THE INTERNET OF THINGS

WHAT THE IoT MEANS FOR THE PUBLIC SECTOR

Contents

Executive Summary

Let's get one thing right straight out of the gate — no matter that it sounds like a futuristic buzzword, the Internet of Things (IoT) is not a new concept. "Home automation has existed for about 40 years," said Dr. Joseph Ronzio, Health System Specialist and Special Assistant to the Chief Health Technology Officer at the Department of Veterans Affairs.

Some trace IoT's origins as far back as, incredibly, the 1800s. "In 1832, Baron Schilling von Canstatt invented the electromagnetic telegraph. A keyboard with 16 black-and-white keys served as a transmitting device, while six galvanometers with magnetic needles suspended from silk threads acted as the receiving instrument," according to the Atmel blog. "Later that year, Schilling managed a short-distance transmission of signals between two telegraphs in different rooms of his apartment. Not long after, Carl Friedrich Gauss and Wilhelm Weber developed their own code to communicate over a distance of 1,200 meters within Göttingen, Germany."

Looking for a slightly more modern timeline? Forbes created a very detailed history of how we got to IoT as we know it today. It cites various markers along the way, including how members of the "1980s computer science department at Carnegie-Mellon [University] installed micro-switches in the Coke vending machine and connected it to the PDP-10 departmental computer so they could see on their computer screens how many bottles were present in the machine and if they were cold or not."

Jump ahead a decade and Forbes describes how Columbia University's Steven Feiner, Blair MacIntyre and Dorée Seligmann "developed KARMA — Knowledge-based Augmented Reality for Maintenance Assistance. KARMA overlaid wireframe schematics and maintenance instructions on top of whatever was being repaired."

By 2004, Neil Gershenfeld, Raffi Krikorian and Danny Cohen wrote in "The Internet of Things" in Scientific American that: "Giving everyday objects the ability to connect to a data network would have a range of benefits: making it easier for homeowners to configure their lights and switches, reducing the cost and complexity of building construction, assisting with home health care. Many alternative standards currently compete to do just that — a situation reminiscent of the early days of the Internet, when computers and networks came in multiple incompatible types."

For many of us, our first understanding of IoT came in 2012 when "Google began testing its Google Glass prototype, which is a pair of glasses with an optical head-mounted display that displays information collected wirelessly according to the user's specification," notes FierceGovernment.

And finally, the technology publication Venture Beat called 2013 the year of IoT.

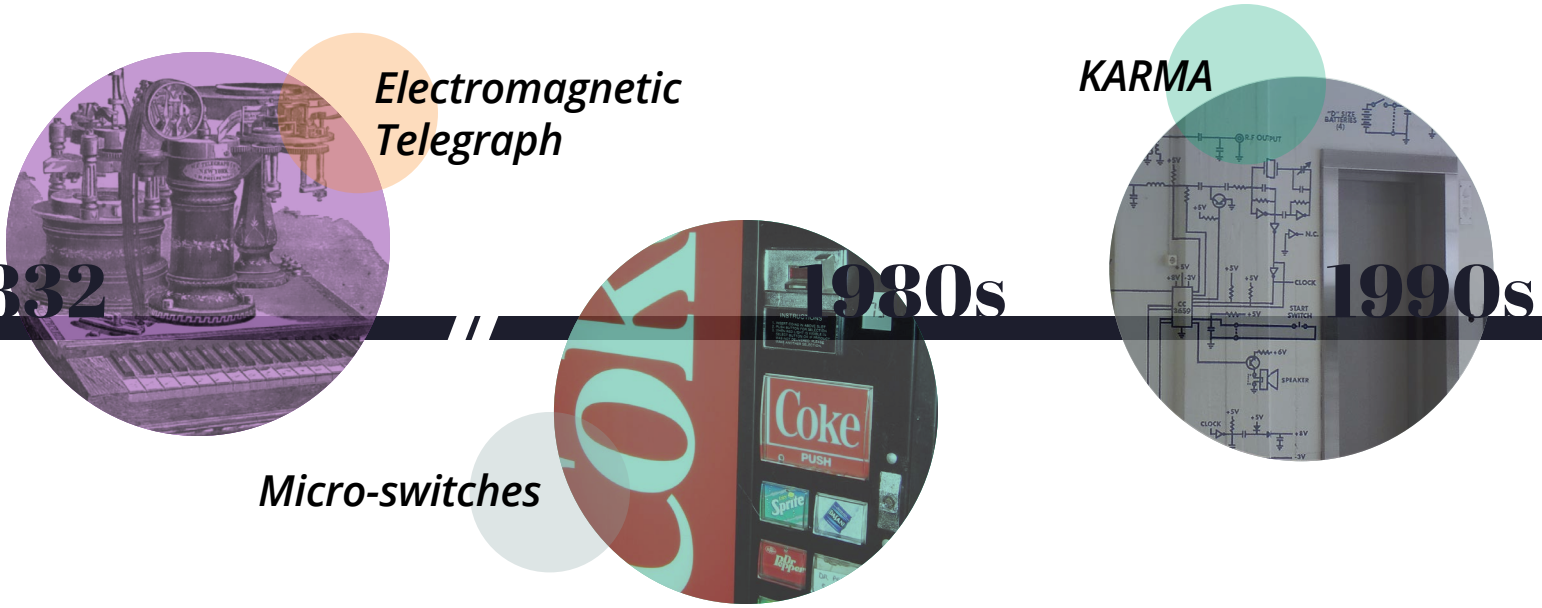
Today? Government is setting up pilot programs and doing something with IoT, not just talking about it.

Some of you may still be asking: What is IoT? Simply put, IoT is a series of devices connected to one another via the Internet — and these devices can communicate with you through the information you enter or sensors you wear and operate. And most of it is automated, meaning these interactions can happen without your having to do anything. It might sound simple, but it's a big deal: Internet-connected machines are expected to number 200 billion by 2020, according to research firm IDC Corp.

At that rate, these automated machine-to-machine transactions will outnumber human-to-computer transactions. So what does this mean for the public sector? And what programs are agencies and organizations developing to make use of this new technology?

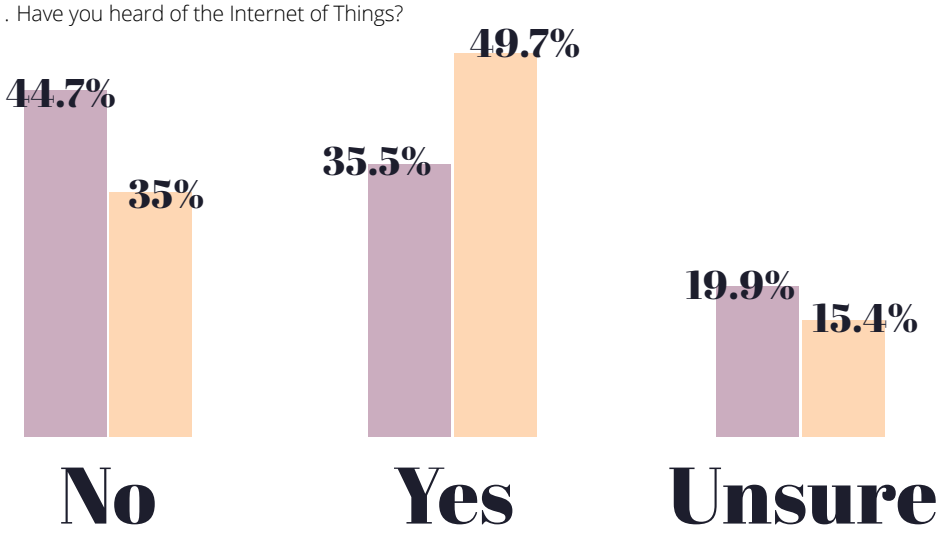
Our latest GovLoop case studies guide will feature stories of real-world public-sector uses of IoT, with best practices, implementation tips and examples of how you can use this revolutionary technology.

Read on for how IoT is changing everything from disaster responses to basic transportation.

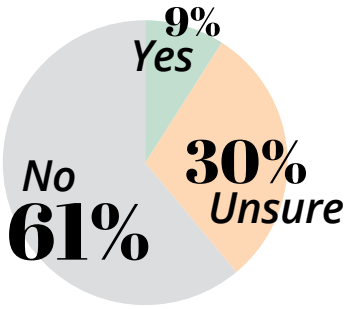


GovLoop Community Survey Data

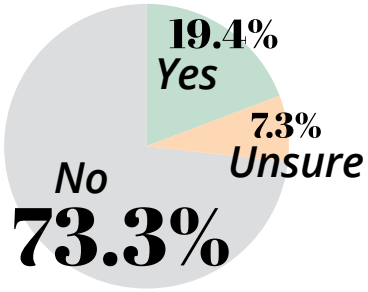
1. Have you heard of the Internet of Things?

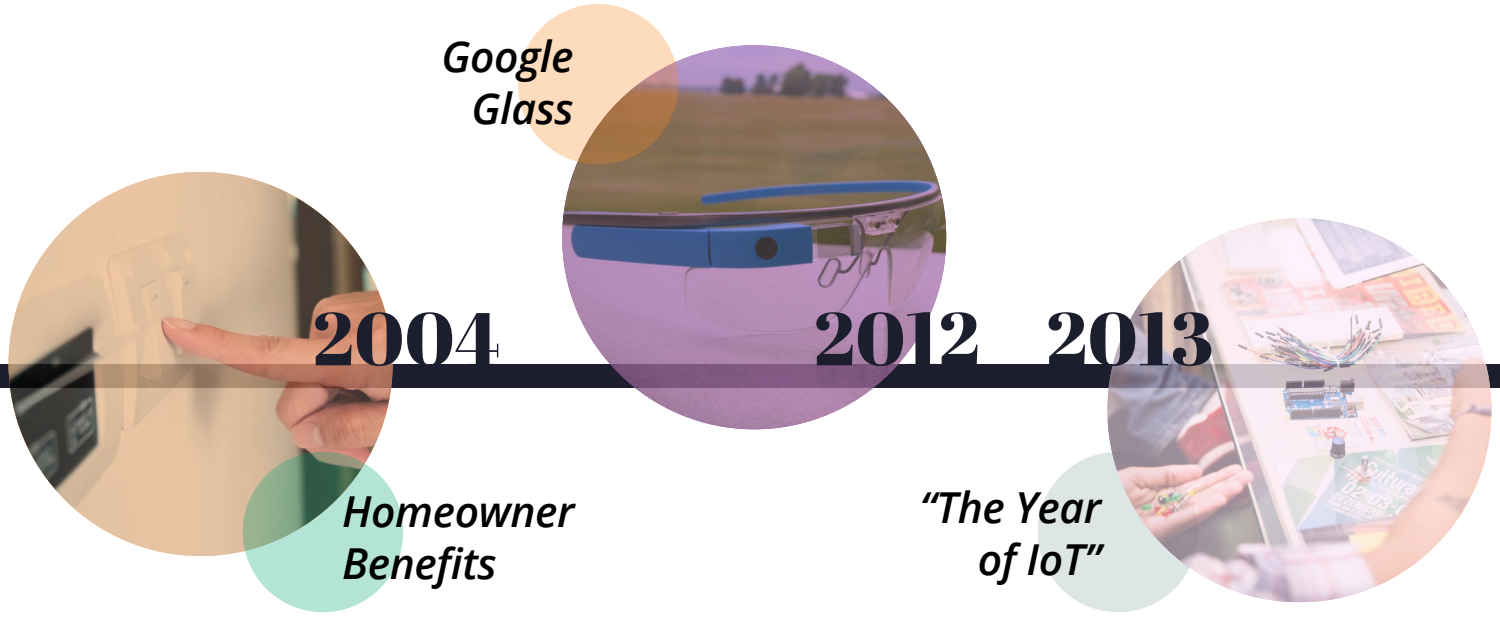


2. Is your agency or organization actively exploring or using the Internet of Things?



3. Will your organization be using the Internet of Things in someway within the next three years?





Improving Quality of Life through the Internet of Things

An Interview with Christian Heiter, Chief Technology Officer, Hitachi Data Systems Federal

Hitachi Data Systems Federal (HDS Federal) focuses on the Internet of Things that matter. Using the interconnection of mission-critical systems, the company works to leverage advanced data analytics for large amounts of sensor information. The data is incorporated into Hitachi's social innovation initiative that aims to create a safer, smarter, and healthier society. Particular focus areas include public safety, healthcare, transportation, energy, telecom, and IT analytics.

