Internet of Things

Move Past the Rhetoric and Focus on Success

Innovate Forward

Booz | Allen | Hamilton

Move Past the Rhetoric and Focus on Success

THE TERM “INTERNET OF THINGS” (IOT) IS UBIQUITOUS IN TODAY’S TECHNOLOGY LITERATURE. WE HEAR IT USED IN CONJUNCTION WITH PHRASES LIKE “UNLOCKING HIDDEN VALUE” OR “INTEGRATING DATA TO DRIVE EFFICIENCIES.” THESE PHRASES, WHILE HONEST IN SPIRIT, OFTEN LEAVE THE IMPRESSION THAT IOT IS EASY, QUICK, AND CHEAP. WE’RE AT A PLACE WHERE THE MARKETING MATERIALS AND LARGER IOT INDUSTRY CONVERSATION SOUNDS SIMILAR TO WHAT WE HEARD ABOUT THE CLOUD A FEW YEARS AGO.

But just as the Cloud is delivering on its promises, we similarly believe that IoT will deliver as well, if you plan appropriately. Embracing this fast-evolving idea is only the start. Education during the planning phases and staying in step with the industry as IoT evolves will ensure success. To maximize your efforts as you begin to take on what is only the beginning of IoT, we will explain the immediate and long-term value of IoT, break down undervalued business consequences of IoT, and introduce a blueprint for building future success.

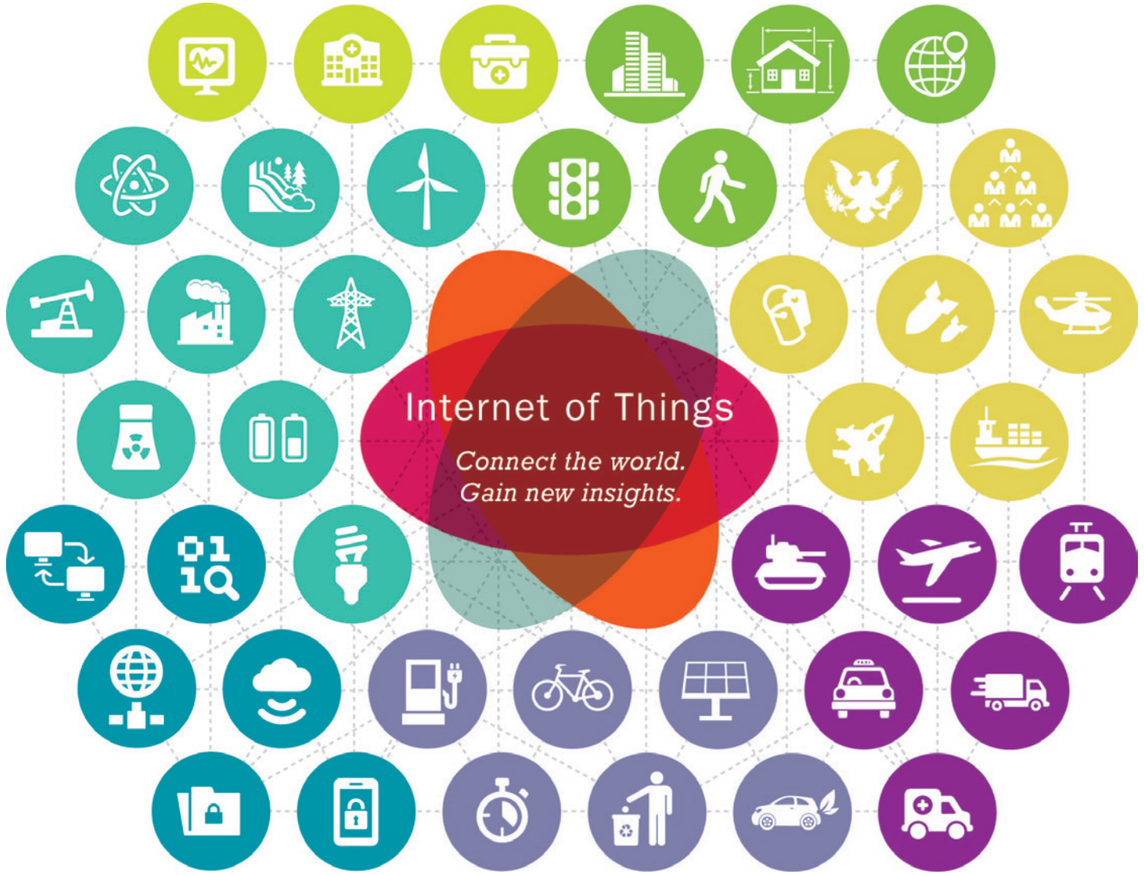
What is the Internet of Things? An explanation and brief history.

