INTERNET OF THINGS: PROGRESS, RISKS, AND OPPORTUNITIES

TechRepublic

TABLE OF CONTENTS

03 How IoT is reinventing IT architecture
06 Internet of Things: A guide for business leaders
15 Internet of Things in 2019: Five predictions
17 The five biggest IoT security failures of 2018
20 Four ways to combat new IoT security threats at the firmware level
22 Six ways government projects will influence big data and IoT in 2019
24 How IoT medical devices save your life and threaten your privacy
26 How to leverage the industrial Internet of Things
28 How to become an IoT developer: Six tips
31 The five industries leading the IoT revolution

HOW IOT IS REINVENTING IT ARCHITECTURE

BY MARY SHACKLETT

For the last five years, technology pundits have been talking about how cloud computing, big data, and security will reinvent IT architecture and thinking. But companies move at different rates than pundits do, so while IT architecture has changed, change has often come about informally and incrementally—and not as part of any long-range strategic plan.

However, IoT—with its reliance on edge computing—is a different story, because edge computing takes you away from the central data centers and data repositories that characterize traditional IT architecture. Corporate security governance must also be extended in new ways to the edges of the enterprise and different types of clouds and on-premises systems must be able to seamlessly and securely exchange information.

In this new world, strong middleware that can automate integration between systems, clouds, and on-premises systems is critical. So is awareness of all your company's IT assets and the ability to fail over systems if disaster recovery becomes necessary.

How can IT leaders ensure that they're covering all the bases when they implement IoT? Here are five best practices.

1. MANAGE YOUR ASSETS

As many as 65% of companies today do not have fully developed IT asset tracking and management systems. This comes at a time when shadow IT—where end users are purchasing and installing systems and devices without IT's knowledge—makes up 30% to 40% of enterprise IT spending, according to Gartner.

If no one is actively managing these assets, they become vulnerable to security penetration and breaches.

IT asset management software can detect new appliances and systems as they enter IT networks and can provide a way for logging and monitoring these assets. If your company lacks such a system, now is the time to consider acquiring one. Knowing every piece of technology that is in your enterprise, and the data it contains, is vital to developing a comprehensive and totally inclusive IT architecture.

2. BE PREPARED FOR ODDBALL IOT

One of the implementation challenges of IoT is that every IoT vendor, whether it is providing an RFID reader, a robot, or a CNC machine, is primarily concerned with the immediate operating and data universe of the IoT solution itself. Consequently, there are many "oddball" IoT communications protocols that don't necessarily talk to other devices or systems. Fortunately, there is commercial middleware software that can automatically translate these oddball IoT protocols into more common protocols that will make communications with your other devices and systems possible. Your IT architecture should reserve a spot for an automated communications protocol translator.

3. FORMALIZE A PLAN FOR EDGE AND HYBRID CLOUD COMPUTING

Internet bandwidth is too limited to enable real-time data payload transmissions from servers in plants and remote facilities to a headquarters data center. This is a challenge because you ultimately want to bring all this data together in a central repository, most likely on premises and at headquarters, so your managers and others with a business need to know can query and perform analytics.

For most sites, finding a way to move data that is locally collected at the edges of the enterprise to a central data repository requires a combination of cloud and on-premises computing, in concert with a scripted communications plan that schedules data payload shipments from the remote edges of the enterprise to cloud storage—and from cloud storage to your central data repository, which could be on premises.

Orchestrating this data storage and transport plan requires a reworking of your IT architecture.

4. REVISE YOUR DISASTER RECOVERY AND BACKUP PLAN

If you're like most companies, which now use a combination of on-premises, private cloud, and public cloud computing—where do you back up and recover your data during a disaster?

Many organizations are opting to back up central data to the cloud on a nightly basis, with the cloud being either private or a single-tenant public cloud. This means reworking the DR plan so that it now includes both cloud and on-premises computing and so it's in concurrence with revisions to your IT architecture.

Revising the DR plan will be on companies' to-do list anyway, since 30% still have no disaster recovery plan in place.