GovLoop sat down with Christian Heiter, CTO of HDS Federal, to hear how they are leveraging the Internet of Things (IoT) and predictive analytics to improve overall quality of life for the citizens of the United States and government employees.

While many tend to think about IoT in terms of data and smart homes, Hitachi considers it a way to improve quality of life for society. "What we're trying to do is take it to the next level by interconnecting infrastructure, like power plants, traffic management, and safety information," Heiter said. He cited examples of providing macro-level capabilities by improving social infrastructure, like redirecting traffic in a city so drivers are not as vulnerable to accidents. He also discussed how Hitachi's data analytics and social platform combined can be used for improving public safety.

"We do a lot of work with construction machinery. It's very expensive equipment with a huge number of sensors on them," he said. "Using our products, we can identify maintenance issues, schedule maintenance, reroute, and plan with geo-location. This let's us help public employees work smarter, more efficiently, and be more proactive in terms of equipment maintenance."

While IoT is helping with infrastructure issues, there are still data issues to understand. "One of the biggest problems everybody is dealing with, whether it's a federal or commercial agency, is the huge volume of data. There's a tidal wave of information increasing day by day," Heiter said. "We have much more advanced sensors that provide more data. So we need to be much smarter about how we do the analytics."

Eventually, Heiter hopes most of Hitachi's analytic capabilities and activities can be fully automated. "Let's take the intelligence, take the expertise, and automate as much as possible, and get it to the point where you only require human intervention when there's a problem flagged by the system," he said.

One important step in leveraging the massive amounts of data that IoT generates is encrypting the data where necessary to allow access to those with certified credentials. It's also important to properly store data. "We want to make sure the data is secure, not only from a privacy point of view, but also from a data integrity and quality point of view," Heiter said.

Heiter emphasized that IoT cannot be analyzed or implemented properly without collaborative efforts between industry, the federal government, and the private sector. "We need to work together as a whole, both the federal and commercial sector, on building a consistent set of standards that everyone can employ," Heiter said.

"If we have those consistent strategies for protecting the information, along with the appropriate policies, then I think that will enable the government and commercial sector to become much more efficient. We won't have so many ways to solve the same problem," he said.

The trend in government seems to be IoT on an agency-by-agency basis, which leads to disparate policies, strategies, and subsequent analysis and use of data. Heiter pointed out the following: "If we want to make the government more efficient, then some collaboration would be helpful in improving efficiency and security. From a commercial point of view, it could create entirely new business models."

In addition to promoting better innovation, HDS Federal can be used by public safety departments to leverage IoT for the protection of citizens. One method is through using video images and sensors to provide predictive analysis, so that government can better protect large crowds of citizens, like during parades or inaugural events.

"We have a public safety vertical, and what we've done there is bring in some companies to provide video and sensor information that allows us to protect critical infrastructures, whether they're nuclear power plants, government facilities, or airports," Heiter said. "By monitoring and providing data through video images, ground-based sensors, geo-located information, or vibration information, we can protect facilities from being attacked by bad actors."

Heiter concluded, "[W]hat makes Hitachi different is that we are the generators of our own data. We're solving our own problems and trying to use what we learn to help other communities, government, and commercial entities leverage the capabilities in an efficient manner and improve quality of life for all."

SECTION ONE

The Internet of Things & Emergency Management

When disaster strikes, we rely on first responders and emergency managers to contain the situation and safeguard the public. In turn, those safety personnel rely on communication infrastructures to relay up-to-date information about the disaster area and coordinate response efforts.

Unfortunately, robust information and communications are two assets that disasters such as fires, earthquakes and floods often reduce or eliminate. When that happens, emergency response suffers.

Off-site emergency managers get disconnected from the disaster zone, unable to communicate with responders in the field or determine conditions on the ground. As a result, they must coordinate disaster management plans without sufficient data to inform decisions, leading them to deploy inappropriate resources or send supplies to the wrong areas at the wrong times.

Similarly, emergency responders are disconnected from off-site information that could provide a more informed, dynamic perspective of the disaster area. They also have difficulty coordinating across teams when responders are spread across a large, complex environment without clear communication channels between them.

Finally, the general public is put at risk. Without real-time information, citizens can't effectively evade or, in worst-case scenarios, escape disaster areas. Without a means of communication, they also cannot effectively assist first responders in rescue efforts. Ultimately, the very safety that emergency managers work to ensure is put at greater risk.

Fortunately, when deployed effectively, IoT technology can mitigate many of the challenges to emergency response including a weak communication network and information lag.

By virtue of its name, many people consider IoT to refer only to Internet-connected devices. In fact, IoT technology can be used to extend the Internet into new areas and create an ad hoc communication structure. This is achieved in the same way you might use a router to transform your local, hard-line connection to the web into a wireless connection across your home. Similarly, devices can be equipped with technology to extend connectivity into new areas when traditional communications fail.

Once a communications infrastructure is deployed, first responders and emergency managers can use this new network to better coordinate response tactics. Additionally, connected sensors within disaster areas can relay real-time information to ensure emergency managers make decisions based on the most recent information.

In many scenarios, sensor-enabled technology offers yet another capability to emergency managers and responders. Unmanned aerial vehicles (UAVs) and ground robots can often access areas that would be unsafe for humans to enter. In an emergency situation, this capability can be a game-changing advantage. Not only does it reduce the risk to personnel on the scene, it also means that previously inaccessible information can be gathered and used to inform better response decisions.

Emergency response happens in real time. IoT not only provides the necessary communication and up-to-date information required to execute that response, it enhances the way first responders and emergency managers are able to use those necessary assets.

TAKEAWAY: ***Leveraging sensor-equipped devices doesn't always require creating those devices.***

WILDFIRE MAPPING

MAPPING WILDFIRES BETTER AND FASTER WITH THE FOREST SERVICE

In 2000, the United States experienced a number of unusually severe wildfires. The previous year, NASA launched the Moderate Resolution Imaging Spectroradiometer to provide near real-time images of the Earth's surface. That timing, said Brad Quayle, who works at the U.S. Forest Service's Remote Sensing Applications Center, was perfect to spark a transformation in the way wildfires are mapped and managed.

"We have always used airborne infrared flights to support tactical fire management. We routinely provide that once on a daily basis for requesting incidents. Imagery and derived information products are used at the incident level to make decisions regarding fire suppression activities," he said. "But with the evolution of these high temporal satellite observation technologies, we felt there was an unmet niche where we could provide additional information at strategic scale to fire managers as well."

As wildfires raged in 2000, Forest Service staff pursued a partnership with NASA to use the space agency's real-time imagery to detect where fires were and how quickly they spread. This collaboration evolved into an ongoing project called the Active Fire Mapping Program (AFM). Now, the program maps wildfire incidents across the United States and Canada in near real time.

Quayle explained the program's value: "[These maps] are intended to be used by fire and land managers at the regional and national levels to monitor the location and intensity of fire activity. The data and information products inform strategic decision-making and planning responses to current fire activity. The detection data — imagery, etc. — also provide managers, other members of the interagency fire community and the general public the ability to observe and monitor the effects of recent and ongoing fires — things like how intense the fires are burning, where the smoke is going or coming from, where there are burn scars and more."

"The data provided by the Active Fire Mapping program is also ingested into decision support applications utilized by the interagency wildfire management community, such as the Wildland Fire Decision Support System, which requires information on the current location and extent of fire activity," he continued.

Although the Forest Service manages the program, Quayle said it is by no means a single-agency endeavor. "As an agency, we are not in the business of building our own sensors," he said. "We don't have that kind of budget. So we rely on the space agencies, NASA and [the National Oceanic and Atmospheric Administration], and we use their assets."

Through an interagency agreement, NASA provides more than sensors to the Forest Service program. "Everything we are able to provide through this program is predicated not only on the particular sensors provided by NASA, but also on the data processing technologies and science algorithms they have developed," Quayle said. "All that capability is provided to our agency through this partnership."

This partnership also connects the Forest Service to academic institutions, such as the universities of Maryland and California at Davis, particularly through NASA-funded research projects. "NASA requires that researchers submitting a proposal have an operational partner in their project because NASA wants to make sure that [projects] actually get transitioned into operations and used by agencies," explained Quayle. "So, depending on the research/development topic, the Forest Service may be asked to be an operational partner. We collaborate with the project investigators in the development and refinement of the project so that we get an output that fits our information needs."

Beyond this collaboration, the Forest Service runs the day-to-day operation of the program. Quayle said his department primarily focuses on making sure data is collected and analyzed quickly so that it can be pushed to the public in a timely manner.

Given the sheer volume of the data derived from satellite observations, this quick processing requires automation. "We spend a lot of our time working on the automation piece to make sure the ingestion of data and subsequent processing execute autonomously and continuously using the technologies and algorithms provided by NASA," said Quayle. "We also ensure that derivative data and products are quickly generated, packaged up, and made available for folks to consume."

Ultimately, that's the ambition of this sensor-based project — to provide the public with the information necessary to monitor and manage wildfires.

Key Takeaway: Leveraging sensor-equipped devices doesn't always require creating those devices. For agencies that don't have the resources or know-how to manufacture devices, partnerships with other agencies and academic institutions are a smart way to quickly deploy IoT with minimal investment.

EMERGENCY DRONES

***TAKEAWAY:* Public misperception, regulatory roadblocks and insufficient funding can often delay IoT implementation.**

IN AUSTIN: DRONES, EMERGENCY RESPONSE AND THE INTERNET OF THINGS

The Smart Emergency Response System (SERS) is a disaster management project that deploys Unmanned Aerial Vehicles (UAVs), commonly called drones, into emergency zones. The UAVs serve two purposes. First, they create an on-demand communication structure — often needed when standard communications fail — between the emergency management center and the disaster area. Second, they gather and disseminate real-time information and imagery from the disaster area to on-the-ground rescue robots. Together, these two capabilities create an emergency response ecosystem that is automated and informed.

