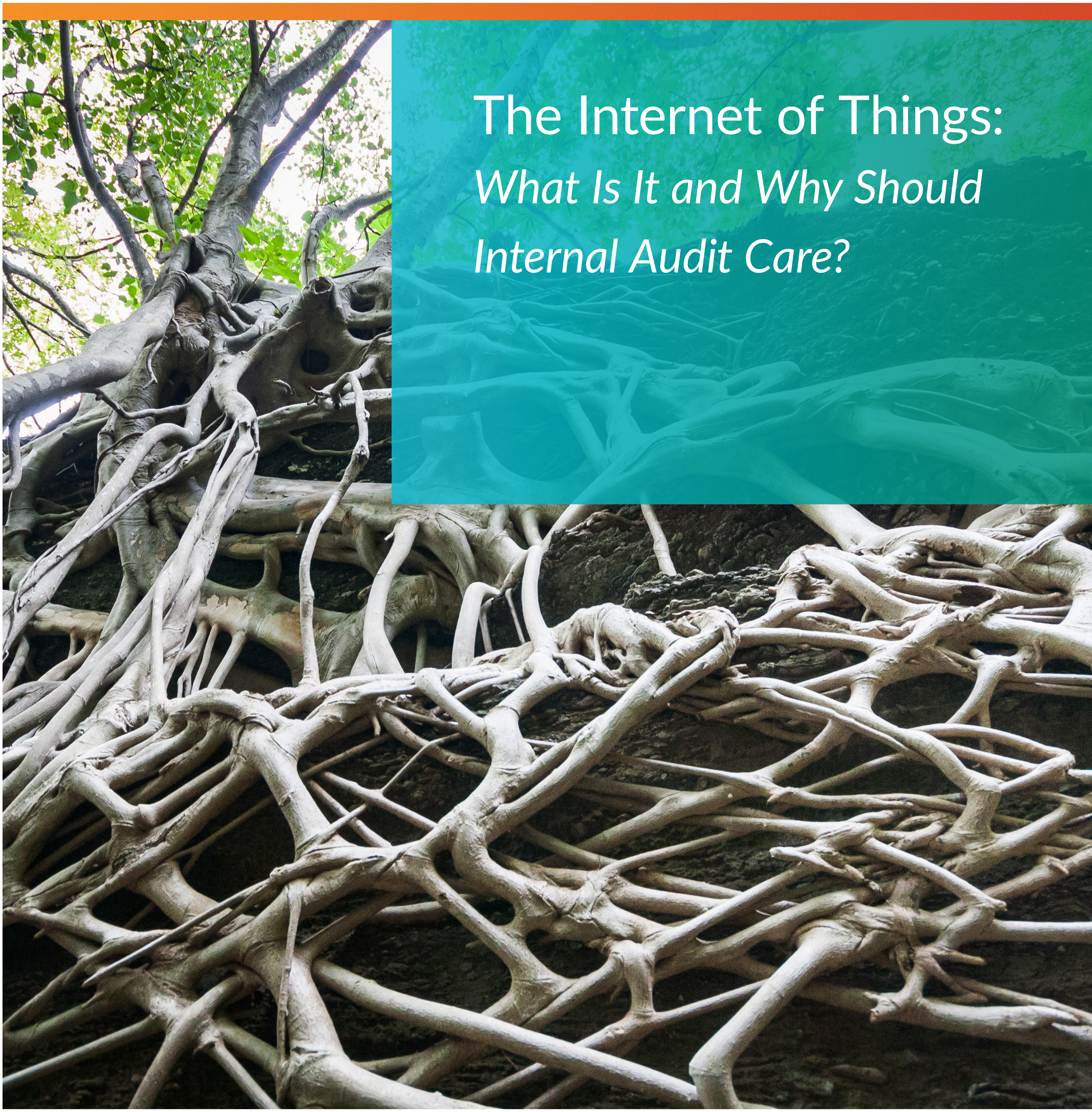
protiviti®

Face the Future with Confidence

The Internet of Things: *What Is It and Why Should Internal Audit Care?*



Internal Audit, Risk, Business & Technology Consulting

Executive Summary

The Internet of Things (IoT) is evolving rapidly, with a wide array of "smart" systems, mobile apps, personal communication devices and other platforms already networked together. Research firm IDC projects that there will be 30 billion connected things by 2020.[1] And to paraphrase *Forbes* in defining the IoT, if something can be connected to the internet, it's only a matter of time before it will be.[2]

In an increasingly digital world, internal auditors need to be keen observers of all technological change that could potentially impact the business and its risk profile — a conclusion drawn from Protiviti's latest round of interviews for our most recent edition of *Internal Auditing Around the World*.[3] The IoT is exactly that type of disruptive change. Internal auditors therefore must be prepared to quickly identify the signs of IoT change and any related implications to the business model or strategic objectives of the organization.

