/en/ecall-time-saved-lives-saved*

[16] Halperin, Daniel; Thomas S. Heydt-Benjamin; Benjamin Ransford; Shane S. Clark; Benessa Defend; Will Morgan; Kevin Fu; Tadayoshi Kohno; William H. Maisel; "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses," IEEE Symposium on Security and Privacy, May 2008, Archimedes, *www.secure-medicine.org/public/publications/icd-study.pdf*

Similar life-threatening attacks have been demonstrated against automobile systems, including the ability to disable the braking systems of an automobile when it is in motion.[17]

Privacy is also a significant business risk consideration. The *2014 ISACA Risk/Reward Barometer* found that 69 percent of those surveyed were "very concerned" about personal privacy.[18] Many examples of privacy impact exist, but one noteworthy example of unwanted privacy impact is home monitoring systems. These systems are designed to protect the home and its inhabitants, but can be vulnerable to wireless attacks that violate privacy and security. Video baby monitors are often placed in a child's bedroom, so that parents can check on the child remotely, from almost anywhere. These monitors can broadcast to TVs, handheld receivers or wirelessly to PCs or smartphones. Many incidents of intruders hacking into Internet-enabled video baby monitors have been reported. Most monitors have security features, but parents are responsible for enabling these features and setting a password. In 2009, an Illinois man sued a baby monitoring system manufacturer after discovering that a neighbor, using the same system, could see into the baby's room.[19] In another legal case, the US Federal Trade Commission filed charges against the marketer of an Internet-connected home security video camera for "lax security practices that exposed the private lives of hundreds of consumers to public viewing on the Internet."[20]

Not only human agents, i.e., attackers, can bring about these health and safety impacts; for example, malware can infect a system with a critical safety role, such as a navigation system in an airplane, an automobile braking system or a smoke sensor. Although it was later determined to not be the sole cause, a malware infection of an airplane monitoring system may have been a contributory factor in the crash of Spanair flight 5022 in 2008.[21]

In addition to health and safety risk, regulatory risk is also possible. Regulatory concerns can occur when embedded computing components:

- Process potentially sensitive data (e.g., PoS systems that process payment information)
- Intersect with regulatory-governed business processes (e.g., financial reporting for public companies or patient care in a clinical environment)
- Impact critical infrastructure (e.g., power and industrial control systems)

Regulatory mandates often apply to the communication-enabled devices in the previous examples and others. If regulatory mandates apply, the complexity of the regulated environment can be compounded because of devices of this type. For example, a PoS system in a retail location may be built to conform to payment card industry (PCI) requirements, but a smoke detector on the same network may not conform; or a magnetic resonance imaging (MRI) machine may be built to comply with the Health Insurance Portability and Accountability Act (HIPAA) technical requirements, but the thermostat in an operating theater may not comply.

Devices that process the personal, private or potentially sensitive information of customers (e.g., imaging equipment in a healthcare context) have the potential to impact user privacy. Like compliance challenges, privacy impacts should be evaluated prior to deployment.

Unexpected costs can occur if an existing, non-computing-capable device is replaced with a computing-capable device because it may require additional connectivity (possibly requiring personnel resources or capital expenditure), or it may require additional support to realize the full value. Practitioners should therefore evaluate whether connection of a device to the network adds sufficient business value to justify potential increases in risk.

[17] Greenberg, Andy;"Hackers Reveal Nasty New Car Attacks—With Me Behind The Wheel (Video)", Forbes, 24 July 2013, *www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/*

[18] ISACA, "ISACA 2014 IT Risk/Reward Barometer", 2014, *www.isaca.org/pages/2014-risk-reward-barometer.aspx*

[19] Choney, Suzanne; "Hacker Attempts to Harass Toddler Through Baby Monitor," NBC NEWS, 14 August 2013, *www.nbcnews.com/tech/security/hacker-attempts-harass-toddler-through-baby-monitor-f6C10916536*

[20] Federal Trade Commission, "Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy," 4 September 2013, *www.ftc.gov/news-events/press*

[21] Leyden, John; "Trojan-ridden Warning System Implicated in Spanair Crash, The Register, 20 August 2010, *www.theregister.co.uk/2010/08/20/spanair_malware/*

Operational Risk

In addition to business risk, the operational aspects of using an embedded system must be considered. For example, machine-to-machine communication must be appropriately secured to ensure that only appropriate personnel (or appropriately authorized devices) have access to make configuration changes and gather telemetry data. In most cases, this security requires operational planning and needs to tie into existing security and monitoring controls to ensure that the level of access is appropriate.