Coitt Kessler of the Austin, Texas, Fire Department (AFD), one of three government partners for the project, explained how and why his department became involved in the project.

He said what initially drew him to it was a desire to fuse a hobby with his career as a firefighter. "It's not that glamorous, but I was on YouTube looking at aerial photography," Kessler said. "I was looking at the perspective a quadcopter or a helicopter can provide, and it made all the sense in the world to use it [for emergency management]."

But Kessler said getting his idea off the ground was difficult — literally. His department didn't have the resources or connections to successfully navigate Federal Aviation Administration (FAA) regulations and receive permission to use airspace for a drone project. "It's almost like the Wild West out there in that there's very limited communication between public safety agencies, the government and researchers," he said.

Kessler determined he needed cross-sector collaborators to gain the resources and know-how for his project. After more online research, he connected with Dr. Robin Murphy at the Center for Robot-Assisted Search and Rescue at Texas A&M University.

Kessler also sought organizations that were already flying such systems. No fire departments had formal programs, but the police departments of Mesa County, Colo.; Grand Forks, N.D.; and Arlington, Texas, all had active flying programs.

Those departments taught Kessler valuable lessons that he applied to his program. "Working with these other organizations, it really helped us answer some of our questions and it provided us guidance on how to move forward," he said. "They taught us that there are three big hurdles you have to overcome: public perception, policy and procedure, and funding."

They also helped them overcome these hurdles. For instance, they explained how to overcome public hesitation about drone use. "That was really where they guided our agency," he said. "They said to get with your public information officers to set up a message. Then, take it to the public. You have to take the scary out of this whole process, and you do that by repeating it and making everyone comfortable with what's going on."

They also said such communication could help Kessler's department navigate UAV use policies and procedures. "Because we're working in the national airspace and we're doing it as a public entity, we have to be able to work other units that are in the air. So you have to define exactly what you're doing and how you're going to do it," Kessler said.

The third challenge — funding — brought Kessler into a formal agreement with the SERS team. "We need to design equipment that's made specifically for what we're doing," he said. "I found that we really needed to have an alliance, to actively collaborate between research, industry and public safety. That's why we teamed up with the Global City [Teams] Challenge group."

The SERS team is composed of three university partners, three industry partners and three government partners, including AFD. Together, they participate in the National Institute of Standards and Technology's Global City Teams Challenge to develop and fund their project, although industry partners also contribute significant resources.

AFD's program is not yet fully operational, but it shows significant promise for the field of emergency response, informed by aerial sensors. In fact, the department has already overcome its biggest hurdle by receiving FAA approval. "We are very proud to be the first metro fire department with that authorization from the government," Kessler said.

Currently, the SERS team is in the research and development phase. Kessler said it's making progress toward Step 2, however. "In order to develop our program and research further, you need to do hands-on training," he said. "That's the area we're approaching now is research through training with the equipment."

Key Takeaway: Public misperception, regulatory roadblocks and insufficient funding can often delay IoT implementation. Rather than confronting these obstacles alone, seek partners who have already overcome them. Learn from them to make headway on your own projects.

SECTION TWO

The Internet of Things & Smart Buildings

IoT seems new, but it's really just gaining momentum. The technology has long been making inroads in terms of energy efficiencies, particularly in newer buildings.

The problems it solves are clear and two-fold: the manual manipulation of building energies (such as heating and air-conditioning systems) is inefficient, and small problems that should be easily detected (such as small leaks in building water pipes) are often found far too late.

Whether building managers are spending too much on unneeded air conditioning, wasting electricity by having lights on in empty rooms or missing small infrastructure problems that become big ones, IoT can help.

How, exactly, though? Many government facilities, whether they're small, midsize or large, have facility systems that take huge resources to maintain and engage. IoT helps make these systems smarter and can help collect and aggregate data from a variety of sources to better understand the needs and capabilities of a given system.

An example that many will already be familiar with is from the private sector. By now, you've probably heard of Nest Labs, in no small part because Google purchased the company last year for $3.2 billion. Nest is best known for making a "smart," or connected, thermostat for homeowners. Most thermostats let you set a desired temperature, monitor the current temperature, and switch between heat and air conditioning. Programming thermostats can be annoying. You might forget to turn it off or incorrectly program it, and an un-programmed thermostat can add 20 percent to your heating and cooling bill.

Nest's Learning Thermostat aims to solve this problem. It has four types of sensors: activity sensors that detect when someone is home, humidity sensors, weather sensors and temperature sensors that detect how quickly the temperature is changing. Nest's thermostat programs itself by learning your behavior patterns and desired temperatures for certain days and times during the week and then building a schedule for your HVAC.

Another example of how IoT can help make buildings smarter and facilities management easier resides in something every public building is required to have: a fire extinguisher. Smart fire extinguishers are being developed that monitor for tank pressure and space. If these levels are not up to par, the devices notify building managers through automated Bluetooth technology.

When applied to public-sector buildings and facilities or large infrastructure such as bridges and water systems, IoT-enabled sensors can do everything from automatically monitoring and adjusting energy levels or HVAC systems to detecting if an interstate bridge is developing cracks that need repair. Such automation and early detection can save millions of taxpayer dollars — and possibly save lives as well.

The following two case studies will detail how the city of Seattle and the General Services Administration are using IoT to save money and be more environmentally friendly.

SEATTLE SMART BUILDINGS

TAKEAWAY:
To begin creating smart buildings with IoT, find examples where you can prove your return on investment within 24 months.

SEATTLE GOES EVEN GREENER WITH THE INTERNET OF THINGS

Think of Seattle and a few iconic images come to mind: Pike Place Fish Market, steaming mugs of Starbucks coffee, Mount Rainier rising over the city's skyline, ferries and water.

Now you can add to those mental images buildings pulsing with IoT-enabled sensors. In a city that's already pretty darn green, such buildings are helping it go even greener.

IoT-enabled smart buildings nationwide are using sensors, data and analytics to measure and respond to the way the facilities use energy. Seattle saw this emerging in the 2000s, and officials decided to invest in IoT to become a leader in the field and a hub for IoT technology.

GovLoop spoke with Stephanie Gowing, Green Business Manager for Seattle, to learn more about how the city is using IoT to save energy and increase buildings' efficiency.

In 2013, Gowing said, Seattle announced the High-Performance Buildings Pilot Project, a new smart buildings partnership among the city of Seattle, Microsoft and the Seattle 2030 District, a group formed to meet certain energy reductions and goals by 2030. The project aimed to reduce power consumption through real-time data analysis of Seattle buildings.

"With the environmental ethic we already have in Seattle, and because the cost of energy in general is less expensive here, we thought this was a great market to kind of try this new pilot project and try this technology with the idea that if we can show a bunch of energy savings for buildings here, there's a lot of really great potential for other markets," Gowing said.

This is how the technology in the Seattle smart buildings works: Building managers apply a set of assets via a vendor dashboard to analytics of the building data. These assets and the dashboard then work to optimize equipment and other related processors for energy reduction and comfort requirements. Essentially, it's software that identifies equipment and system inefficiencies and alerts building managers to areas wasting energy. All data and information is stored in the cloud, and engineers can virtually see it on the dashboard.

"Since it's online and in the cloud, its storage is great because it collects a lot of data in real time," Gowing said.

Each building runs the system on a variety of machines, collecting information comes from elevators, HVACs, heating and cooling towers, and more. The four buildings that are in the programs have 547 sensors collecting an average of about 5,000 data points every three and a half minutes.

Gowing also said a range of buildings were selected for the test. "There's a hotel, a medical facility, a manufacturing facility and then an office building," she said. "The idea is to be able to test with those different types of buildings that have quite different needs as well [as] to be able to show how the Internet of Things can be used across different types of buildings."

Right now the pilot program is still assessing the outcomes and data, but Gowing expects that when the data is complete, other buildings throughout Seattle will be interested in using this type of technology.

"Our goal is to continue to communicate the successes and the challenges that comes from these pilot buildings," Gowing said.

Key Takeaway: To begin creating smart buildings with IoT, find examples where you can prove your return on investment within 24 months, Gowing said. "We found that those programs that could prove the technology would actually be saving buildings and building managers money within two years were the ones that got everybody most excited," she said.

GSA'S DATA SENSORS

TAKEAWAY:
Although the IoT data you're using can lead to myriad efficiencies and improvements, it doesn't matter if that data is not standardized and able to talk to one another.

THE GENERAL SERVICES ADMINISTRATION'S BUILDINGS ARE GETTING SMARTER

GSA's mission is "to deliver the best value in real estate, acquisition, and technology services to government and the American people."

And with GSA's latest use of IoT technology, the agency is delivering on that promise and beyond.

For the past few years, GSA has been experimenting with an IoT-driven smart building strategy, connecting building management systems to a central cloud-based platform, improving efficiency and saving up to $15 million in taxpayer money per year.

"Commercial buildings account for nearly 40% of the United States' primary energy use and GSA owns nearly 182 million square feet of office space nationwide. GSA's plan to meet the requirements of President Obama's Executive Order 13514 includes a goal of reducing energy consumption in federal buildings by 30% by 2015."

So what does this effort and initiative look like at GSA? Think sensors. Lots and lots of sensors. As a Washington Post article from last summer reported:

"At the General Services Administration in downtown Washington, tiny white sensors pepper the windows, ceiling tiles, heating units, water tanks and fan coolers, almost blending in to the building's open-plan decor. Some detect how much sunlight shines through a window, and indoor bulbs dim or shades raise themselves accordingly. Others sense motion, turning off lights, air conditioners or power sources when employees are away from their desks. Some sensors simply relay information about total utility consumption, such as how much cooled water or energy employees have used in a day."

"In every building in [our] test, there's an average of 2,000 sensors on various points in the building," said former GSA Administrator Dan Tangherlini at an IoT event in 2014. "We then measure the performance data against the manufacturer's expectations for usage to determine if the buildings are consuming the right amount of energy, and to determine whether there's an opportunity for cost savings."

Two thousand sensors sound like a lot, but that number pales in comparison to the amount of data those sensors collect. According to a Federal Computer Week article, those sensors can collect 29 million data points per day. With them, GSA can monitor "everything from light use to humidity, enabling the agency to boost productivity and promote good health by optimizing conditions when workers are present and saving on energy costs when they're not," the article reporter.

Will GSA eventually require all leased buildings to adhere to IoT technology and smart buildings policies? Not for now, but officials believe things are trending that way. As a recent statement on GSA.gov notes, "GSA is currently not requiring leased facilities to adhere to the GSA Smart Building policy and strategy, however, GSA is making the building industry market with its Smart Building strategies and policies. As the market shifts from non-converged buildings to Smart Buildings GSA believes that the leasing market will follow GSA's lead."

Key Takeaway: Although the IoT data you're using can lead to myriad efficiencies and improvements, it doesn't matter if that data is not standardized and able to talk to one another. GSA spokesperson Matthew Burrell is quoted in this article as saying, "As the blurry line between industrial systems and IT systems becomes more clear, we are finding that it is critically important to work with industry to homogenize the data so that one system's data stream and reporting capability is the same as the next."