5. ENACT "ALL POINTS" SECURITY

One way to ensure security at the edges of your enterprise where end users are likely running the technology is to implement a zero-trust network, which automatically verifies IP addresses and authenticates users from both inside and outside corporate walls. No one gains admission to the network until all security criteria have been met. With an enterprise-wide zero-trust network, IT doesn't need to confront end users about security when they self-enable their technology.

INTERNET OF THINGS: A GUIDE FOR BUSINESS LEADERS

BY TEENA MADDOX

The Internet of Things (IoT), refers to the billions of devices around the world that are connected to the internet through sensors or Wi-Fi. Each device collects data, and this data, known collectively as big data, is exchanged and analyzed.

An IoT-connected smart device can be an everyday item such as a phone, car, watch, washing machine, or refrigerator. IoT devices can also be components of machines and systems, such as those found on an oil rig or airplane engine.

As costs go down, IoT is more accessible than ever. Gartner estimates that about 8.4 billion IoT devices were in use in 2017, up 31% from the previous year, and expects the number to hit 20.4 billion by 2020. Total world spending on IoT reached about $2 trillion in 2017.

IHS, a global data and information services business, said that by 2030, 125 billion connected devices will be part of our daily lives.

WHAT IS THE IOT?

IoT is a layer of digital intelligence that makes a device smarter than it would be on its own. When connectivity is added to a device, the items become known as smart: smartwatch, smartphone, smart refrigerator.

As Lisa Elénius Taylor, head of IoT marketing for Ericsson explained, "at the most basic level, the Internet of Things is a network of devices, vehicles, and appliances that have software and connectivity capabilities that enable them to connect with one another and exchange data."

Examples of common IoT devices include a diverse collection of small items such as smart thermostats that learn your preferred home temperature, light bulbs that alert you to outdoor air quality, smart locks you can open from an app on your phone, and stuffed toys that calm your child at night. It also includes bigger items, such as driverless vehicles, jet engines, and sensors on a machine in a manufacturing plant, which are sometimes called machine-to-machine (M2M). In addition, there is industrial IoT, which is known as IIoT.

Typically, IoT devices are items that, in the past, weren't connected to the internet. Every year at CES, for instance, there's a wealth of new IoT-connected devices that amuse and astound, such as connected diapers to tell you when your baby needs to be changed, and pillows that stop your spouse from snoring.

However, it's not just **things** that make up IoT—it's devices, as well as insights gathered from the data, and the action taken based on the data.

IOT AND BIG DATA

The vast amount of data collected by IoT devices is known as *big data*. This data is used for everything from predictive analytics to determining the best way to market to a customer. Many companies have spent years collecting data and still haven't figured out what to do with it. This data is valuable, and data scientists are among the most in-demand careers in tech.

Cisco calculates that machine-to-machine connections that support IoT applications will account for more than half of the total 27.1 billion devices and connections and will account for 5% of global IP traffic by 2021.

IOT AND THE CLOUD

Since such vast quantities of data are being transmitted through IoT devices, for many companies it is necessary to use the cloud for data processing. Cloud computing giants such as Microsoft, Amazon Web Services, and Google Cloud are among those offering IoT services.

Additional resources

- Quick glossary: Internet of Things (Tech Pro Research)
- Edge computing: A cheat sheet (TechRepublic)
- MiOS, a software platform for IoT: Cheat sheet (TechRepublic)
- The power of IoT and big data (Tech Pro Research)
- Research: BYOD, wearables, and IoT (Tech Pro Research)

WHEN DID THE IOT REVOLUTION BEGIN?

The 1980s and 1990s were about more than bad fashion and better music—the concept of adding sensors and intelligence to commonplace items became a topic of discussion. The technology didn't yet exist to make it happen, so progress was slow.

The adoption of RFID tags (low-power chips that can communicate wirelessly) solved some of this issue, along with the increasing availability of broadband internet and cellular and wireless networking, according to ZDNet's Steve Ranger. The adoption of IPv6 was also a necessary step for IoT to scale.

Kevin Ashton, a British technology pioneer working on RFID, coined the phrase "Internet of Things" in 1999, although it took at least another decade for the technology to catch up with the vision.