Likewise, from an operational perspective, challenges can be introduced when devices are deployed without the knowledge of the personnel that hold a stake in configuring, monitoring, maintaining and securing the device. Shadow IT is the deployment of technology components without centralized oversight and appropriate governance and can have a significant detrimental impact on IoT usage. Without someone "at the switch" to ensure that risk scenarios are addressed, devices behave as expected and devices are appropriately secured, the enterprise may unknowingly take on risk that is outside of the enterprise comfort level.

Technical Risk

At a technical level, embedded computing has the potential for a more complex set of challenges than traditional IT. Embedded (IoT) devices, like traditional computing devices, can be attacked, suffer outages and be compromised by malware. Because IoT devices are addressable and connected to a network, they are also a potential target for attack. However, because the underlying operation of IoT devices may be less transparent (due to less clear organizational administration responsibility) and because a large quantity of IoT devices is possible over the long term, keeping them secured is likely to be more complex than for traditional computing devices.

In terms of technical risk, attacks against the IoT devices should be considered. Many well-publicized attacks against embedded systems illustrate how these types of attacks can detrimentally impact IoT computing. For example, Spanish security researchers Javier Vazquez-Vidal and Alberto Garcia Illera developed the CAN Hacking Tool (CHT) from off-the-shelf electronic components. This tool is a proof of concept of hacking a car and wirelessly interacting with it in ways that can make operation potentially unsafe.[22]

Attacks against IoT devices can be challenging for manufacturers to respond to. In some situations, the pathway to remediate the issues requires a hardware upgrade rather than modifications to firmware alone. This dynamic can expose enterprises that employ IoT devices to attacks, with minimal ability to implement countermeasures. Even in situations where a firmware update remediates the issue, a new attack against—or vulnerability discovered in—an IoT hardware device requires operations personnel to maintain awareness of those developments and implement mechanisms to respond.

From a device management standpoint, many enterprises are not equipped to extend existing security management mechanisms to these devices. Issues like conducting inventory, monitoring device access and architectural placement of the device on the network and other challenges must be considered, in the same way that they are considered for traditional IT components.

[22] Greenberg, Andy; "This iPhone-Sized Device Can Hack a Car, Researchers Plan to Demonstrate," Forbes, 5 February 2014, *www.forbes.com/sites/andygreenberg/2014/02/05/this-iphone-sized-device-can-hack-a-car-researchers-plan-to-demonstrate/*

QUESTIONS PRACTITIONERS SHOULD ASK

Stakeholder engagement and awareness are critical for IoT-related risk, as they are with any other risk. Following are some of the key questions that practitioners should ask stakeholders when IoT deployment is being considered:

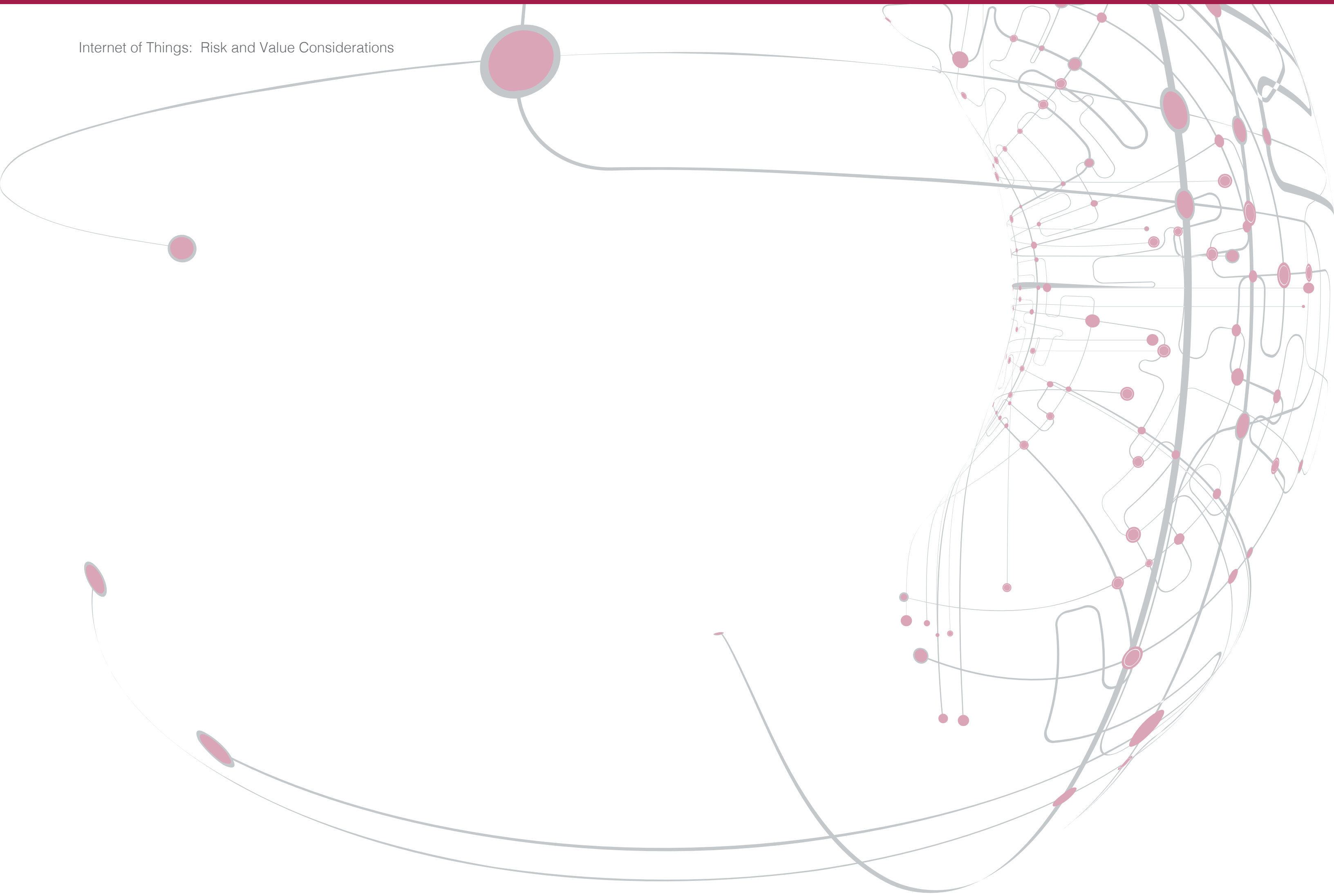
1. How will the device be used from a business perspective? What business processes are supported and what business value is expected to be generated?
2. What is the threat environment for the device? What threats are anticipated and how will they be mitigated?
3. Who will have access to the device and how will their identities be established and proven?
4. What is the process for updating the device in the event of a published attack or vulnerability?
5. Who is responsible for monitoring for new attacks or vulnerabilities pertaining to the device? How will they perform that monitoring?
6. Have all risk scenarios been evaluated and compared to anticipated business value?
7. What personal information is collected, stored or processed by the IoT devices and systems?
8. Do the individuals about whom the personal information applies know that their information is being collected and used? Have they given consent to such uses and collection?
9. With whom will the data be shared/disclosed?

DOS AND DON'TS

Figure 3 presents some important areas for practitioners to consider—the important things that practitioners should do and the important things that practitioners should not do. This is a partial list and numerous other considerations will apply, based on individual usage.

Figure 3—Points to Consider

Dos	Don'ts
• Prepare a threat model. • Evaluate business value. • Holisticaly evalute and manage risk. • Balance risk and rewards. • Notify all stakeholders of anticipated usage. • Engage with business teams early. • Gather all stakeholders to ensure engagement and thorough planning. • Look for points of integration with existing security and operational protections. • Examine and document information that is collected and transmitted by devices to analyze possible privacy impacts. • Discuss with relevant stakeholders when, how and with whom that information will be shared and under what circumstances.	• Deploy quickly without consulting business or other stakeholders. • Disregard existing policy requirements, such as security and privacy. • Ignore regulatory mandates. • Assume vendors (hardware, software, middleware or any other) have thought through your particular usage or security requirements. • Disregard device-specific attacks or vulnerabilities. • Discount privacy considerations or "hide" data that are collected/transmitted from end users.



CONCLUSION

Internet of Things can be a powerful concept. However, like any new technology deployment, risk must be evaluated holistically to ensure that business value is maximized while risk is minimized. This evaluation should be a collaborative effort among all stakeholders, including business teams, compliance, operations, information security, privacy and all other pertinent areas.

IoT has the potential to be huge and is already changing the way people live, work and play. Its advantages are numerous and can be life changing and lifesaving. IoT is in its very early stages and already ubiquitous, although most people are unaware. Much more is still to come. The wave of changes from IoT also brings with it new and more complex risk and problems. With the adoption of any change, it is crucial to be well prepared. IoT can be a powerful concept, but making use of it responsibly requires forward thinking, appropriate planning and open dialog.