Struggling to stay up-to-date with tracking and securing IT hardware and software across your organization?

YOU'RE DOING IT WRONG.

Government agencies IT estates are more complex than ever. Moving to cloud, virtual, and mobile environments, along with the emerging Internet of Things, will increase the difficulty of tracking IT hardware and software across the entire enterprise. You can't manage and protect your IT assets—if you can't accurately define your IT baseline.

If you don't understand what you have, you can't manage it. But you can change that, with Enterprise IT Data from BDNA. You'll have the most complete information to make the best possible decisions, lowering your costs and eliminating risk. And there isn't a department in your organization that couldn't use that kind of insight.

Want to start doing IT right? Start with BDNA.

Call for a demo at +1 (650) 625-9530
or visit BDNA.com to learn more today!

BDNA

Managing Enterprise IT Data to Secure the Internet of Things

An Interview with Walker White, President, and Clark Campbell, Vice President, Public Sector, BDNA

The cyber world is a dangerous place. In a rapidly escalating environment of cyberthreats, obsolete devices, software beyond end of life, and poor visibility of your IT infrastructure, the risks an organization faces are extremely heightened. Additionally, the Internet of Things' rapid growth is making it even more difficult for organizations to keep their technology up-to-date and secure.

GovLoop sat down with BDNA's President Walker White and Vice President, Public Sector Clark Campbell to discuss how BDNA's enterprise IT data management software can help organizations take control of their IT infrastructure to become more secure in this era of the Internet of Things.

Step one? Look at your "end of life" products.

Software, hardware and devices that have reached end of life are vulnerable assets that vendors no longer support. Because they stop receiving security updates over time, keeping track of end of life products is essential to an organization's cybersecurity. Hackers target outdated devices, software and packages to infiltrate the IT infrastructure and acquire an organization's valuable, private information.

However, given tight budgets, government agencies still often use technology that is near or past end of life, leaving federal agencies especially vulnerable to cyberattacks. And many organizations have no way of tracking whether their technology is near its end of life.

BDNA is helping change this.

BDNA's enterprise data management software tracks the technology in an organization's environment, providing centralized, up-to-date, reliable information about how close technology is to its end of life.

"Being able to monitor this is an extremely valuable piece of information to give to someone in IT operations," said White. This is because in no small part it allows IT to address potential risks before a cybersecurity threat arises.

As we move into the era of the Internet of Things, keeping software updated is even more critical. "If many of the breaches are coming through end of life software in the traditional IT space, there's no reason for us to think that won't be the case with the Internet of Things," White said.

"As attackers are getting more sophisticated, people using these devices need to make a better effort to keep their IT up-to-date," White explained. Organizations must make sense of the massive amounts of data that will come back from IoT device sensors and apply proactive cybersecurity practices rather than reactionary ones.

However, because of the sheer volume of data produced by IoT, enterprises often lose track of their technology and end up overspending on IT goods and services. Today, IT departments can waste more than 25 percent of their budget if they leave their enterprise IT data unmanaged.

But by using BDNA's enterprise IT data management software to implement security-focused IT asset management, organizations can simultaneously cut costs and mitigate security risks before they become a larger issue.

As IoT expands into private areas such as the healthcare and medical fields, "A lot of damage can be done if we don't posture security at the very outset of what we are doing," White said. With so much information being generated by these devices, making sense of information quickly, "is going to be absolutely essential to identifying issues and gaps," he explained.

A few years ago, the Department of Energy fell victim to a successful cyberattack that allowed hackers to access the personally identifiable information of 50,000 people. The cause: an outdated version of a software application leaving the information vulnerable in cyberspace. As a result, the Department now spends $4 million per year in credit monitoring services for victims of the hack.

"Now, because the DoE is using BDNA software, they have the awareness of what their end of life situation is on their hardware," Campbell said. Government agencies do not have the budget to replace all of their devices before their end of life, Campbell stated. "Today, the DoE has visibility into what percentage of their hardware and software assets are near or beyond end of life because of BDNA's enterprise IT data management software. They have end of life information readily accessible, allowing them to effectively rank which technologies need to be upgraded first, enabling them to prioritize their department's budget and mission needs."

As IoT expands, it will grow increasingly important for government agencies to understand what outdated IT is still in their environment. Hackers will continue to target the technologies with the most vulnerability. By aggregating and analyzing information on the government's end of life products, BDNA's enterprise IT data management software is helping federal agencies determine the most critical equipment to replace, proactively addressing cyberthreats before they become a bigger problem.

THE INTERNET of THINGS
WITH RED HAT JBOSS MIDDLEWARE

Red Hat has expertise in helping customers design, develop, and implement secure, stable (IoT) solutions.

Red Hat® JBoss® Middleware provides key technologies to help your agency:

Aggregate

Transform

Analyze IoT data

redhat.

Bringing the Internet of Things to Life Quickly and Cost-Effectively

An Interview with Michelle Davis, Senior Solution Architect, Red Hat

We live in a complex world. With millions of new devices and applications being produced every day, the sheer volume of data produced by Internet of Things can make it even more complex.

But it doesn't have to be that way. GovLoop sat down with Michelle Davis, Senior Solution Architect at Red Hat, to discuss how open source software helps organizations optimize data produced by the Internet of Things to align IT strategies with business goals.

Today, Davis said, "organizations have a wealth of information at their disposal to help them make data-driven decisions. Sensors on billions of devices around the world disseminate information that enterprises collect to help make better services and smarter decisions. For the data produced by these devices to be useful, agencies must compare new information with existing data from traditional sources. The large influx of information from IoT devices presents serious aggregation, ingestion and analytical challenges for both government agencies and IT organizations."

For many organizations, there is no standard way of integrating this information. Red Hat wants to change that. They believe there should be a flexible, inexpensive standards-based solution for IoT data that would reduce risk and support a variety of environments.

"Open source is one of the drivers for the Internet of Things because it allows people to rapidly create new innovations," Davis explained. As an enterprise open source software company, Red Hat offers solutions with essential tools to tackle the staggering amount of IoT data.

Driven by a passion for innovation and open source software, and a desire to help enterprises create applications faster in a smarter way, Red Hat offers their JBoss Middleware portfolio. "JBoss Middleware is a family of enterprise-class, cloud friendly integration and middleware products that one would use to build, create, connect, deploy and run intelligent applications." Davis said. This middleware provides tools to embrace and include IoT.

Red Hat JBoss Fuse allows organizations to create and deploy integrated applications, utilizing standards, which ultimately improves portability and reduces time to market while removing risk. Giving developers the flexibility that they need to build new applications, Red Hat JBoss Data Virtualization is providing government agencies and private organizations a unique solution that effectively marries new information with existing infrastructures. Across the country, organizations are using Red Hat's JBoss Middleware portfolio to build scalable, secure solutions to aggregate, ingest, transform and analyze IoT data.

An example? Following several demands for better train safety, Meteorcomm, the leader in data communications infrastructure solutions for the railroad industry, worked with Red Hat to implement a sensor-based solution to address this problem. Armed with a new network of interconnected devices, these sensors use automated communication to ensure that trains maintain safety and efficiency.

In the near future, Red Hat expects most agencies will be incorporating smart devices and sensors to improve quality of services such as border patrol cargo inspections, or veterans' medical visits by automatically linking patient's electronic health records with biomedical research databases. Innovations like these would significantly improve border inspector's productivity to secure our border and healthcare providers' ability to treat veterans quickly and effectively. By collecting and integrating isolated data, Red Hat helps government agencies become more innovative and efficient.

For government agencies, security is one of the biggest challenges in the world of the Internet of Things. "The ability to move this information back and forth securely is necessary," Davis said. JBoss Fuse provides encryption, authorization and identification with different IoT protocols like MQTT, STOMP or AMQP to securely move IoT data from one network to another.

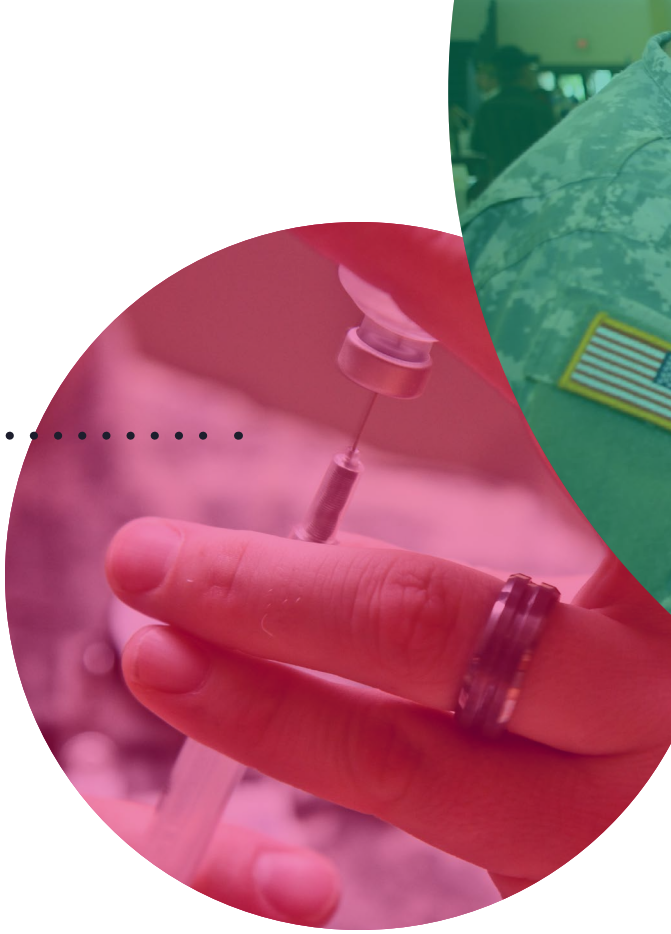
With JBoss Fuse, agencies can ingest IoT data in a secure, scalable manner. JBoss Fuse is a lightweight integration platform that can connect any application, data or device. The JBoss Data Virtualization software then lets agencies analyze this new data alongside traditional data. With this analysis, government organizations are able to make better decisions and improve their services to citizens. Red Hat's IoT reach goes beyond middleware as the need for smarter storage or an on-premise cloud-like scaling platform increases.

The sheer volume of new information being generated by the Internet of Things presents challenges and opportunities for both the public and private sector, Davis said. This information, which years ago would have been considered isolated, will allow a new collaboration between government and industry and citizens. This creates whole new categories of information gathered, and opportunities to use devices to more effectively manipulate objects. These in turn gives rise to new opportunities for the government to share information, innovate, save lives, make more informed decisions, and actually extend the scope of machine and human impact.

Red Hat's JBoss Middleware portfolio has made the complex world of IoT easier for government to navigate. With secure and accessible information, the government's way of doing business is becoming more efficient and data driven, changing the lives of citizens for the better.

SECTION THREE

The Internet of Things & Healthcare



Think of the human body as a car. For years, drivers have been able to monitor the health of their vehicles with oil and pressure gauges that give alerts when there is a problem. But unlike a souped-up BMW, patients with chronic medical issues lack alerts for when a tune-up is needed. There is no caution light for diabetes or heart disease — until recently.