IoT was at first used mostly in the enterprise, such as in manufacturing, but now when most people think of IoT, they also think of smart devices in their home, ranging from thermostats to AI-powered speakers and home security systems.

WHAT ARE THE BENEFITS OF IOT FOR BUSINESSES?

Businesses use IoT for detecting and troubleshooting issues remotely, predicting maintenance needs, tracking production line efficiency, monitoring devices, and in other ways. These are all things that directly impact a company's revenue.

IoT is growing fast, and businesses are relying more on IoT for operations. Often, the addition of IoT in the enterprise is known as a *digital transformation*.

International Data Corp. reported that the three industries expected to spend the most on IoT this year are manufacturing ($189 billion), transportation ($85 billion), and utilities ($73 billion).

Taylor said, "IoT has the potential to change industries at its core. The digitalization that IoT is part of is sometime called the 4th industrial revolution. Since IoT can affect anything that can be connected it means that IoT is truly an ecosystem of ecosystems where coopetition is a typical element. Companies work together in different constellations for different business needs and create joint benefits. To act in an ecosystem environment is paramount in IoT. The value of IoT lies in the data that the connected devices collect."

Additional resources

- Enterprise IoT calculator: TCO and ROI (Tech Pro Research)
- Harnessing IoT in the enterprise (ZDNet special report) | Download the report as a PDF (TechRepublic)
- How to start an IoT project at your company (TechRepublic)
- How to monetize your IoT project: 6 steps (TechRepublic)
- How to use IoT to save money on your office bills (TechRepublic)

WHAT ARE THE BENEFITS OF IOT FOR PERSONAL USE?

IoT can make tasks easier. If you have a connected refrigerator, it's possible to use a mobile app to glance inside your refrigerator to see whether you have an ingredient, even when you're at the grocery store. By adding connected light bulbs to your home, you can turn on lights with simple voice commands. The possibilities are endless.

Additional resources

- How Louisville became the first smart city on the IFTTT platform (ZDNet)
- Smart hubs, IFTTT & Raspberry Pi: How to get started with home automation (CNET)
- A personal story: Did the Apple Watch save my life? (ZDNet)
- How wearable sensors helped the US Olympic team win 121 medals at Rio (TechRepublic)

WHAT ARE THE SECURITY RISKS OF IOT?

The biggest downsides of IoT include reduced privacy and security risks. If an item you use is connected to the internet, the opportunity for undetected surveillance is enormous.

IoT privacy and IoT security are ongoing concerns for consumers and enterprises. No one wants to have their personal information shared without permission, yet when a customer opts in to an app or shares their data with their smartwatch manufacturer, personal details are being collected and analyzed.

Sensors throughout the home can be used to determine all sorts of details about the home's occupants. Wearing a smartwatch during sex can even lead the manufacturer to know when you and your partner are having intercourse because of mutually elevated heart rates and activity via real-time data.

"The IoT bridges the gap between the digital world and the physical world, which means that hacking into devices can have dangerous real-world consequences. Hacking into the sensors controlling the temperature in a power station could trick the operators into making a catastrophic decision; taking control of a driverless car could also end in disaster," Ranger said.

Additional resources

- As IoT attacks increase 600% in one year, businesses need to up their security (TechRepublic)
- IoT security: What you should know, what you can do (free PDF) (TechRepublic)
- Photos: The 11 least secure connected devices (TechRepublic)

HOW DO SPECIFIC INDUSTRIES AND SMART CITIES USE IOT?

IoT for manufacturing

Manufacturing equipment can be monitored through sensors and advanced analytics; this is also known as M2M, Industry 4.0, and IIoT. The combination of predictive analytics and maintenance may reduce expensive

downtime in a manufacturing facility. Operational productivity and profitability are improved in a connected factory.

Connected factories include tools with sensors and mobile apps that can be used to help workers and technicians be more efficient and accurate. GE Aviation is using Upskill's Skylight industrial AR platform with Google Glass to improve efficiency and avoid manufacturing maintenance errors.