As the IoT expands and the world becomes more interconnected — and devices in the IoT collect more and richer data from objects, machines and people — organizations across industries will face new opportunities and risks. Privacy issues, hacking and other cybercrime, and the potential for catastrophic business failure due to heavy reliance on the internet are examples of risks that internal auditors and their organizations will need to monitor closely in the IoT landscape.

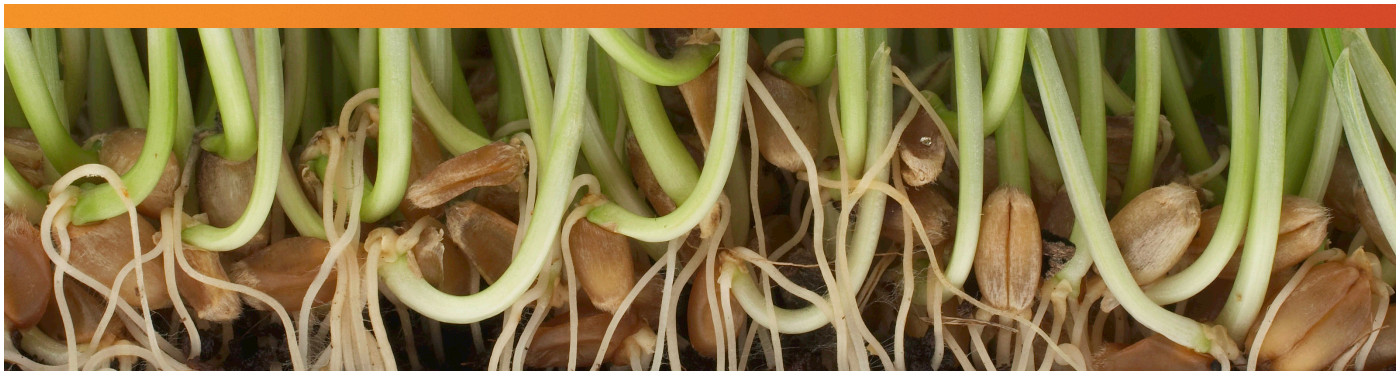
This white paper discusses the emerging IoT and provides an overview of IoT opportunities and risks for businesses, including how the IoT potentially could help organizations mitigate risk. More importantly, it presents a number of questions that internal auditors should seek to answer in collaboration with management and boards of directors so that the business is well-positioned to take advantage of IoT technologies and capabilities and operate in a future "Internet of Everything" world.[4]

[1] "Connecting the IoT: The Road to Success," IDC: http://www.idc.com/infographics/IoT.

[2] "A Simple Explanation of The Internet of Things," by Jacob Morgan, *Forbes*, May 2014: http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#3def0f206828.

[3] "Internal Auditing Around the World," Protiviti, July 2016: https://www.protiviti.com/US-en/insights/internal-auditing-around-world.

[4] Cisco defines the IoE as "the intelligent connection of people, data, process and things." For more information, see the "Internet of Everything FAQ," Cisco: http://ioeassessment.cisco.com/learn/ioe-faq.



What Is the IoT?

The IoT is an environment in which "things" — objects, animals or people — are provided with unique identifiers on the internet and the ability to transfer data over a network without the need for human-to-human or human-to-computer interaction. The IoT has evolved from the convergence of wireless technologies, micro-electromechanical systems (MEMS) and the internet.

A major enabler of the IoT is IPv6, a communications protocol that provides an identification and location system for computers on networks and routes traffic across the internet. IPv6 was developed in 1999 to replace IPv4, as the more than 4 billion IPv4 IP addresses had essentially been exhausted.

IPv6 allows for 340 undecillion addresses. To put that massive number in context, it means every single atom on the surface of the Earth could be assigned an IP address — and, according to some, there would still be enough addresses remaining for another 100 Earths.[5]

In short, IPv6 presents an opportunity to make everything connectable. However, the IoT isn't just about connecting and gathering data from things like wireless smart devices and systems — a category that today includes everything from mobile phones and personal fitness trackers to home appliances, buildings and cars. The IoT is a critical technology transition that is essential to the development of a much bigger and deeply interconnected network, the Internet of Everything, or IoE, and to advancing and supporting digital business.

The key components of the IoT are:

1. **Data Collection:** At the core of the IoT are sensors and actuators that collect, transmit, store and act on data at the source. These devices range in size and capability. Some have minimal operating systems (OS). Others have robust embedded OS, including Microsoft Windows and Google Android.
2. **Connectivity:** The IoT cannot exist without the interconnection of devices and sensors. Bluetooth, near-field communication (NFC), Wi-Fi and cellular are familiar technologies for enabling connectivity. On the horizon is NB-IoT, a narrowband IoT protocol based on current cellular technology. It will support quality of service (QoS), as well as the critical success

[5] "Are there enough IPv6 addresses for every atom on the surface of the Earth?," StackExchange: http://skeptics.stackexchange.com/questions/22501/are-there-enough-ipv6-addresses-for-every-atom-on-the-surface-of-the-earth.

factor for any IoT implementation: a low-power wide area network. NB-IoT will also offer security — something that many current platforms and protocols for connectivity lack.