VA doctors have been looking to use smart healthcare devices to make healthcare not only more accessible, but also more effective for patients. IoT-based healthcare innovations include fetal, heart, temperature and blood glucose level monitors in addition to robotic mental health assistants.

And it's not just VA investing in IoT solutions. The Centers for Disease Control and Prevention, the Department of Health and Human Services (HHS), and many state health organizations are looking to IoT to provide better healthcare to patients in their homes.

In addition to improving patient care, the use of IoT could save $63 billion in healthcare costs over 15 years with a 15 percent to 30 percent reduction in hospital equipment costs and a 15 percent to 20 percent increase in patient communications, an Atlantic Council report found.

However, connected medical devices do pose some serious challenges to the security and privacy of patients' health information. The devices beg the questions: Who owns the data? Who is authorized to act based on the data? And is the data actually secure? In large part, the medical field is still grappling with the answers.

IoT devices have also run into some difficulties in dealing with requirements set by HIPAA — also known as the federal Health Insurance Portability and Accountability Act of 1996. The primary goal of the law is to protect the confidentiality and security of healthcare information.

In January 2015, the Federal Trade Commission released a staff report titled "Internet of Things: Privacy & Security in a Connected World." The report details what protected health information (or PHI) is off-limits for IoT-enabled health devices. "Namely, HIPAA regulates only that information qualifying as PHI and only regulates uses/disclosures, privacy and security of PHI by HIPAA-covered entities and business associates."

Despite the very real concerns of privacy and security, health IoT advocates point to the possibilities that such devices could give patients. "[Data] has to be part of how consumers and patients think about their care experience," said Patrick Conway, Chief Medical Officer at the Centers for Medicare and Medicaid Services at the annual Health Datapalooza. By giving patients robust data, they are better able to make informed decisions about their health.

For example, the University of New Hampshire is using smart beds that can detect when they are occupied and when a patient is attempting to get up. The smart bed can also adjust itself to ensure patients receive the appropriate pressure and support without the manual interaction of nurses.

Government agencies are also teaming up to help administrate the field. The Food and Drug Administration offers guidelines for medical devices, and regulators will likely continue to control connected devices that patients use. HHS has also created an information technology strategic plan to help agencies share information and collaborate on IoT.

The following two case studies will detail how VA and the city of Chattanooga, Tenn., are using IoT to save money, be more efficient and make communities healthier.

MEDICAL ALERTS

TAKEAWAY: ***Ronzio advises developers to keep the user as the central focus when creating new IoT sensors.***

CONNECTING HEALTH AT THE DEPARTMENT OF VETERANS AFFAIRS

VA has been on the leading edge of connected devices for years. Right now the department is working on more than 50 Internet-connected devices — everything from sensors that gauge a person's gait to monitor for future falls to robotic mental health providers.

One of the department's most promising projects is a prototype for a flu shot alert system that would prompt people entering their local drug stores to get a flu shot.

"As the individual walks into the store, there is the capability through multiple platforms and geo-location to have an iPhone or an Android device prompt you that you are actually at a VA-approved location that can give you a flu shot," said VA's Ronzio. "A patient can walk up to the counter, give them a coupon code and get their flu shot. It's simple, cost-effective and convenient, which means more people will take the right steps to stay healthy."

VA isn't stopping at flu shot notifications. It's also looking at similar technology to help monitor chronic illnesses. "Let's say you have your medical records on your device, and you have a disease like diabetes. There's routine blood work and routine tests that you should have accomplished," Ronzio said. "Many convenience stores now are getting into that market where they have mini clinics. Well, if we have contracts with them, patients can get an alert based on their medical information and their disease management protocols to go get the lab work done while they're there. So instead of having to make a trip to a lab, patients can handle their blood work right in the convenience store."

The medical data can be tracked electronically using VA's Blue Button online medical records program.

The device can also alert Type I Diabetes patients that it's been six months since their last hemoglobin A1C test. These alerts free up medical staff because they don't have to take time to call patients to remind them to get their blood work done.

The alerts will also help keep patients in control of their medical decisions and not overwhelm VA with data. Ronzio wants to create systems and software so that patients get the information first. They have the option of saying, "I'm concerned with this data, the software's concerned with this data, I want to send this snippet of data to my medical provider and have a discussion."

"We've got to give the veteran the complete control over how they share data, who they share it with, and be fiscally responsible about how we're going to protect our data systems in the future," Ronzio said. "Because once the VA gets that data, and we put it as part of the patient's permanent medical record, the VA now has a legal responsibility to maintain that data for their lifetime plus some years. Typically that equates to a rough number of 125 years."

While most of VA's IoT devices are still in the development stage, Ronzio insists that focusing on IoT development is essential for the health of veterans and the public. "If you want to live to be 100 years, we're going to have to do things differently than if you want to live to be 70," he said. "We are going to hit a magic point where we have enough data on your genetics, your basic building blocks and the blueprint design of your body, so that we can help you live longer, healthier and happier. We will be able to track the baseline of your body, so we know when things are off course and correct it."

Key Takeaway: Ronzio advises developers to keep the user as the central focus when creating new IoT sensors. "I would recommend some sort of stop light-colored cue to inform patients of their current health state. Green means you are in good shape, yellow means there is some area of concern, red means seek a medical professional immediately. The simpler you can make the interface, the better."

ALLERGEN SENSING

TAKEAWAY: ***The GASP platform will provide an open application programming interface for other developers to experiment with.***

BREATHING EASIER IN CHATTANOOGA, TENN.

Tennessee's fourth largest city, Chattanooga, is a bastion for outdoor explorers. Rock climbers, kayakers, hikers and bikers flock to the city to take advantage of its natural resources. In fact, in 2012, Blue Ridge Outdoors Magazine rated Chattanooga its "best outdoor city."

Nestled between the Appalachian Mountains and the Cumberland Plateau, the 170,000 residents of the "Scenic City," are proud of their foliage. Since 1990, Chattanooga has been a card-carrying member of Tree City USA, a tree and care organization sponsored by the Arbor Day Foundation.

Unfortunately, all of those trees create some serious pollen. According to city officials, Chattanoogans suffer from terrible allergies as a result of the bowl-shaped valley the city sits in.

"Pollen counts are high because pollen gets caught in this natural feature and creates unwanted misery and malaise for both residents and visitors," said Nate Hill, Director of the Chattanooga Public Library/Chattanooga Enterprise Center. The pollen count is so high that the Times Free Press rated Chattanooga the 11th worst place for people with allergies to live. The paper notes that allergies and asthma contribute to more than 14 million missed school days a year, making those ailments the most common reason children miss school.

And it's not just residents who feel the pollen pinch. Tourists account for more than $1 billion in revenue that could be lost if they stay away because of poor air quality. City officials decided to take action to address the pollen problem by using IoT.

To start off, Chattanooga entered the National Institutes of Health's US Ignite Challenge, a program that pairs community leaders with federal experts and industry insiders to help craft solutions.

Through US Ignite, Chattanooga launched a pilot project called GASP, or Geolocated Allergen Sensing Platform. The idea was to place at least 10 sensors at municipal electric power distributor substations evenly distributed across the city. The sensors could even be installed on public buses or be developed as wearable devices.

"These sensors will collect data about the particulate matter in the air, specifically but not necessarily limited to plant pollen, and will report that data back in real time," according to GASP's impact statement. "GASP will create a mobile web application, using open web standards, to analyze, interpret, and display allergy-related information in real time for the benefit of end users."

Although the pilot program is still in the early development stages, organizers' first step is to provide airborne particulate mapping for Chattanooga. In the future, they hope "the data collection approach and initial visualization tools developed in Chattanooga can be used to support a nationwide open-access dissemination platform on the order of Google's Street View, but called Pollution View."

One of Chattanooga's partners in GASP is the University of Texas at Dallas. The university is already focused on expanding the pilot's reach. "A PollutionView tool will contribute significantly to a transformation of the Environmental Public Health field in the United States," according to a grant proposal the university wrote. "The project involves real-time big data analysis at a fine-grain geographic level. This will involve trades with sensing and computing especially if the sensor package is to be deployed at scale. The project will help determine if real-time allergen collection and visualization can improve health and wellness. Thus, this project will combine Cyber Physical Systems (CPS) and gigabit networks to address major health concerns due to air pollution."

The university has already allocated more than $150,000 in grants to work on GASP.

According to the US Ignite proposal, all GASP data collected will be considered open and public and will be made available via the Chattanooga Public Library open data portal. "We know that we can't anticipate all of the ways that designers and developers might choose to use the data, so this open solution will allow for unintended innovations by allowing open API access to the data" the proposal read. "Similarly, while the group may pursue development Android and iOS versions of the core mobile application proposed here, an HTML5-based responsive web application is the highest priority."

Key Takeaway: The GASP platform will provide an open application programming interface for other developers to experiment with. Although Chattanooga has some of the worst pollen in the country, officials there want to make sure that other governments can use their IoT technology to gain a clearer understanding of the air they breathe.

SECTION FOUR

The Internet of Things & Transportation

Road warriors who commute at least 30 minutes to and from work in our nation's most congested cities — Los Angeles, San Francisco and Honolulu — sit in traffic for an average of 90 hours per year. That's nearly four vacation days that motorists waste stuck in traffic.

And if you think U.S. roadways are congested today, imagine what daily commutes will be like in 30 years. The Department of Transportation is already considering how our congested transportation system will accommodate the travel needs of some 70 million additional people in 2045. These sobering statistics from DOT give context to the growing problem:

- By 2040, nearly 30,000 miles of our busiest highways will be clogged on a daily basis.
- The annual financial cost of congestion is $121 billion.
- By 2045, freight volume will increase 45 percent, leading to far more trucks on the road.
- In 2045, there will be nearly twice as many older Americans and a greater need for quality transit to help them travel safely.
- The total number of vehicles operating across the United States reached a record 252.7 million last year.

As federal, state and local governments work to ease congestion on busy roadways, they must also focus on motorists' and pedestrians' safety. According to DOT, Americans spend more than 1 million days in the hospital each year because of crash injuries. The most recent data from 2013 shows that 32,719 people died in motor vehicle crashes, including 4,735 pedestrians, 4,668 motorcyclists, 743 cyclists and 396 children under the age of 5.

"People have tried many times before to predict events that will happen in the future, and some of them have failed spectacularly," said DOT Secretary Anthony Foxx, noting erroneous speculations from the mid-1900s that future computers may weigh no more than 1.5 tons and the belief that nuclear-powered vacuum cleaners would likely be a reality in 10 years.

"Data is telling us some important things about the future," Foxx said. "That said, if we're going to build a transportation system fit for the era of big data, Washington won't be the place where we find all the answers."

The good news is bright minds in government and industry are finding answers to our most pressing transportation needs. They are turning to Internet-connected devices, sensor technologies and better data analysis to identify problems and potential solutions.

In Nashville, Tenn., for instance, transit officials and researchers are developing a smartphone app, powered by sensor data, to increase ridership on city buses. The app could play a key role in convincing road warriors to let go of the wheel and take a bus to work. It may also ease the fears of residents who aren't familiar with city bus routes and those who are worried about missing the bus.