Hershey leveraged IoT, cloud computing, machine learning, and big data to regulate production at its factories and save $500,000 for every 1% of improved efficiency.

Additional resources

- How an Indiana IoT lab is digitally transforming manufacturing and agriculture (TechRepublic)
- How to leverage the industrial internet of things (ZDNet)
- How IoT and big data improved Toyota's manufacturing process (TechRepublic)

IoT for smart cities

This year, 2.3 billion connected things will be used in smart cities, according to Gartner. The global market for smart city solutions and services was $36.8 billion in 2016 and is expected to top $88.7 billion by 2025, according to Navigant Research.

Smart cities have a variety of IoT devices in place, from parking sensors connected to a mobile app to alert drivers of open parking spots to video cameras in smart streetlights, weather sensors, and gunshot detection devices. Buildings in a smart city are filled with IoT solutions to improve energy efficiency and reduce operating costs.

A smart city is a safer city, with better traffic regulation, emergency systems that are more efficient, and faster police and EMT response times.

Additional resources

- The world's smartest cities: What IoT and smart governments will mean for you (TechRepublic cover story)
- Portland kicks off smart city initiative with traffic sensor safety project (ZDNet)
- Raspberry Pi-powered Boom IoT sensor detects nuclear explosions, tornadoes, rockets (TechRepublic)

IoT for utilities

IoT is essential for utilities, as these companies scramble to keep up with consumer demand for water and energy. The International Energy Agency expects global energy demand to increase by 28% by 2040.

Energy and water use can be more efficient with IoT solutions, with smart meters connecting to a smart energy grid to more effectively manage energy flow into buildings.

Smart water sensors track water quality, temperature, pressure, and usage. This data is used by the water company to analyze how customers are using water and to help them be more efficient. Water leak detectors are used to find tiny leaks that can lead to huge water waste.

Additional resources

- South Korea's IoT in full swing: From water meters to AI-powered smart buildings (ZDNet)
- Water data is the new oil: Using data to preserve water (ZDNet)

IoT for transportation

Gartner has predicted that by 2020, there will be a quarter billion connected vehicles on the road.

When a layer of IoT is added to vehicles, it helps improve transportation and logistics through remote monitoring and data analysis. For the enterprise, this means using predictive analytics to fix potential issues in vehicles before a breakdown occurs; it also means optimizing delivery routes in real time. For individuals, it means having IoT-enabled vehicles that connect to smartphones and even to their own home for a seamless experience.

Additional resources

- Keeping transportation safe in tomorrow's smart city means taking wireless security seriously (TechRepublic)
- How the IoT is keeping traffic moving and the streetlights shining (ZDNet)

IoT for retail

According to a research report by Global Market Insights, Inc., IoT devices in the retail market are predicted to reach more than $30 billion by 2024.

In retail, data from beacons, video cameras, and smart shelves give a retailer information on how customers shop in their stores. Consumers can be helped through digital kiosks and mobile apps to give them a more personalized experience. Smart shelves will help with inventory tracking.

Retailers who use IoT make merchandising decisions based on data collected from the sensors that show how customer traffic flows through the store. Operational efficiency can be improved by better allocating staff to needed areas.

Additional resources

- Data, AI, IoT: The future of retail (ZDNet special report) | Download the report as a PDF (TechRepublic)
- 4 ways IoT can improve the customer experience (TechRepublic)

IoT for healthcare

In healthcare, IoT is used for the care and treatment of patients, equipment maintenance, and hospital operations.

Medical assets such as supplies and medicine can be tracked by an IoT cloud platform. Vital medical equipment can be kept in top condition with predictive maintenance. Sensors can be used to monitor a patient's room temperature or how often the patient moves in bed.

Some patients receive care outside of a hospital setting through wearable sensors that track heart rate, blood pressure, and more. When there's a problem, their doctor is alerted and treatment can be scheduled.

Additional resources

- AT&T's IoT connectivity helping divers in shark-infested waters (TechRepublic)
- A smart toilet may be the future of IoT healthcare (TechRepublic)
- Detected documentary: Discover how an IoT bra can detect early signs of breast cancer (TechRepublic)

IoT for smart homes

The range of products available for a smart home are growing daily. There's everything from smart light bulbs to smart refrigerators to smart thermostats—and of course, smart speakers, such as the AI-enabled voice assistants from Google, Amazon, and Apple.