3. **People and processes:** As the number of connected devices grows, so too will the need for new methods of managing, interpreting and acting on the massive volumes of data being generated and collected by those devices. The type and amount of data being collected holds potentially powerful insights. The value proposition behind the IoT is based on the idea that action will be taken based on this data. In some cases, the action may be immediate; in others, data may accumulate over time to provide trending, metrics across populations, or predictive analytics. This is where people, processes and risk management come into play. Processes must be designed to ensure data-driven actions are well thought out, consistent, and aligned with strategic objectives and risk management protocols. The real promise of the IoT lies in this third component. The integration of people and processes in the IoT is required to help the IoE evolve.

Real-World Example: The "Connected" Cow

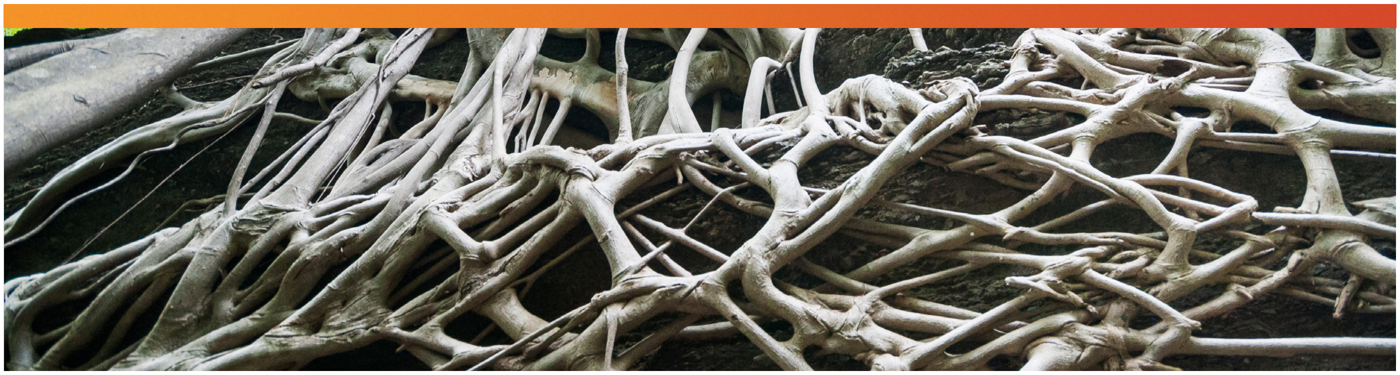
There are already compelling examples of how the use of internet-connected sensors by businesses and industries can generate insights that create real value. One is the "connected" cow.

To help cattle ranchers increase the success rate of artificial insemination in cows, Japanese electronics firm Fujitsu developed a system of internet-connected pedometers that count the cows' steps. Cattle breeders know that when cows significantly increase their walking activity, it's a sign that they are fertile. This helps to pinpoint the very short window of time when the cow is fertile — a period that often occurs at night, so breeders miss it.[6]

Fujitsu reports that the success rate for a single artificial insemination attempt for a cow wearing its pedometer is nearly double the rate for cows that aren't connected. The "connected cow and farm" market, which includes other "cow applications" like automated milking and feeding, is expected to grow to a $10.1 billion industry in 2021, from $1.2 billion today.[7]

[6] "The Smart Home Is a Fantasy, but 'Smart Cows' Are Already Real," by Arik Hesseldahl, Recode, April 2016: http://www.recode.net/2016/4/9/11586010/iot-internet-ofthings-cows.

[7] *"Connected Cow and Farm Market (2016 — 2021)," Arcluster, 2016:* https://arcluster.com/research/connected-cow-market-2016-2021/.



Why Is the IoT Important for Internal Audit?

Why, specifically, should internal audit pay close attention to the IoT? The emerging IoT presents both a new challenge for businesses (we discuss the risks of IoT further in this paper), and an important opportunity for internal auditors to help their businesses stay ahead of the "disruption curve" and meet the challenge confidently. Whereas disruptive innovations may have once taken a decade or more to transform an industry, the elapsed time frame to disruption has compressed considerably in recent years — and will continue to accelerate as the IoT, and the IoE, evolve. Monitoring this emerging risk is fully in the scope of internal audit's responsibilities — "identify known and emerging risk areas" was rated the number one in-scope task, beyond assurance, by 85 percent of North American respondents in the Global Internal Audit Common Body of Knowledge stakeholder report.[8]

Internal auditors recognize a need to improve their knowledge and understanding of the IoT, according to findings in Protiviti's 2016 Internal Audit Capabilities and Needs Survey. The IoT ranked fifth in the "General Technical Knowledge" category as a "need to improve" priority for internal audit, with an overall competency score of 2.6 (5 being the highest level of competency).[9] This was the first time the IoT was included in the survey as an area of technical knowledge; that internal auditors ranked it as a top area for improvement underscores just how quickly the IoT is evolving and becoming a top-of-mind issue for businesses across industries.