The project in Nashville is one of several IoT initiatives aimed at improving how we move, how we move things and how we move smarter. DOT's National Highway Traffic Safety Administration (NHTSA) is exploring how IoT solutions can reduce traffic accidents and improve overall safety on our roadways. The technology, known as vehicle-to-vehicle (V2V) communications, is designed to warn drivers of impending crashes and avoid accidents.

"IoT applications hold great promise for achieving a wide array of societal and economic benefits," said Daniel Morgan, DOT's Chief Data Officer. His advice to those exploring IoT is "to link these activities to your strategic plan and goals. Doing so will help you measure the IoT investment's results. Remember that it's possible to [use] Agile and iterative with IoT technologies — start small and measure along the way. Learn about risk and return on investment, and share those results broadly so that other public-sector agencies can learn and scale."

CONNECTED VEHICLES

TAKEAWAY: ***Morgan says that in general, it's important to spend some time early on thinking about risk and ROI.***

CONNECTED VEHICLES COULD SAVE LIVES

Talking cars are no longer a futuristic wonder reserved for the big screen. We can tell our cars which radio stations to play or what temperature we like the air conditioner set on and they respond to our requests. But even more impressive is the new technology being developed to enable vehicles to communicate with one another.

V2V is being hailed as a game changer. So much so that DOT's Foxx recently announced "that we're going to accelerate our rulemaking process around vehicle-to-vehicle technology so that the government is rolling out the open door for technology to enter in and to help make our transportation system more innovative and more safe."

By year's end, Foxx plans to send a proposed rule to the Office of Management and Budget requiring V2V communication devices in new vehicles.

From there, the proposal will undergo an OMB and interagency review, followed by a public comment period, said Gordon Trowbridge, NHTSA's Communications Director. "We had projected that the public comment period on the [notice of proposed rulemaking] would close by the end of next July. Then we would go through another round of analysis, interagency review and public comment on a final rule."

Speaking at the Global City Teams Challenge Expo in June 2015, Foxx said, "We're putting [in] place smart policies so that we can prepare for the future."

Unlike the current onboard sensors and cameras in some vehicles, V2V communications "use on-board dedicated short-range radio communication devices to transmit messages about a vehicle's speed, heading, brake status and other information to other vehicles and receive the same information from the messages," according to an August 2014 report by NHTSA.

The agency points to two V2V capabilities in particular that it estimates could prevent up to 592,000 crashes and save 1,083 lives per year. One is Left Turn Assist, which warns drivers not to turn left in front of another vehicle traveling in the opposite direction. The other, Intersection Movement Assist, warns drivers not to enter an intersection because the probability of colliding with other vehicles is high.

To help accelerate implementation of connected vehicle technology, NHTSA is launching pilots to test "initial deployments of connected vehicle technology in real-world settings," according to the agency. The goal is to provide near-term safety, mobility and environmental benefits to the public. The CV Pilot Program is a continuation of the connected vehicle research NHTSA has already conducted.

"Now that the NHTSA is pursuing rulemaking, the pilots will serve to spur innovation and enhance existing systems," according to the agency.

A proposed schedule for the program shows two waves of solicitations and awards for connected vehicle technology starting this year. The pilots are scheduled to end in September 2020.

The programs will help answer the following questions:

- What are the institutional, legal and technical issues that may help or hinder the use of connected vehicle technologies?
- Are state and local agencies prepared to implement and maintain connected vehicle technologies?
- How effective is a security credential management system in enabling connected vehicle communications?
- Can customer satisfaction with demonstrated applications be measured?

Key Takeaway: Morgan says that in general, it's important to spend some time early on thinking about risk and ROI. Before forming large-scale partnerships on IoT investments, consider demonstration projects that can help prove your business case and better inform questions about risk allocation. Remember that IoT is an evolving field, and the path to a public/private partnership is not always clear.

NASHVILLE PUBLIC TRANSIT

TAKEAWAY: ***Be aware of what's happening in your community in terms of the resources that are available.***

TAKING GUESSWORK OUT OF PUBLIC TRANSIT IN NASHVILLE

If you've ever visited or lived in a major metropolitan area, then you know firsthand the struggles of being a motorist there.

In Nashville, congestion on the city's roadways has nearly doubled in the past decade, and those numbers will likely grow as the population increases. By 2040, the number of residents in the 10-county metro region could hit 3 million. It doesn't take a traffic engineer to realize that will mean serious headaches for drivers, unless city officials start planning now.

Some of the challenges Nashville faces are limitations in deploying the types of mass transportation networks that larger cities provide, improving public engagement and increasing the efficiency of public transit.

One way to alleviate traffic is to increase ridership among so-called choice riders and to encourage those who never use transit to get on board, said Rob McElhaney, IT Manager at Nashville's Metropolitan Transit Authority (MTA).

For Nashville, the answer may lie in a new app called TransitHub, or T-HUB for short. What makes this app interesting is all the magic happening behind the scenes that allows users to track bus locations in real time, estimate trip times and receive alerts when they leave their current locations to catch a bus.

The city is partnering with Vanderbilt University's Institute for Software Integrated Systems and Siemens Corporate Technology to develop the app. Nashville MTA had already been working on a project to install sensors on its fleet of about 170 public buses, said Dan Freudberg, the authority's Scheduling Manager. The system of sensors provides MTA with real-time vehicle location information and data showing about how far ahead of or behind schedule buses are running.

Here's how T-HUB works:

The system, which is composed of hardware and software, uses a simulator to predict traffic patterns and advanced analytics to determine arrival and departure times for the buses. Data feeds from the city power the system.

The city collects sensor data from the buses every minute (on a staggered schedule), and that information is posted to a server that the university can access. All data on the server is updated every 10 seconds to keep pace with the various data feeds coming in, McElhaney said.

T-HUB allows riders to plan future trips and evaluate multiple trip options simultaneously. It also enables city officials to assess and improve routes and transit options, based on models generated from ridership data.

The work began in January 2015, and MTA engineers are now partnering with the university to test the app's alpha version, said Abhishek Dubey, Vanderbilt's Principal Investigator for the project. The goal is to have a functioning app available for iOS smartphones by year's end and eventually for Android phones, too.

The team is still finalizing additional features, such as calculating the calories people burn by using public transportation and walking, a carbon emissions count, and other campaigns that could allow users to collect points for using the app and to redeem them for free or reduced bus fares, Dubey said.

"The heart of it is to make transit easier to use," Freudberg said of T-HUB.

Key Takeaway: Be aware of what's happening in your community in terms of the resources that are available, McElhaney advised. Even if they aren't working specifically in your field, there are folks who have the expertise to solve the problems that you're facing.

WELCOME TO THE

Internet of Everything

Every day, the Internet of Everything grows exponentially. Millions of devices and people are connecting, developing ideas and solutions that are the first of their kind. But these firsts are only truly interesting for the lasts they create. The last traffic jam. The last product recall. The last blackout. These are what motivate us, because we know big things are never achieved by thinking small. And those big things start here and now.

cisco.com/go/convergencegov

CISCO

The Future of the Internet of Everything in Government

An interview with Chris Cressy, Federal Sales Manager for Internet of Things, Cisco

At its essence, the Internet of Everything (IoE) is the connection of people, processes, data and things over Internet protocol (IP) networks. And the public sector needs to be paying close attention as this buzzword develops into actionable technology. That's because IoE is creating unprecedented value to both the private and public sector. Cisco estimates that IoE will generate $19 trillion in value over the next 10 years for the private and public sectors combined.

To learn more about the future of IoE in the public sector, GovLoop sat down with Chris Cressy, Federal Sales Manager for Internet of Things at Cisco, to discuss how government can take advantage of this technology.

First, Cressy stressed that there is a difference between two terms – Internet of Everything and Internet of Things – that the public sector needs to recognize.

"The Internet of Things is about connectivity – connecting machines, devices, sensors, and non-IT systems," Cressy explained. "The Internet of Everything expands on IoT by connecting devices to people, managing immense amounts of IoT data, and processing this data into actionable intelligence, increased productivity, and value for customers. Another way to look at it, said Cressy, is that the Internet of Everything are solutions that are developed around the Internet of Things.

So what does the Internet of Everything mean in the context of government and government services? In short, the technology will affect every sector, from the military to state and local government.

"Some of the key uses of the Internet of Everything in the public sector are in reducing and managing energy usage; networking and monitoring of critical infrastructure for protection and cybersecurity; deployment of sensor systems for both intelligence and citizen services, and secure mobile communications," Cressy said. Cisco has been working with U.S. defense agencies to deploy secure mobile communications systems for over 10 years. Cisco embedded routers and switches are deployed in thousands of ruggedized, mobile communications kits. Cisco embedded products, along with industrial Ethernet, wireless and security products are now being adopted by civilian agencies for border security and state and local law enforcement.

Based on bottom-up analysis of 40 public sector use cases covering cities, agencies, and verticals such as healthcare, education, and defense, Cressy explained that benefits government can gain from IoE technology include increased revenue, increased productivity, new operational capabilities, and enhanced citizen services.

For those in government looking to implement the Internet of Everything, Cressy had a variety of best practices to offer.

"Public sector administrators and CIOs should look for starting points with converged IoE solutions that provide immediate value and ROI, but also lay the framework for future IoE solutions," he said. "At Cisco, we have focused on validated designs and solution architectures for many years. Those architectures now provide a powerful framework to implement IoE solutions. For example, a converged network of fiber, copper, wireless, and security can provide a pervasive framework for IoE across a campus or an entire city."

Security is paramount for IoE. "At Cisco, what we have developed a comprehensive security architecture for the enterprise that we are now extending to IoE systems," Cressy explained. "We are using essentially the same security tools to secure IoE infrastructure that we do for an enterprise. That means that organizations can establish consistent, comprehensive security policies for access, authentication, and intrusion across all their infrastructure, whether it is IT or Operation Technologies (OT). Moreover, OT systems can be made more secure by real-time cybersecurity monitoring over IT networks. The old paradigm of separate, isolated networks and air-gap security is no longer sufficient. So whether it is connectivity to building systems, energy systems or transportation systems, all these systems can now benefit from IT security solutions.

Cressy concluded by encouraging public sector leaders to truly realize the scope of IoE technology.

"We are going to be connecting orders of magnitude more devices with IoE than we have now – at least tenfold in the next ten years," he said. "Ten years from now, everything that can be, will be connected. The power and value of the IoE networks will be hundreds of times, if not thousands of times greater than the value of a today's networks. I think the transformation that that IoE expansion will have in the world is going to be completely unprecedented. And what that means is, we need to prepare today."

SECTION FIVE

The Internet of Things & the Workforce

IoT is changing the public workforce, from how employers and employees interact to how employees are trained. This means preparing workforces accordingly and managing IoT platforms will become essential. The challenges that lie ahead for IoT and the workforce include everything from training and ethics to security.

One example? Through Global Positioning System technology and sensors, IoT has enabled public employers to track their employees. Some agencies are creating visual maps of workers' days in hopes of improving productivity. Public emergency response teams have already begun using IoT for simulation training. These efforts, however, are still in the beginning stages of development.