A smart home security system enables the user to monitor who enters and leaves their home at any time of day, and it's possible to remotely unlock a door to allow a housekeeper or someone else to enter.

For seniors, a smart home can make them feel more secure, with an adult child able to monitor them from afar and help them if they are ill or injured.

Currently, less than a quarter (23%) of consumers use smart home devices; however, more than a third (36%) are interested in testing out connected home applications, according to CSG's The Future of the DIgital Experience: IoT Edition.

Additional resources

- Best Smart Home Devices for 2018 (CNET)
- How IoT is empowering the elderly to become healthier and more productive (TechRepublic)

WHAT ARE THE HOTTEST IOT JOBS?

IoT is booming. With billions of connected devices already in play, and billions more predicted to be added in coming years, it makes sense to focus careers on areas that encompass the Internet of Things. The addition of IoT devices has led to bigger IT budgets, security concerns, and jobs for skilled pros who can deploy and manage connected networks.

There are three general types of IoT jobs:

Jobs that focus on the technology behind IoT projects. This includes the software, hardware, and network side of things, such as IoT solution architect, IoT software engineer, IoT analyst, cloud engineer, IoT app developer, machine learning designer/developer/engineer, and IoT software developer.

Jobs that focus on big data and how to analyze it for insights. This includes data scientist, database architect, business intelligence (BI) analyst, data engineer, and data analyst.

Jobs that focus on IoT security to keep the network and devices secure. This includes security engineer, security analyst, security specialist, security architect, security management specialist, and infrastructure engineer.

Additional resources

- 3 ways general IT pros can become IoT experts before the jobs boom (TechRepublic)
- How to become an IoT developer: 6 tips (TechRepublic)
- Hiring kit: IoT developer (Tech Pro Research)
- Cheat sheet: How to become a cybersecurity pro (TechRepublic)

WHAT'S NEXT FOR IOT?

IoT will continue to grow, as the associated costs drop and it becomes even easier to add devices. And whom better to ask about the future of IoT than the man who coined the term Internet of Things?

Ashton, when speaking to TechRepublic's Alison DeNisco Rayome at LiveWorx 2018, said, "I don't think the progression of the Internet of Things is going to be linear. We're going to see more and more Internet of Things, applications, more and more Internet of Things value every year. So although we're 17 years in, we're

not 17% done yet. And I think what we're going to see is increasing integration of network sensors into things like manufacturing processes, robotics, transportation systems."

The smart home is receiving plenty of attention, but Ashton said he's more interested in self-driving cars because they will have a radical impact on how we live.

Ashton said, "I really believe that adjusting to the Internet of Things age is a gradual, continuous process, not some sudden revolution that delivers immediate benefits."

Ericsson's Taylor said that in the future, "we expect to see a connection to 5G. In our discussions with our customers, it's clear that IoT and 5G are now components of the same strategic discussion. A year ago, they were treated separately. Networks and distributed computing will form the basis of advanced high-value use cases as 5G technology emerges and grows. The work starts now to define the use cases where the value is created."

Additional resources

- 17 ways the Internet of Things is changing the world (TechRepublic)
- The future of IoT? State-sponsored attacks, say security professionals (ZDNet)
- Blockchain will be critical for connecting IoT devices says Samsung (TechRepublic)
- The future of enterprise IoT: 2 factors to watch (ZDNet)
- The Future of IoT, book review: It's all about the data (ZDNet)

INTERNET OF THINGS IN 2019: FIVE PREDICTIONS

BY MACY BAYERN

The internet of things (IoT) is not only changing how businesses operate, but also how people live. With the wide availability of sensors, cloud and edge infrastructures, platforms, analytics, and more, IoT technology has evolved in recent years. But in 2019, the presence of IoT in the enterprise will transform as a whole, according to Forrester's Predictions 2019: The Internet of Things report, released in November.