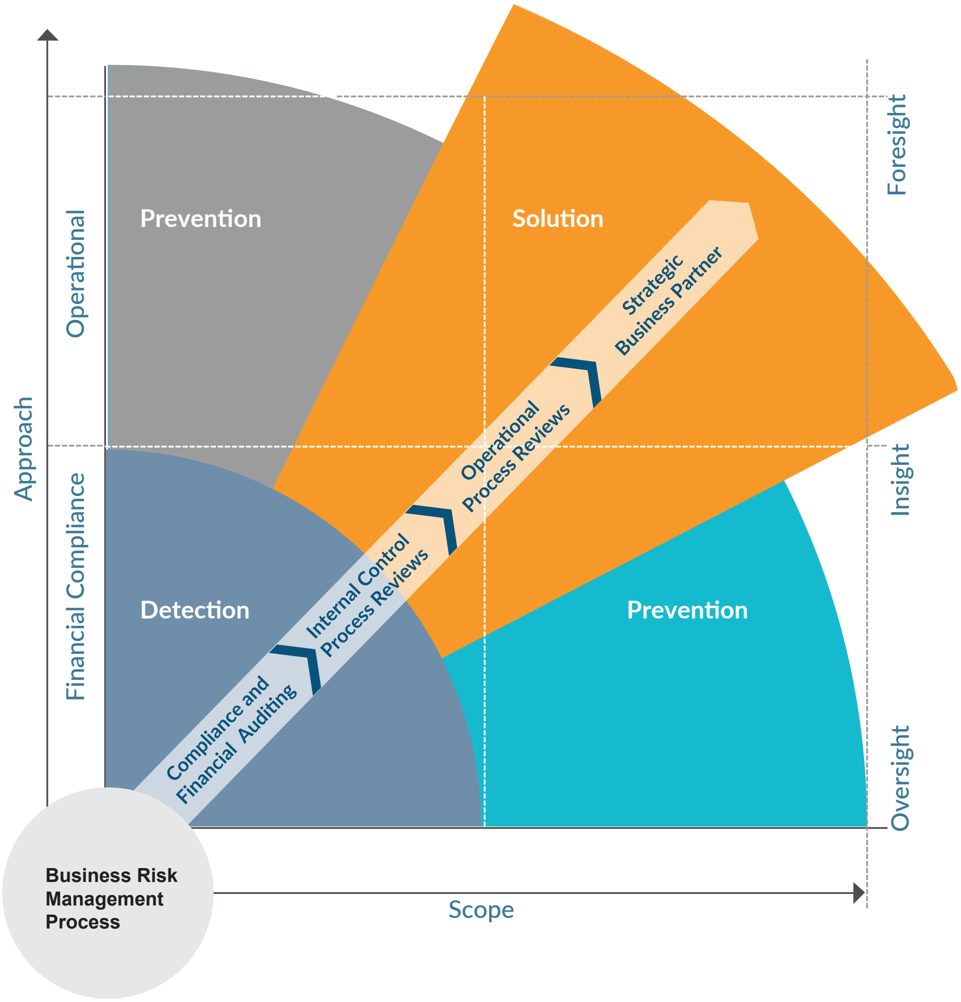
One compelling reason for internal auditors to improve their IoT competency is to meet the call for a more strategic business partner role in their companies. Stakeholders expressed approval, and need, for this kind of role in The Institute of Internal Auditors' Common Body of Knowledge (CBOK) Voice of the Customer Stakeholder report.[10] Boards and C-level executives specifically stated that while the assurance role of internal audit is assumed and remains primary, internal audit's active participation in evaluating strategic risks is also highly desirable, provided the competency and capacity exist. In such a role, internal audit should become an advocate for IoT opportunities for the business while also assessing the risks it might bring. Internal audit can also help the business explore ways to mitigate the risks of the IoT, discussed in more detail later in this paper.

[8] "Relationships and Risk: Insights from Stakeholders in North America," The IIA: https://global.theiia.org/iiarf/Pages/CBOK-Research-Resource-Library-Stakeholder-Study.aspx.

[9] *2016 Internal Audit Capabilities and Needs Survey Report*, Protiviti, 2016: http://www.protiviti.com/en-US/Pages/IA-Capabilities-and-Needs-Survey.aspx.

[10] "Voice of the Customer: Stakeholders' Messages for Internal Audit," The IIA: http://theiia.mkt5790.com/CBOK_2015_Voice_of_the_Customer/?webSyncID=d94260b3-9025-d0ca-a42a-3166784abeb5&sessio:nGUID=b81e8927-4cad-137a-95dd-8216d5143661.