But privacy and ethical concerns surrounding tracking employees must be considered. Some workers' advocates say that tracking employees in this manner can affect employee morale and build resentment toward employers.

The military is also investing more in IoT through robotics and unmanned systems. The Defense Department's investment in robotics has been surprisingly slow, however, and most of these systems are still semi-autonomous. What's more, many ethical and security-based concerns remain here, too: Will robots take soldiers' jobs? Will soldiers be willing to fight alongside autonomous robots? Can they depend on them in the battlefield? The idea of robots completely replacing human-operated systems on the battlefield conjures up images of a scary sci-fi film: "Robots Take over the World."

Furthermore, critics are concerned that dependency on IoT (through robotics and unmanned systems) could compromise human safety. Such systems lack humans' agility and complexity, and there is always room for error — even with technology.

So how do we navigate these challenges?

If used effectively, IoT can improve public workforce effectiveness, help save lives and protect our soldiers. There are many ways to enhance worker productivity while ensuring privacy. Additionally, investment in autonomous systems shows much promise for the military workforce, which can dispel fears of robots stealing jobs.

Additionally, there are ways to navigate the privacy and ethics challenges. Informed consent is key to better simulation training. Make sure that participants are aware of the purposes of sensors, employee tracking and visual mapping. Demonstrate to employees how such methods have improved performance in the past. Assure employees that information collected during simulations is used solely for training purposes, and attain written consent before publishing any data.

Government cannot be alone in merging IoT and the workforce. Successful local and federal IoT projects came about through the collaboration of public and private entities. Draw on expertise from academic institutions, private companies and other government agencies. Do not be afraid to get creative. Most of these projects can be put together at low costs and by groups of volunteers. Tap into the passion and creativity in your community. You'll be surprised at what individuals can tackle by bringing in expertise to address IoT.

To better use IoT technologies, you need to help employees trust them. That's why trial and error is essential. Demonstrate and practice with systems to enhance familiarity and safety. Though they'll never be like humans, IoT systems can enhance workforce capabilities and help complete the most dangerous jobs.

The following local and federal case studies can help you see the benefits of IoT to the workforce — particularly in the areas of emergency response training and combat.

EMPLOYEE TRAINING

TAKEAWAY: ***Using sensors and ecosystems for simulation training requires employees to learn from mistakes and failures.***

HOW IOT CAN IMPROVE EMPLOYEE TRAININGS

The Ecosystem for Smart Medical Team Training (ESMTT) in Fairfax, Va., was composed of a complex, live training drill that transmitted sensor data from a first responder team at a simulated accident site to a medical team at Inova Fairfax Hospital. The project was conducted by a team of emergency response professionals from the hospital and Fairfax County Fire and Rescue in addition to professors and students from Georgetown University, George Mason University and University of Maryland.

"The ecosystem allows for devices to talk to one another and automatically collect data through a software protocol called Experience API," said Dr. Brenda Bannan, Associate Professor in Instructional Technology/ Learning Technologies Design Research Programs at Mason and a team leader of ESMTT.

Bannan explained the basics of the exercise, first developed by DoD's Advanced Distributed Learning Initiative as open source software. Dozens of Bluetooth proximity beacons, activity sensors and ultra small microcomputers were attached to emergency response technicians, firefighters, the dummy "victim," equipment and ambulances. Those sensors were also wirelessly connected to a cloud-based data analytics system.

During the exercise, the locations of responders in relation to the victim and to one another were collected for later analysis. The information was also transmitted to emergency room doctors waiting for the patient. The data was displayed for responders to review on a visual network graph, made possible through a system called Yet Core. Designed by Yet Analytics, it's a learning management system that connects operation and training data from existing systems.

"What excites me about IoT is it improves our everyday real-world types of experiences, which is great for training and performance," Bannan said. "We're also able to automatically collect data about real-world behavior. We're busting out of the box of the computer and allowing for networked capability that allows for automatic and invisible data collection."

The invisible exchange of information through IoT helped firefighters and public responders better identify what can go wrong in an emergency response. After the simulation, participants took part in a collaborative debriefing session to review and learn from the exercise.

"Most of the learning happens in debrief. Emergency response and medical teams all debrief together in one room, which is pretty unusual," said Bannan. Usually, there is little analysis of response tactics after an emergency incident. By facilitating this group discussion, participants were better able to identify exactly what went wrong during the simulation.

For example, one trauma surgeon said that even though she thought her team was doing everything quickly and efficiently, she really couldn't tell in real time. She thought this type of simulation could help the team address exactly what can go wrong in an emergency response.

"The simulation is able to track fine-grain behavior," said Bannan. "You can see how many people walked in and out right after the emergency happened. Then, you can drill down into individuals' behaviors. One of the best ways to improve behavior is to show that behavior back to the teams for their own reflection and enhanced awareness. That helps improve employee performance over time."

But when it comes to IoT, there are always challenges in implementation, especially with government. "Every technology that comes along has pros and cons," she said. "Challenges include privacy and ethics. We have so much to gain by understanding the good of what these technologies can do by facing these challenges and doing it in a way that is sensitive to the individual."

She suggested that Fairfax Fire and Rescue, for example, safeguard data being transcribed during simulations and infuse informed consent into such trainings for personnel. "This helps to protect human subjects who may not know what the data is going to be used for. It's a real tension, as sometimes data is used for things it wasn't intended for," she said.

As for using IoT to improve the training of public workforces, Bannan said "government should try new things and look at the Internet of Things. There's always opportunity for design and you're always going to have constraints. Charge your teams to be change agents. Government employees do a great job of working in their restraints, trying to solve problems and innovate."

She added: "It's a process of looking for spaces to make a difference in some way. Use creativity to innovate and try something even if it may fail."

Key Takeaway: "Fail early and fail often." Using sensors and ecosystems for simulation training requires employees to learn from mistakes and failures. "To not be afraid of failure means trying new experiences. There are things that went right, there are things that went wrong," said Bannan. "But we have learned in an amazing amount of time just by designing, implementing and then learning from that experience."

TAKEAWAY: ***Killion advises that government agencies take advantage of the advances in autonomous technology being made.***

UNMANNED VEHICLES

UNMANNED VEHICLES AND AUTONOMOUS SYSTEMS

The Office of Naval Research's (ONR) Office of Technology facilitates technology transition to the fleet, force and acquisition communities. It serves as the Science and Technology Directorate under the Department of the Navy. Recently, ONR has dedicated more time and resources to unmanned vehicles including UAVs, unmanned surface vehicles (USVs) and Unmanned Underwater Vehicles as well as robotics — particularly transitioning from semiautonomous to fully autonomous capabilities and systems.

'The advantage of unmanned systems is that they take care of the dull, dirty and dangerous jobs," said Dr. Tom Killion, Director of the Office of Technology. "Dull as in being stationed for a very long time where human endurance is limited; dirty in terms of operating in toxic environments for humans; and dangerous where humans would be exposed to explosive devices and hostile forces."

Just last summer, ONR demonstrated its first Control Architecture for Robotic Agent Command and Sensing (CARACaS), which is part of its autonomous swarm boat strategy. Using sensors and advanced software, CARACaS allows unmanned Navy vessels to operate without a sailor at the controls. Other features include ease of installment in any boat, operating in sync with other unmanned vessels, choosing routes independently, swarming to intersect enemy vessels and protecting naval assets.

However, Killion emphasized that even with autonomous systems, the human element is not likely to be eliminated. Instead, the nature of the job is shifted. "In all cases, there's a human element to unmanned systems, even if it's nothing else than managing those assets, planning how they would be used and launching their mission while controlling certain decisions," he said. "The only thing unmanned about unmanned systems is the platform itself. These don't eliminate the need for humans. They allow humans to do their job in a different way and with less risk."

One challenge with developing completely autonomous systems is that they often lack sophistication that humans have when navigating complex and ambiguous environments.

"We've made progress but we're not there yet. These robots and USVs can operate autonomously for significant periods of time, but they still require intervention at critical points. We had problems with unmanned ground vehicles being able to maneuver independently across terrain. We eventually had to get sensors that allowed them to do that," Killion said.

Another challenge is verifying autonomous systems' performance. "How can humans using these software-based entities be sure they're programmed effectively enough to operate on their own?" Killion asked. "How do you test that to the point where you trust it to operate safely and effectively in a wide variety of environments and under what conditions?"

This is why most autonomous technologies are actually semiautonomous. Yet, there is hope for government to develop completely autonomous systems in the future. "The good news is that there are new technologies coming about, like neuromorphic chips," Killion said. "They're built into hardware and operate like the neural network that underpins our intelligence, our brains, and how we operate. That will allow these systems to do rapid scene recognition more effectively and better adapt in the environment."

In terms of the future of IoT and autonomous systems, Killion said, "the biggest thing going forward is really about building trust in unmanned systems, just like you would trust another person in your squad."

When considering government strategies for incorporating more autonomous systems, it is helpful to look to DoD and its use of unmanned vehicles. "The good news about the experience we had in Iraq and Afghanistan with unmanned ground vehicles was our soldiers got used to it and, as a result, were less at risk because they could use the robot to go into more dangerous situations," said Killion. "We were also training an entire generation of soldiers, sailors, airmen and Marines to incorporate robots as partners in their operations."

But we still have a long way to go before we see completely autonomous systems and robotics in the military. The key to progress is to "demonstrate, demonstrate, demonstrate," Killion said. "You want to give whoever the user is the chance to have experience with these systems on a routine basis. It's not just about the technology; it's about the people who enable that technology."

Key Takeaway: Killion advises that government agencies take advantage of the advances in autonomous technology being made. "We do a lot of research with universities in the area of autonomy and the basic sciences that underpin it," he said. "Google and Amazon have gotten interested in autonomous systems for various applications and are starting to invest in the researchers and industry partners that we have traditionally funded. That's good news for us. Somebody else is helping to invest and pay for advances in the technology that will then come back and benefit us in the long run."

SPOTLIGHT

The Thingstitute of Montgomery County, Md.

AN INTERVIEW WITH DAN HOFFMAN, CHIEF INNOVATION OFFICER FOR MONTGOMERY COUNTY, MD.

In a recent interview, Dan Hoffman, Chief Innovation Officer for Montgomery County, Md., answered our questions about his Thingstitute, an incubation lab for the county's Innovation Program and its IoT projects. The Thingstitute is fostering IoT innovation through a combination of private-sector know-how and the convening power of government.

GovLoop: *What is the Thingstitute?*

Hoffman: The Thingstitute is an organizing body. It's an initiative within the Innovation Program of Montgomery County that's meant to establish the county as a living lab for IoT devices. It's really meant to organize test beds, which give opportunity not only to the county to deploy devices and see how they impact [the] public sector, but also to startups and companies that have devices they want to prove in a real-world setting.

GovLoop: *Why are you focusing on IoT within Montgomery County?*

Hoffman: There's a recent story that shows why it's important to get government involved in IoT. This past winter, a family in Maryland had their power shut off. The dad ran the generator overnight to keep the house warm, but the house filled with carbon monoxide and the family died.