Here are the five ways Forrester predicts IoT will shape the enterprise in 2019.

1. BUNDLED IOT SERVICES WILL TRY TO MOTIVATE A SLOW CONSUMER MARKET

The vision of an interconnected, centralized smart home is currently more of the enterprises' dream, rather than the consumers', the report said. Right now, consumers are easing into the smart home device industry, buying one app-enabled device at a time, which will probably continue in 2019. While industries may try to bundle services and tack on discounts as incentives, consumers aren't ready for that kind of integrated connectivity.

"The reality of connecting many different devices and environments, for many consumers that's just not happening yet. So the initial momentum is certainly still coming from the enterprise," said Michele Pelino, principal Forrester analyst of infrastructure and operations professionals.

2. IOT AS AN UMBRELLA TERM WILL DIMINISH

The conversation is going to shift away from an ambiguous buzzword to the actual use of technology. "Internet of things is not valuable in and of itself. It's about the use cases, it's about the solutions, it's about the applications, managing and monitoring assets, performance management solutions, different kinds of solutions coming together to solve a problem—that's really what the value proposition is, Pelino said."

"No matter what you call this concept of IoT, it's about a use case that's addressing a problem, that's solving an issue you have: monitoring around a sensor's capabilities, understanding what's happening, dealing with analytics in real time, bringing together elements of the application in the service, and wrapping security around that."

3. IOT VENDORS WILL COMPETE TO BE THE DESTINATION FOR IOT PLATFORMS

IoT platform vendors will be narrowing their scope in 2019, homing in on specific use cases. Business professionals aren't looking for one industrial IoT platform to manage every process going on at their company, the report said. Instead, they're looking for platforms that focus on specific tasks.

In 2019, the enterprise can expect to see many more IoT platform partnerships unfold, as major platform vendors attempt to appeal to more people by specializing in more use cases.

4. CYBERCRIMINALS WILL TARGET SMART CITIES

Cities are becoming smarter and smarter in an effort to improve efficiency in operations, but many cities aren't bringing security to their connected devices. Between smart lighting, traffic controls, and public transportation, smart cities are bringing in a whole new family of threat vectors.

In 2019, the report predicts an increase in targeted smart city ransomware attacks, which could cause major disruptions to citizen services. Smart cities need to take precautions and start preparing now.

5. A MARKET FOR IOT MANAGED SERVICES WILL DEVELOP

The next year will see a market developing that will help manage and operate fragmented IoT assets. "The idea of managing the ongoing end-to-end life cycle of a connected product is becoming more important, and ultimately, this managed service opportunity is going to need momentum in the coming year," Pelino said. "This one is really tied to the fact that we're seeing more and more kinds of products that are connected in an industrial setting."

THE FIVE BIGGEST IOT SECURITY FAILURES OF 2018

BY JAMES SANDERS

With the ubiquity of smartphones, smart speakers, and wirelessly connected devices around the world, design flaws and security vulnerabilities more easily surface. For example, 2018 saw a spectrum of IoT security failures, inclucing problems with vendor implementation, state actors co-opting legitimate products, service providers outright selling data to third parties with negligible security practices, and cascading failures from voice recognition gone wrong.

1. SIRENJACK VULNERABILITY HIGHLIGHTS FLAWS OF SECURITY-BY-OBSCURITY

Many emergency broadcast systems in place today were designed in the 1980s, without the expectation that malicious actors would attempt to commandeer the systems. Though the alert of a ballistic missile threat broadcast in Hawaii on January 13th was the result of human error, the 38 minutes between that broadcasted alert and retraction caused panic and anxiety, particularly as North Korea had been testing missiles in late 2017.

Bastille Security found a vulnerability in emergency broadcast systems produced by Acoustic Technology Inc. (ATI) that allowed for command packets broadcast over the air to be captured, modified, and replayed. ATI deployed a patch to address the issue, though it is unclear if all the affected systems were patched before the 90-day disclosure window or if all vulnerable systems were patched. Oddly, ATI's public statement on the vulnerability claimed Bastille's research is "largely theoretical" and "is against the law," though ATI's statement highlights public safety communications systems as being exempt from the statute it cited.