Chart 1: The Internal Audit Continuum


Approach
Operational
Financial Compliance
Prevention
Solution
Detection
Prevention
Strategic Business Partner
Operational Process Reviews
Internal Control Process Reviews
Compliance and Financial Auditing
Foresight
Insight
Oversight
Business Risk Management Process
Scope

DETECTION	PREVENTION	PREVENTION	SOLUTION
• Report problems, recommend solutions • Check compliance against established policy	• Benchmark performance of operational processes against best practices	• Actively promote compliance with internal controls • Assist finance and operations in enhancing internal controls	• Enterprisewide risk management • Facilitate positive change and internal best practices

With regard to the IoT, internal auditors need to focus on providing value at the "solution" level of the continuum by becoming facilitators of positive change and internal best practices around this new risk. Staying abreast of thought leadership, meeting with peers at other organizations to evaluate their IoT exposure, and facilitating IoT-related discussions with senior management and the board are just some ways internal auditors can help the business develop an effective enterprisewide risk management approach for the IoT. See the last section of this paper for a list of IoT-related questions and discussion topics internal auditors can use to spur conversation with boards and executive management.

What Opportunities Does the IOT Present?

IDC projects a revenue of $1.7 trillion for the IoT ecosystem in 2020.[11] So, in addition to understanding key IoT-related risks, discussed later in this paper, internal auditors must recognize opportunities the IoT presents to the business, remembering that failure to take advantage of the IoT opportunity is a risk in and of itself. These opportunities may be unexpected, and previously unimagined. The example of the "connected cow" discussed earlier shows how the IoT can bring positive disruption and innovation to a very traditional and non-digital industry — one that was not an obvious candidate to employ IoT technology in its processes.

Here is a sampling of IoT applications for various industries:

- **Consumer technology:** Smartphones and tablets, personal activity trackers and other wearables, smart home appliances and smart thermostats are already widely available and in use. Amazon Dash, the Wi-Fi connected device that lets users reorder their favorite product through Amazon with the press of a button, was not only adopted literally overnight, but was soon hacked by users to enable it to do other things, such as order a pizza or call an Uber. Through risk exposure, came an opportunity to adapt and improve. Amazon is now offering a configurable Dash Button that consumers can use to link to a host of IoT-enabled services.[12] This is just one example of how consumers themselves are driving the market for IoT-enabled technology, and the untapped potential there.
- **Electricity and utilities:** Smart grid technology is enabling distribution intelligence and providing a two-way opportunity to send electricity back to the grid, particularly during peak usage periods. Automatic detection of outages by smart meters can lead to faster repairs. Other IoT advancements, such as the ability to schedule smart home appliances to run during lower usage periods, are helping to reduce consumers' energy consumption.
- **Oil and gas:** IoT technology is helping businesses in this sector to increase efficiency through advancements in pressure, temperature and flow rate monitoring, as well as in the measurement of handoffs, volume and pipeline integrity. Sensors in the field can enable smart forecasting and help companies optimize well production. By becoming "digital technology companies," oil and

[11] "Connecting the IoT: The Road to Success," IDC: http://www.idc.com/infographics/IoT.

[12] "Amazon Expands Dash Button Lineup With Programmable IoT Button," by Megan Crouse, *Manufacturing Net*, May 13, 2016: http://www.manufacturing.net/news/2016/05/amazon-expands-dash-button-lineup-programmable-iot-button.

gas companies can further improve rig uptime and oil recovery rates, reduce oil spillage, boost employee productivity, shrink costs, and more. For example, a U.S. oilfield services company that employs advanced drilling techniques, which are service-intensive and require specific expertise to operate and maintain, is now using collaborative technologies, such as unified communications, to provide on-demand expert guidance and faster problem resolution, leading to reduced costs and downtime for the business.[13]

- **Insurance:** Geospatial applications can alert drivers to potential severe weather events (e.g., hailstorms), helping them to avoid vehicle damage and the need to file an insurance claim. Environmental sensors in workplaces and other buildings and facilities are already being used to detect temperature, smoke, toxic fumes, mold, earthquake motion, and more.[14]
- **Automotive:** Autonomous cars can help reduce traffic and increase road safety. Road sensors can alert drivers of sensor-equipped cars to rain, frost and ice. Some road sensors also can measure the thickness of ice, analyze the makeup of chemicals on the road surface that have been used for deicing, and then report back to departments of transportation so they can improve their application of those chemicals.
- **Medical:** Patient care is an obvious application for IoT technologies — from scheduling appointments to monitoring conditions like diabetes to ensuring the proper dosage of medicine has been administered. Medical device downtime also can be reduced through remote monitoring and support. IoT technology is already helping hospitals optimize the supply chain while reducing risk: Supply cabinets with built-in RFID readers with antennas can record which staff members have accessed the inventory, what they took and when.

[13] "A New Reality for Oil & Gas: Complex Market Dynamics Create Urgent Need for Digital Transformation," by Robert Moriarty, Kathy O'Connell, Nicolaas Smit, Andy Noronha and Joel Barbier, Cisco, April 2015: http://www.cisco.com/c/dam/en_us/solutions/industries/energy/docs/OilGasDigitalTransformationWhitePaper.pdf.

[14] "5 Ways the IoT Will Transform the Insurance Industry," by Robert Reiss, *Forbes*, Feb. 1, 2016: http://www.forbes.com/sites/robertreiss/2016/02/01/5-ways-the-iot-will-transform-the-insurance-industry/#7b2bca3d72cb.