IoT is a concept that describes a state where everyday physical objects and devices—“things”— are connected to the Internet. These “things” are everywhere, and include modes of transport such as cars and airplanes, utilities like traffic lights and gas pipes, and even wearable fitness trackers. IoT goes beyond simply connecting objects to the Internet; it enables devices to intelligently self-identify and communicate with other devices. This creates a new model of information-sharing among people, facilitated by our devices.

Imagine someone driving along a highway that’s marked by digital signs with embedded sensors. The sensors detect black ice and send automatic messages to incoming vehicles to slow down. This sensor-driven action prevents accidents, reduces the potential for injury and death, cuts emergency service costs, and decreases overall traffic congestion. IoT brings the physical world surrounding us to life within a digital world, as part of a system to help people, communities, and organizations unearth and maximize untapped potential.

Over the past decade, the explosion of broadband Internet, cloud maturity, IPv6 protocols, decreased costs, and increased network reliability have collectively fueled the drive for new capabilities that once existed only in isolation. Global technology is now moving towards becoming hyper-connected and intelligent. By designing and engineering software, organizations will be able to empower traditionally “dumb” objects or things—bridges, water mains, tires, and heating ventilation and air conditioning (HVAC) units—with a mash-up of embedded sensors that connect and secure existing infrastructure without demolishing it. Equipping these everyday objects to be IoT-enabled will allow organizations to maximize existing investments, securely transmit and analyze data, and provide near-real-time decision support experiences that will change how business is done.

“IoT is an interconnected set of devices, sensors and objects that merge the physical with the digital world.”



IoT technology exists today—it’s not some far-flung idea from the future. Whether it’s in transportation, energy, health, or the military, industries are already benefiting from IoT. As you read through this, we’ve provided four vignettes that bring IoT to life and get you to think about it in a new, real way.

IOT CHARACTERISTICS

+ **CONNECTS** the physical world around itself to other things, the Internet, a network, etc.
+ **COMPUTES** by processing the inputs it collects or receives, and making those inputs meaningful to other systems.
+ **COMMUNICATES** with a unique identity on the network, with other things, and the workforce

What You Really Need to Know

SOON, IOT WILL AFFECT YOUR ORGANIZATION IN WAYS THAT ARE HARD TO IMAGINE TODAY. THE PROMISE OF CONNECTING MILLIONS AND BILLIONS OF DEVICES AND "THINGS"— INSTRUMENTED WITH SENSORS, EXCHANGING AND AGGREGATING COLLECTED DATA, AND AUTOMATING TRADITIONALLY MANUAL PROCESSES—OFFERS DISRUPTIVE POTENTIAL. WE OFFER THE FOLLOWING THREE IOT VIEWPOINTS FOR CONSIDERATION AMONG FEDERAL GOVERNMENT LEADERS:

+ **NEW MODELS FOR SECURITY:** The proliferation of IoT devices drastically increases the attack surface and creates attractive, and sometimes easy, targets for attackers. Traditional means of securing networks will no longer suffice as attack risks increase exponentially. We will help you learn how to think about security in an IoT world and new security models.

+ **RETHINKING THE WORKFORCE:** IoT will fundamentally change how organizations conduct business today. Activities that require significant human effort can become automated [like inspecting electrical meters], capabilities or skillsets may become obsolete while others grow in demand [such as data scientists and privacy officers], and employees will require new skills [such as product managers and project managers]. We will highlight some of the key impacts to your workforce to plan for success up front with your IoT deployment.