That's why we're doing this. Having a connected device in that situation could have alerted the fire department. The power was off, but it could have even told the fire department that the battery on this device was dead or the device was not functioning. Those are all that could have prevented that. Making IoT affordable and available for everybody is one of the underlying goals of the project.

GovLoop: *How does the Thingstitute benefit IoT device and sensor developers?*

Hoffman: If you are a startup and you have a sensor device or particular complementary IoT technology, you might not know where to go to find the right person to talk to. You need somebody within the local government that's going to help shepherd your project and make sure you're getting introduced to the right folks. Those are the types of things that we try to facilitate.

We also really bring a lot of other complementary startups together. In our senior living facility, for example, we have 15 different organizations, including academic institutions as well as a bunch of different startups that have a variety of products. Some of them just make the sensor chip, for example. Other ones may actually make the mesh networking devices that the chips can sit on. Some of them are cloud service providers or cellular providers, like AT&T or IBM. We bring together a small ecosystem and create partnerships that one startup, by itself, couldn't bring together.

GovLoop: *Can you give me an example of how this works in practice?*

Hoffman: Our first test bed is at a senior living facility where we're working with residents to deploy devices, test devices and in some cases even prototype devices. It's called SCALE, which stands for Safe Community Alert Network.

GovLoop: *What can you apply from SCALE to future Thingstitute endeavors?*

Hoffman: SCALE was the first and biggest test bed. Now, it's also providing a platform for everything else because we can replicate what we built in SCALE for other areas. For SCALE, we built a data-in-motion exchange, which is an open data platform for sensor data that we built in the cloud. We can feed sensor data from many sources into the data exchange.

From there, we can build applications on top of it. So for instance, we can gather data from a correction center and if one of the sensors senses an event that we need to be alerted to, the data goes up into the data exchanges. Then, it can trigger text alerts to our cell phone, it can reach to our dashboard and it can inform our emergency operation center.

GovLoop: *Why is it important for the public sector to drive IoT development?*

Hoffman: Right now, the government really only controls a fraction of the infrastructure that residents encounter in their day-to-day life. But I equip my house with a variety of sensors for my health and safety. How do we get that data in a way that is efficient and useful to a first responder?

We can't tell people to go buy the Honeywell device or the Samsung device or the Nest device. That's not the role of government. The role of government is just to get the data we need and make sure people are safe.

We need standards and they have to be national because no one is going to make a smoke detector to the Montgomery County specification. That's why we work so closely with NIST, the National Institute of Standards and Technology, to help move that conversation along so that there are standards in place that will allow us to get this project and the devices to share data with us.

software AG
Government Solutions

Take a “Special Forces” Approach to Enterprise IT

Helping Agencies Prove IT First and Prove IT Fast

Software AG Government Solutions is a leading software solutions company, delivering massive-scale, complex and real-time solutions for:

- Business Process Management
- Integration
- Analytics & Visualization
- Application Optimization

Put our team to the test.
Learn how our "special forces" approach can get fast results for your most complex integration and process challenges. Visit: www.SoftwareAGgov.com

GET THERE FASTER

Extracting Value from Your IoT Data

An interview with Chris Steel, Chief Solutions Architect at Software AG Government Solutions

As organizations connect more devices, they produce more data. This isn't an earth-shattering revelation. In fact, that's the point of the Internet of Things (IoT). However, Chris Steel, Chief Solutions Architect at Software AG Government Solutions, an enterprise software company, explained that the implications of that data deluge are worth thinking about.

"If you think of the amount of additional data that agencies are now going to being exposed to through the Internet of Things, they are just simply not prepared to deal with it," Steel said.

According to Steel, many organizations make the mistake of accumulating unnecessary data, in case they find relevance for it later. "Up until now that's been fine, because our storage capacity has been increasing exponentially over last 20 years," he explained. "But what the Internet of Things does is bring a whole new magnitude to the amount of information that we're trying to grab, and we just simply aren't going to be able to take the traditional approach and store all that data for later analysis."

Accommodating IoT data requires a more thoughtful approach. "What we need to do is decide up front what the valuable data is and triage it. Determine what data you'll ingest, how you're going to store it, and for how long," Steel said. "Otherwise we're going to be overwhelmed with this deluge of unnecessary information that's going to tie up all of our storage and hamper efforts to analyze it."

Steel advised starting your IoT data analytics journey by first deciding what questions you're trying to answer or what opportunities you're trying to seize. This is in contrast to the approach many organizations take, where they look at their cache of data to determine both the problem and solutions it might provide. However, starting with a problem allows an agency to extract the data that could offer a solution and discard the data that won't.

Once an organization targets the data that will solve its original problem, it can begin to invest in analytics. Steel said agencies, in order to best approach this investment, must take a holistic approach. "We're not going to have one tool or one process that's going to allow us to seize these opportunities. What we need is an entire architecture that's going to have a lot of different pieces," he said.

According to Steel, specific components of this architecture will vary depending on unique business needs. However, certain tools will be necessary across all organizations:

- **Real-time streaming analytics engine:** "This is going to be able to scale to millions of events per second," Steel explained. "That will allow us to ingest all the different data we're getting from different sensors and devices and perform our analyses in flight, storing only the results, rather than all the unnecessary raw data."
- **Predictive analytics:** This capability allows organizations to detect and mitigate problems before they occur, preventing disruptions, saving costs, and decreasing maintenance requirements.
- **Visual analytics capabilities:** "Now that we have all this data, it's easy to get overwhelmed. What we want is a powerful class of visual analytics tools that allow us to sift through it to find the right data," said Steel. Such a tool permits organizations to easily identify anomalies without having to manually parse through large amounts of data.
- **Integration engine:** This component allows different connected devices, operating on different protocols, to work together.
- **In-memory computing:** The value of data comes from being able to take action. Therefore, "we need to be able to do the analysis right here in the moment, and to do that we need in-memory computing," said Steel. Storing data in memory allows for faster processing speeds to quickly execute analytics.

The way these components integrate to create a holistic architecture specific to an organization's individual needs will vary. That's why Software AG always takes the time to first talk with government customers about what value they want from their connected devices and the data they produce. Then, they create a proof of value demo to test the proposed architecture before it's implemented.

"What we want to do is provide access to the right data in the right time frame so that we can take action on it or gain opportunity out of it," Steel noted.

Finally, Steel re-emphasized that it's important to remember that the power of the IoT lies not in the sheer volume of data and connections that it contains but in the timely access to the right data that it makes possible. With access to the right data sources, with tools to capture, manipulate and make sense of that data in real time, and with an architecture designed to enable a well-considered, real-time response to the opportunities presented by a specific situation, an organization can be well-positioned to succeed in the IoT.

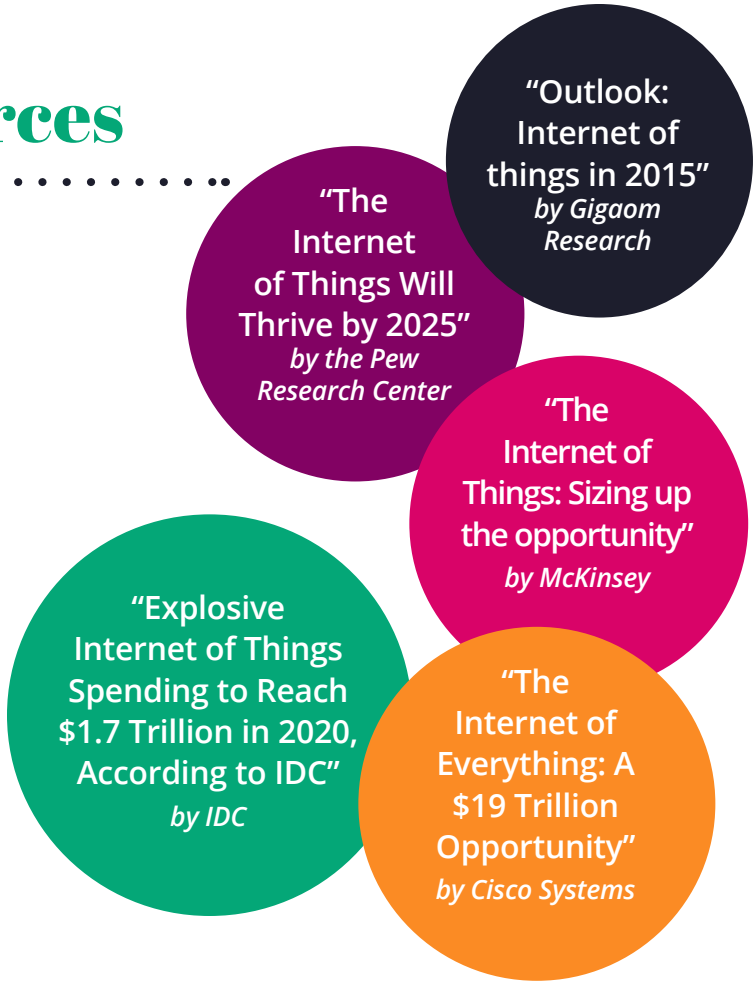
Conclusion & Resources

Whether we're ready or not, the Internet of Things is becoming a reality. A McKinsey study estimates that the economic impact of IoT will be more than $6 trillion in 2025. From selling fitness-tracking consumer devices to building smart sensors in retail stores, the private sector is already actively building IoT and leveraging it to optimize their businesses.

Our question: What role do we see government playing in this new arena?

What's been made clear is that governments are starting to move from the sidelines into IoT. And as we've seen from the case studies in this guide, IoT will have an impact on every vertical within the public sector, including training, transportation, technology and healthcare, just to name a few.

With some efforts in innovation, problem solving and creative uses of technology, the public sector can truly start to take advantage of IoT to create efficiencies and cost savings and to help citizens live better lives. We can't wait to see what you'll do with it.



Acknowledgments

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 200,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

GovLoop
1101 15th St NW, Suite 900
Washington, DC 20005

Phone: (202) 407-7421 | Fax: (202) 407-7501

www.govloop.com | @GovLoop

ACKNOWLEDGMENTS

Thank you to BDNA, Cisco, Hitachi Data Systems, Avnet Government Solutions, Red Hat and Software AG for their support of this valuable resource for public-sector professionals.

AUTHORS

Catherine Andrews, Director of Content
Francesca El-Attrash, Editorial Fellow
Emily Jarvis, Senior Online and Events Editor
Nicole Blake Johnson, Technology Writer
Hannah Moss, Researcher and Writer

DESIGNERS

Jeff Ribeira, Creative Manager
Tommy Bowen, Graphic Designer
Kaitlyn Baker, Design Fellow
Daniella Conti, Design Fellow

PHOTO CREDIT

Family O'Abe, U.S. Navy, COD Newsroom, Montgomery County Planning Commission, Army Medicine, U.S. Army Corps of Engineers Europe District, California National Guard, NPS Climate Change Response, Olabi Makerspace, Ted Eytan, Salticidae.

1101 15th St NW, Suite 900
Washington, DC 20005

Phone: (202) 407-7421 | Fax: (202) 407-7501

www.govloop.com
@GovLoop