The Risks of IoT

Considering the potential opportunities that the IoT presents, perhaps the most significant IoT-related risk for businesses is not moving fast enough, or at all, to develop and leverage new IoT technologies and applications. However, to succeed in the IoT world, organizations must also be aware of and closely monitor their risk exposure in areas such as privacy, business continuity and security.

Privacy

Data is already being collected in more ways than ever before, from more devices and apps, and at an accelerating rate. Much of this data can be associated with specific groups of users, and often, tied to unique individuals or objects. In a more interconnected environment like the IoT, it stands to reason that many more devices will be capturing user data for analysis — and that data will be much richer.

The richer the data, the more valuable it will be to businesses — and to the hacker economy. Malicious actors look to steal more than just users' financial data; they also want email addresses, dates of birth, telephone numbers, account passwords, security questions, and more so they can commit fraud and other crimes. This is exactly the type of personal data that was compromised in a major hacking campaign launched in 2014 that targeted more than half a billion active users of Yahoo.[15]

Businesses developing and using applications and devices within the IoT must be aware of how the data they are collecting, analyzing and sharing impacts user privacy. They must understand the full data life cycle and where all the risks exist throughout it. They also must implement appropriate safeguards — administrative, physical and technical — to reduce known risks to acceptable levels. The following aspects of data should all be considered:

- **Data Collection.** Understand the data that is being collected — some data is clearly more sensitive than other data. Unique identifiers, such as uniquely personal information, increase the risk profile.
- **Data Ownership.** Understand who owns the data once it is gathered. Determining data ownership is often not straightforward; a starting point might be with the question "Who is the entity/individual who would answer to ramifications of data disclosure, were it to occur?"
- **Custodial Responsibility.** In many cases, the data owner is not directly responsible for safeguarding the data, but is ultimately responsible for any exposures. Programs to identify and monitor third-party providers who manage sensitive data are critical on a number of fronts, including the IoT.

[15] "Yahoo Security Head Discusses Worst Hack in History," by Jeff John Roberts, *Fortune*, Sept. 2016: http://fortune.com/2016/09/28/yahoo-breach-bob-lord/.

- **Data Retention and Disclosure.** Retention standards for IoT-type data may not be considered, or may be considered differently than for other types of data. Processes around the disclosure of data, even, or especially, to law enforcement, is a hot topic. Mobile phones often serve as a hub for interconnected devices, and contain a treasure trove of data, including locations, call logs, search results, etc. Clear policies in that regard can help avoid ambiguity and lawsuits.

Risk Mitigation: Identity Management

In an IoT world, the use of biometrics can transform identity management. It's already happening. For instance, financial institutions are providing users the ability to log in through fingerprint, voice or facial recognition. Software company Nymi has developed a new wristband that can verify a user's identity through an EKG. Touch ID, introduced by Apple, adds biometric capabilities to its mobile devices. Several large banks are already using the technology to identify users of their mobile apps.

Interruption of Service

With wide adoption, the IoT can create new, often unexpected vulnerabilities where there were none before. Businesses or industries with heavy reliance on information produced by IoT devices will need to pay more attention than others to IoT availability. These businesses can suffer an interruption of service if the connected devices they have come to rely on malfunction, or become disconnected or damaged, whether intentionally or not. This is especially critical for industries where the safety of consumers, employees, or patients is at stake, such as oil and gas, or healthcare.

Distributed Denial of Service (DDoS) Attacks

DDoS attacks, in which attackers flood the bandwidth or resources of a targeted system such as a web server in order to "take down" an online service (make it unavailable to users), is a risk that is increased significantly by the IoT. In fact, IoT-related DDoS attacks are already making headlines. Just recently, malware-infected components used by a Chinese electronics manufacturer played a role in a massive DDoS attack that slowed or completely shut down major websites in the U.S.[16]

Prior to that, in September 2016, French web hosting firm OVH was hit with two concurrent DDoS attacks due to "botnets made up of compromised IoT devices capable of launching [DDoS] attacks of unprecedented scale."[17] These DDoS attacks followed a massive campaign that targeted krebsonsecurity.com, the website of cybersecurity journalist Brian Krebs, earlier that same month.[18]

Top 10 IoT Risks

The Open Web Application Security Project (OWASP) helps manufacturers, developers and consumers to better understand IoT security issues so that they can make better security decisions when building, deploying or assessing IoT technology.[19] Below is OWASP's list of the top 10 IoT risks, which organizations can use to assess their specific IoT risks:

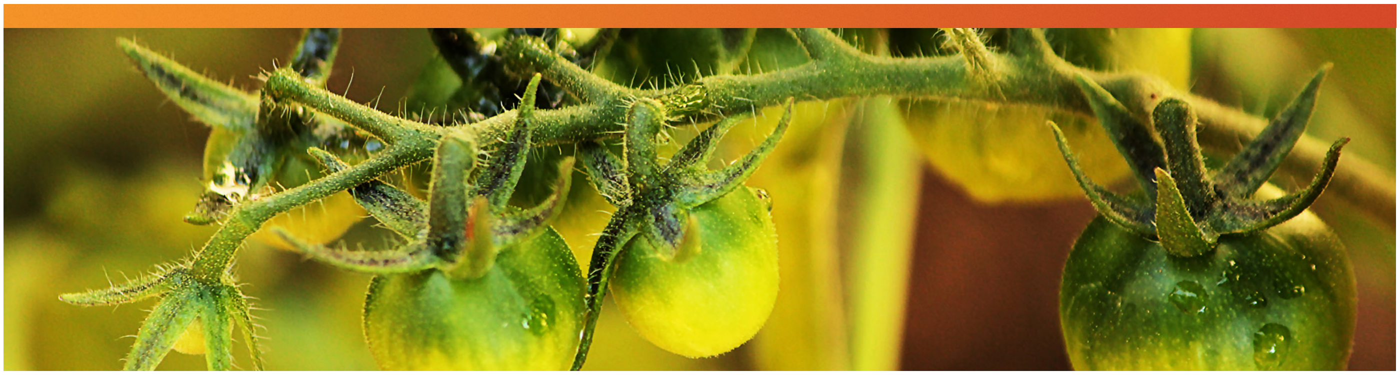
1. Insecure web interface
2. Insufficient authentication/authorization
3. Insecure network services
4. Lack of transport encryption/integrity verification
5. Privacy concerns
6. Insecure cloud interface
7. Insecure mobile interface
8. Insufficient security configurability
9. Insecure software/firmware
10. Poor physical security

[16] "Chinese Firm Admits Its Hacked Products Were Behind Friday's DDoS Attack," by Michael Kan, *Computerworld*, Oct. 23, 2016: http://www.computerworld.com/article/3134097/security/chinese-firm-admits-its-hacked-products-were-behind-fridays-ddos-attack.html.

[17] "Armies of Hacked IoT Devices Launch Unprecedented DDoS Attacks," by Lucian Constantin, *InfoWorld*, Sept. 2016: http://www.infoworld.com/article/3124215/security/armies-of-hacked-iot-devices-launch-unprecedented-ddos-attacks.html.

[18] "KrebsOnSecurity Hit With Record DDoS," KrebsonSecurity blog, Sept. 2016: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/.

[19] For more details on OWASP's IoT Project, visit: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project.



Facing the Future

The IoT is not just a "What if?" scenario for the future; it's already here, and growing every day. Internal auditors need to be on the front lines along with management, helping them prepare the organization to meet new challenges and risks resulting from this wave of disruptive technological change.

The good news is that many of the strategies for managing the challenge of the IoT already exist and are deployed in managing other security and operational activities of the organization. The main difference for internal audit may be in the reporting/aggregation of risks because of the volume and geographic dispersion of the IoT.

With that in mind, internal audit, in collaboration with the business, should seek to answer these questions in order to develop a better understanding of the IOT, and raise awareness throughout the organization about its potential opportunities and risks:

- **How is the IoT deployed in our organization today?** Who owns it, or its components? What is the potential IoT inventory in the organization? For example, is IoT technology part of the products that the business sells, is it installed internally to manage processes, or are third-party vendors deploying IoT technology within the company's solutions?
- **Have we considered the risks associated with our IoT presence?** Have those risks been quantified or controlled? Is the business actively including its IoT inventory in broader risk assessments? Does the business consider the IoT when applying data and privacy policies and practices and evaluating security?
- **Do we know what data is collected, stored and analyzed?** Have we assessed related potential legal, privacy and security implications? For example, if IoT technology is within the company's solution offerings, is the business certain that it is in compliance with customers' agreements about disclosing the potential capture and sharing of information?
- **Do we have contingency plans for internet-connected things that are hijacked or modified for unintended purposes?** Has the business evaluated the use of IoT technology in its processes, and what the potential impact would be if something was, or had to be, taken offline? Is the IoT considered in business continuity management plans? And if the IoT is that important to the business, what procedures are in place for recovery in the event of a catastrophic failure?

- **To what extent are third parties acting on our behalf with regard to IoT technology?** Do we have appropriate processes and service-level agreements (SLAs) in place to monitor them appropriately? As we continue to push out our business processes to other service providers, are those providers using IoT technologies on our behalf? If so, are we monitoring their usage? Are we aware of any components from an IoT perspective that they may have added? Also, are we monitoring the data that we are capturing and delivering through our third-party service providers?
- **What role does the IoT play in our current strategy as an organization?** How are we measuring achievement related to any goals associated with our strategic objectives? Do we actually have an IoT strategy? Has the board evaluated the potential impact of the IoT to the business? What about our competitors? Where do they stand?
- **What is the risk of not considering or leveraging IoT possibilities?** What is the risk if we ignore the IoT? What if we don't take full advantage of data analytics capabilities in the IoT? Do we risk not meeting our strategic objectives simply because we failed to recognize the evolution of a disrupted landscape?