+ **INTEROPERABILITY IS KEY TO EVERYTHING:** IoT implementations typically contain hundreds of sensors embedded in different "things", connected to gateways and the Cloud, with data flowing back and forth via a communication protocol. If each node within the system "speaks" the same language, then the implementation functions seamlessly. When these nodes don't talk with each other, however, you're left with an Internet of one or some things, rather than an Internet of everything.

SECURITY—TODAY'S MODELS WON'T WORK IN AN IOT WORLD

Securing Devices

Anything connected to the Internet is a potential vulnerability to your organization. Current projections indicate that 85% of all devices are disconnected and unsecure. As new devices are lit up and brought online, new risks surface. Because IoT devices often control physical components, from a car to a pacemaker, security is paramount to ensuring safety and, in some cases, protecting life. Consider how thieves recently used a major department store's networked HVAC unit to hack into payment computer systems and steal 40 million credit card numbers. Security can't be an afterthought when designing devices or systems – it must be integrated into design in ways we've never required before. Embedded security at the chip level can protect systems from logic and execution attacks. Other security design principles include authentication, authorization, encryption, and ease of updates. Achieving an appropriate level of security not only requires new approaches and products (to include secure gateways), but also educated workforces that can partner with manufacturers to implement secure IoT systems.

Securing Data

IoT's potential to solve complex problems is linked to data synergy. IoT devices generate, collect, aggregate, correlate, and share data that must be secured in a number of environments, from the edge to the Cloud. As such, organizations must be proactive in their IoT security approaches. As IoT evolves and new security models and approaches are developed, organizations can apply current security best practices to protect IoT devices and data. Organizations should ensure that IoT devices and systems are implemented to take advantage of existing security protections such as data encryption, firewalls, and access control. Organizations should include IoT devices in their continuous monitoring strategy to maintain ongoing awareness of security threats and

BEYOND HYPE AND INTO REALITY

TRANSPORTATION

IoT Devices Getting You from A to Z, Safely and in Real-Time

Imagine your car transmitting data every second (or faster), talking to vehicles, weather sensors, and traffic lights. Imagine driving without fear—where your car is a constant guardian, not just a vehicle. With IoT, where interconnected devices share critical data, this is all possible.

Connected transit infrastructure enables a safer, more efficient driving experience from start to finish, on and off the road. Before you leave for work, your smart phone displays your car's condition—fuel, tire pressure, and brake pads levels. You're informed of weather conditions and traffic patterns, and offered alternate routes as your car reads weather sensors and smart infrastructure. On the road, your car knows when the lights will turn, and guides you to adjust speed to hit the greens. On the freeway, your car alerts you that there's debris in the right lane, 200 yards ahead, and instructs you to safely change lanes. Cars talk to one another, sharing data through secure, dedicated frequencies, while biometric sensors measure your cognitive abilities behind the wheel. Micro-level, time-specific, highly personalized information that helps you navigate safely.

BEYOND HYPE AND INTO REALITY

OIL & GAS AND ENERGY

How IoT Improves Situational Awareness and Safety

The Internet of Things is opening a new world of information, by automatically gathering and analyzing field data. Automated operations improve safety, reduce costs, and enhance production—without compromising health, environmental standards, or precious resources.

Ted is a safety supervisor at an oil production plant, where situational awareness is paramount. He's responsible for ensuring the protection of the facility's most valuable assets—employees—as well as the safety of their most valuable products—Oil. Ted is equipped with a smart tablet that connects him to a large network of sensors, in-facility and out in the field. As he makes his rounds, Ted tracks his personnel—who are outfitted with wristband devices that transmit their location and biometric vitals—and monitors the plant's numerous machines via digital video cameras. Ted's tablet begins to beep, as a virtual map appears on-screen. A sensor in the plant's east wing has detected a pollutant in the air caused by a machine malfunction, and he has to respond quickly. Ted opens a remote-alarm program, which allows him to geo-locate and notify his workers in the east wing of the plant. The employees' wristbands begin vibrating in unison—the signal to suspend operations and vacate. While Ted focuses on his workers, his device automatically transmits the east wing's environmental data to a central command post, where IoT-networked computers analyze the data, identify the malfunction, and shut down the machine at fault. In less than 90 seconds, the east wing workers have safely exited, and the wing is temporarily locked down while the environment is decontaminated of pollutants. These automated, intelligent IoT operations have kept workers safe and minimized production cost losses, while providing critical advanced analytic information that will improve future plant security and production.

vulnerabilities. IoT is happening now and gaining momentum, and it's bringing disruptive innovation to cyber security.

ADAPTING THE WORKFORCE: DON'T SLEEP ON YOUR MOST VALUABLE ASSET

The way that work gets done is changing, and IoT is, and will continue to be, a big contributor to this evolution. IoT technology offers automated data collection, smart sensors, and intelligent gateways; consequently, administrative and operational tasks will become commodities offered by vendors as incentives to consume their products, platforms, and services. As a result, your workforce will need to adapt in order to realize IoT's organizational value. This may take flight in augmented and expanded skills, adoption of curated networks, crowdsourcing and micro-tasking, managing change with complacent staff, and delivering new experiences and incentives to motivate your workforce to evolve.

Augmented & Expanded Skills

While background computing processes will control more and more traditional human tasks and organizational activities, IoT's real power lies in the way automation stands to expand our own skills and capabilities. According to Business Intelligence, 82% of business are planning to implement IoT solutions by 2017. In a recent survey of Chief Information Officers, 42% of respondents revealed they didn't have the skill sets needed to realize IoT. Challenges exist, in standardizing communication and management among management systems (traditional or cloud-based) and to users. To plan for the future, you will need different skills within your workforce to implement and manage IoT. Embedded hardware and software developers, API developers, cyber security, project managers and product managers will be key to driving businesses forward. Organizations will need trained data scientists to analyze and remove the noise from IoT data, and privacy officers will need to analyze vulnerabilities and evolve business policies. Crowdsourcing information will become the standard, as organizations access top talent on demand to conceive new ideas and solutions.