That last question is particularly important for internal auditors and their organizations to answer. Different businesses use, benefit from or are affected by the IoT in different ways. To ensure they are meeting their responsibilities, internal auditors must evaluate not only the risks posed by the IoT, but also the risk of failing to act to take advantage of the IoT, in the context of the business, its competitors and its industry.

ABOUT PROTIVITI

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of Fortune 1000® and 35 percent of Fortune Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

CONTACTS

Brian Christensen
+1.602.273.8020
brian.christensen@protiviti.com

David Brand
+1.404.443.8204
david.brand@protiviti.com

Anthony Samer
+1.415.402.3627
anthony.samer@protiviti.com

Jordan Reed
+1.713.314.4955
jordan.reed@protiviti.com

Jonathan Bronson
+1.213.327.1308
jonathan.bronson@protiviti.com

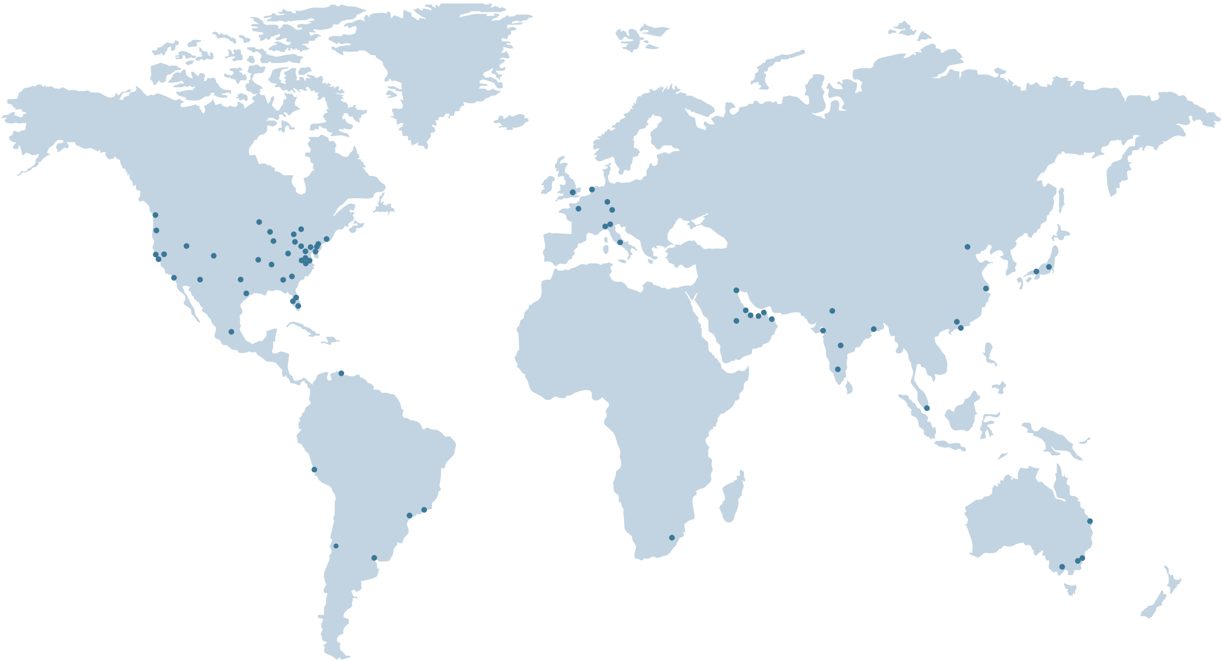
Anthony Chalker
+1.404.926.4314
anthony.chalker@protiviti.com

James Armetta
+1.212.399.8606
james.armetta@protiviti.com

Gordon Braun
+1.913.661.7406
gordon.braun@protiviti.com

Mark Peters
+44.20.7389.0413
mark.peters@protiviti.co.uk

Chris Grant
+61.2.8220.9544
chris.grant@protiviti.com.au



THE AMERICAS

UNITED STATES
Alexandria
Atlanta
Baltimore
Boston
Charlotte
Chicago
Cincinnati
Cleveland
Dallas
Fort Lauderdale
Houston
Kansas City
Los Angeles
Milwaukee
Minneapolis
New York
Orlando
Philadelphia
Phoenix
Pittsburgh
Portland
Richmond
Sacramento
Salt Lake City
San Francisco
San Jose
Seattle
Stamford
St. Louis
Tampa
Washington, D.C.
Winchester
Woodbridge

ARGENTINA*
Buenos Aires

BRAZIL*
Rio de Janeiro
Sao Paulo

CANADA
Kitchener-Waterloo
Toronto

CHILE*
Santiago

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

EUROPE MIDDLE EAST AFRICA

FRANCE
Paris

GERMANY
Frankfurt
Munich

ITALY
Milan
Rome
Turin

NETHERLANDS
Amsterdam

UNITED KINGDOM
London

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

SAUDI ARABIA*
Riyadh

SOUTH AFRICA*
Johannesburg

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

ASIA-PACIFIC

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

INDIA*
Bangalore
Hyderabad
Kolkata
Mumbai
New Delhi

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

*MEMBER FIRM

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.