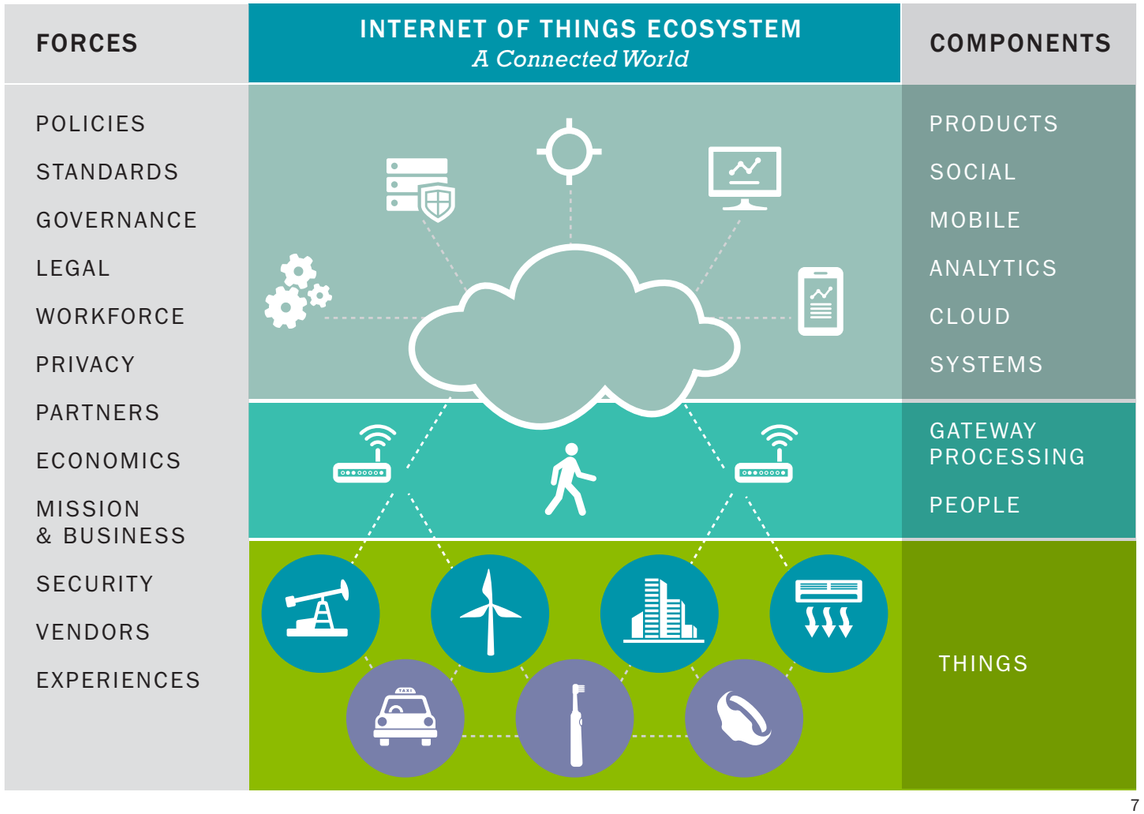
Even Bigger Data

From hospital beds to connected vehicles, and even cows, IoT will continue to bring machines and assets that are critical to business into the connected world. Collecting and sharing data between people and infrastructure means that every object, every interaction, and everything we touch is converted into data. As we begin to decode the world around us, data will enable new insights that can increase efficiency and drive innovation. Cisco predicts that over 50 billion "things" will be connected to the Internet by 2020. As IOT grows and more data is collected automatically, the ability to extract insights from data is critical. There will be an increasing demand for the kind of skills machines can't offer, such as emotional intelligence, creativity, and the ability to deduce meaning from information.

"IoT technology exists today—it's not some far-flung idea from the future. Whether it's in transportation, energy, health, or the military, industries are already benefiting from the IoT. "

A Different Employee Experience

Connected systems within businesses can free up employees' time to focus on high-level, strategic activities. More than that, IoT provides new ways to track information in order to calculate and quantify human behavior more effectively. Happier, healthier, more productive employees who stick around longer—that's the potential benefit of leveraging IoT within the workforce. Organizations that focus too much on bottom-line efficiencies and forced actions may spark backlash, resulting



BEYOND HYPE AND INTO REALITY

MILITARY & DEFENSE

The Future of IoT, from Command Post to Battlefield

Imagine you're a commanding Army officer, preparing your unit for a daylong mission into a sensitive, potentially hostile territory. Mission success depends on your situational awareness, but moreover, on your unit's readiness, safety, and ability to mobilize efficiently. What variables will affect operations today? You approach the line of trucks and Humvees, which are equipped with automatic sensors generating crucial data about your unit's vehicles—fuel levels, tire pressure, engine health. Your secure smartphone, virtually mapping the vehicle line, informs you that a truck in the rear of the formation has a flat tire and requires an oil change. With the push of a button, your device automatically schedules a visit to the vehicle bay for maintenance and pings a unit private responsible for doing this. Meanwhile, wearable biometric sensors attached to each of your unit's soldiers show you vital data in real-time—heart rate, blood pressure, insulin levels—and notify you that a private first class has an unusually high body temperature. Your phone recommends an infirmary visit, and automatically pings your unit corporal to investigate. This mission-critical, condition-based monitoring is smart, efficient, personalized, and relevant. And it's here today, improving mission efficiency and effectiveness. IoT technology makes it feasible, and tomorrow's possibilities are limitless.

in employee distrust. IoT will require training for employees to learn how to control and manage connected, cross-platform devices. Change Management will be critical, but it will also be important to understand new ways to incentivize and motivate employees in genuine ways to meet business objectives.

INTEROPERABILITY: HOW TO GO FROM AN INTERNET OF SOME THINGS TO ALL THINGS

IoT implementation, at its core, is the integration of dozens and up to tens of thousands of devices seamlessly communicating with each other, exchanging information and commands, and revealing insights. However, when devices have different usage scenarios and operating requirements that aren't compatible with other devices, the system can break down. The ability to integrate different elements or nodes within broader systems, or bringing data together to drive insights and improve operations, becomes more complicated and costly. When this occurs, IoT can't reach its potential, and rather than an Internet of everything, you see siloed Internets of some things.

Manufacturers and other key industry players within the IoT industry recognize this problem and the need to work toward a resolution. And there has been progress. Consortiums have been stood-up to advance open standards and open solutions, including the Open Interconnect Consortium (OIC) and Industrial Internet Consortium (IIC). OIC and IIC provide an open opportunity for industry, academia and government to interact and accelerate interoperability with shared architectures, use cases, and taxonomies. They're creating a consistent vocabulary and model to ensure interoperability for current and future devices across an Open IoT Ecosystem. IEEE and the National Institute of Standards and Technology (NIST) have many existing standards that can be applied to IoT, and are exploring new ones as well. These efforts are commendable and an excellent start, but much works remains.

The federal government plays an important role in standard setting. In the summer of 2014, the NIST officially initiated an Internet of Things working group to develop and implement a new cybersecurity framework for IoT - Cyber-Physical System (CPS) Public Working Group (PWG). The NIST CPS PWG has made the foundational step towards an Interoperability Framework defining essential components for data exchange standards both Syntactic (e.g. ensuring that data exchange between systems can be interpreted at the data field level) and Semantic (e.g. shared, common interpretation of data so that the receiving systems can interpret the data). These efforts seek to address issues such as: the identity of the sender; identity of the data; the integrity of the data; and the semantic meaning of the data (including context.) Similarly, the Federal Trade Commission (FTC) held a workshop to discuss IoT-related privacy and security issues. Consider how the federal government can influence and accelerate the development of standards through funding infrastructure projects. Requirements around standards could be tied to the billions of dollars spent annually on infrastructure, thereby creating significant incentives to ensure interoperability through open protocols, data, architectures and solutions.

"IoT implementation, at its core, is the integration of dozens and up to tens of thousands of devices seamlessly communicating with each other, exchanging information and commands, and revealing insights."

BEYOND HYPE AND INTO REALITY

HEALTH

from Homes to Hospitals

Today, IoT devices and advanced data analytics are revolutionizing how doctors connect with and care for patients—at home, in a hospital room, or through remote virtual encounters. Every day, people are wearing personal devices like wristbands to record activities that inform their insurance policies and care instructions. This data, in turn, can inform insurance companies setting health care costs, and help doctors personalize care instructions. Imagine an emergency room visit, where seconds can save lives. EMT staff use IoT devices to access real-time patient data to deliver immediate care, while patient sensors automatically consent to share that data securely. In hospitals, smart IoT-connected kiosks provide real-time data about a patient's medical history, as well as show key information about the room's environment. Doctors no longer need to bring laptops—and the countless contaminants they contain—into hospital rooms to access patient records and make diagnoses. Equipped with smart devices installed in rooms, doctors can visualize patient data that is secured, aggregated, and normalized through advanced analytic algorithms. With the voice command to the kiosk, a doctor can receive real-time vital information, connect with other doctors in the hospital (or wherever they may be), and send blood test orders to labs and prescription orders to pharmacies—all while staying by a patient's bedside. IoT technology is reducing inefficient paper pushing, improving communications, and ultimately increasing time spent with patients.

How do you approach IoT?

IoT is real. It's happening now, and IoT implementations will expand significantly in the future. The benefits are significant—lives saved, money saved, performance increased—and the pathway to realizing these benefits is clearing as costs decrease, technologies expand, and people expect new experiences. As with any new capability or technology, though, it will take time for most people and organizations to get used to IoT, familiarize themselves with it, and start investing and participating in it.

We offer a few key concluding thoughts:

+ **START SMALL.** You may actually have IoT implementations within your organization that you aren't aware of. And if you have any type of health wearable, you are actually already participating in IoT. You don't have to instrument every car, road, and sign to have an Internet of some things.

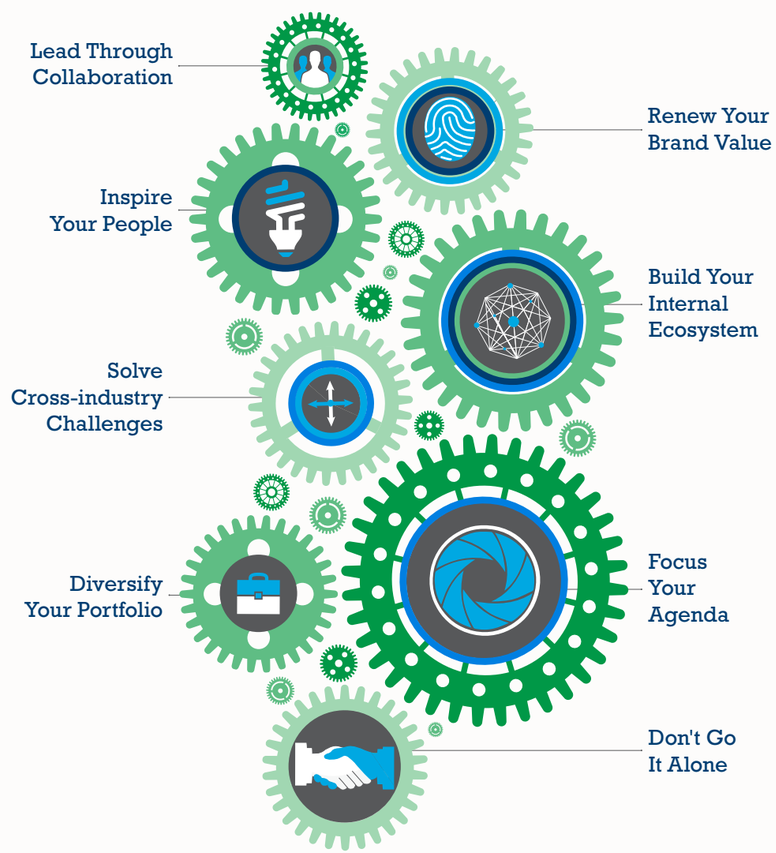
+ **START PLANNING.** Conduct a baseline assessment of opportunities, capabilities, gaps, and barriers for your organization. IoT adoption is a challenge, but you should be prepared. Soon, your customers or constituents will expect it, even though they're not likely to call it "IoT".

+ **FOLLOW A ROAD MAP.** You can't go it alone. Building end-to-end, scalable, and evolving IoT ecosystem requires help. You need partners to bring diverse knowledge, as well as organizational buy-in to discover unknown value. In short, you need to build alliances and build a culture that embraces and harvests new ideas. Fortunately, we have a model to help you do this. It's called our Innovation Blueprint, and it can help your organization build the ecosystem you need to innovate forward and achieve your mission. See it below. Our proven history of solving clients' toughest problems, coupled with our deep technical expertise, can help you achieve the value of IoT and reduce risk and costs, and increase the value of your time today.

Company Background

Booz Allen Hamilton has a proud 100-year history of bringing transformative ideas and impactful solutions to clients through a combination of strategic consulting, emerging technologies and advanced engineering. Our client base includes the defense, intelligence, and civil markets within the U.S. government, as well as major international, corporate, and not-for-profit organizations. As we embark upon our second century, innovation is central to how we deliver value and help solve our clients' most complex challenges. Booz Allen views the Internet of Things (IoT) as the logical, technology-enabled next step to expand our innovation services and help our clients re-envision how they define and address their challenges and opportunities for the future.

THE BOOZ ALLEN INNOVATION BLUEPRINT



About Booz Allen

Booz Allen Hamilton has been at the forefront of strategy and technology consulting for 100 years. Today, the firm provides services primarily to the US government in defense, intelligence, and civil markets, and to major corporations, institutions, and not-for-profit organizations. Booz Allen offers clients deep functional knowledge spanning consulting, analytics, mission operations, technology, and engineering—which it combines with specialized expertise in clients' mission and domain areas to help solve their toughest problems.

Booz Allen is headquartered in McLean, Virginia, employs approximately 23,000 people, and had revenue of $5.76 billion for the 12 months ended March 31, 2013. In 2014, Booz Allen celebrates its 100th anniversary year. To learn more, visit www.boozallen.com. (NYSE: BAH)

DSI-141209-001-1

FOR MORE INFORMATION

Michael Farber
Executive Vice President
Farber_Michael@bah.com

Angela Messer
Executive Vice President
messer_angela@bah.com

Mark Jacobsohn
Senior Vice President
jacobsohn_mark@bah.com

AUTHORS

Craig Swanson
Principal
Swanson_Craig@bah.com

Ron Sokolov
Senior Associate
Sokolov_Ron@bah.com

Booz | Allen | Hamilton