2. RUSSIAN ATTACKERS CO-OPT LOJACK IMPLANT TO GAIN DEVICE CONTROL

The popular device security software LoJack—previously known as Computrace—was leveraged by the Russian state-sponsored cyber espionage group "Fancy Bear." LoJack requires computer manufacturers to insert a dropper in the BIOS that allows the software to persist across Windows installations, though Fancy Bear was able to redirect the dropper in Windows to servers it controls, which impersonate LoJack's infrastructure. The legitimate nature of LoJack as an anti-theft utility prompted antivirus programs to ignore the attack, making it an attractive target for Fancy Bear.

While the May discovery relied on a change inside Windows, a second attack attributed to Fancy Bear was discovered in September. This attack, called LoJax, patches the UEFI data in the computer, making the attack persist across Windows installations and hard drives. This rootkit was discovered in 2018, but it appears to have been in operation since at least 2004. According to ESET, LoJax is the first case of a UEFI rootkit recorded as active in the wild.

3. STATE ACTORS HIDE MALWARE IN ROUTERS, UNDETECTED FOR YEARS

VPNFilter, described by researchers at Cisco Talos as having "capabilities that we have come to expect in a workhorse intelligence-collection platform, such as file collection, command execution, data exfiltration, and device management," was found in routers manufactured by ASUS, D-Link, Huawei, Linksys, MikroTik, Netgear, TP-Link, Ubiquiti, UPVEL, and ZTE, as well as NAS devices by QNAP.

Cisco Talos reported finding 500,000 compromised devices across 54 countries, with evidence of the first infection dating back to 2016. The Ukrainian Security Service called out Russia as the originator of the attack. Initial reports indicated that rebooting the router was enough to clear the infection, but further updates found that insufficient, recommending that users reflash the firmware as well. The malware is known to have code to target control systems using SCADA, but the aims of the attackers remain unknown.

Similarly, the Slingshot malware was discovered to be dormant in routers for six years and is capable of information gathering, persistence, and data exfiltration. Seculist researchers pointed out the similarities between Slingshot and the "Chimay Red" exploit published by WikiLeaks as part of the "Vault 7" releases of vulnerabilities, which WikiLeaks claims originated from the CIA.

4. LOCATIONSMART LEAKED LOCATION DATA OF ALL CELLPHONES IN THE US

An unsecured product demo from geolocation data firm LocationSmart allowed any user to look up the location of any mobile phone without needing to supply a password or any other credentials for any phone on the four major US carriers, as well as US Cellular and the Canadian carriers Bell, Rogers, and Telus. This vulnerability was found after Securus—a company that provides smartphone tracking tools for US law enforcement—was hacked. The backend data provider of that company was LocationSmart, according to a ZDNet report.

To make matters worse, mobile network operators were selling this personally identifiable data to LocationSmart. Verizon was the first to pledge to stop data sharing, with AT&T, Sprint, and T-Mobile following shortly thereafter.

5. AMAZON ECHO RANDOMLY RECORDED AND SENT A PORTLAND COUPLE'S CONVERSATION

A Portland couple claimed that their Amazon Echo smart speaker recorded a conversation and transmitted it to someone in their contact list—one of their employees—in Seattle. The original report is suspect, though Amazon confirmed to CNET that the incident occurred as described.

The model of the Echo Dot photographed in the original report can output sound to an external speaker through a 3.5mm audio cable. If a speaker was attached to the Echo Dot but turned off, the microphone in the Echo Dot unit would still be active, though it would have been impossible for the owners to hear an audio prompt through the speaker. The original report fails to mention this possibility; likewise, the report fails to correctly identify the device as an Amazon Echo.

Despite this, Amazon does have an Alexa problem. *New York Times* tech columnist Farhad Manjoo wrote in February about an incident in which his Echo Dot wailed "like a child screaming in a horror-movie dream." Amazon also made changes to how Alexa operates in March after a spate of reports indicating that Alexa-powered devices were randomly laughing, seemingly unprompted.

FOUR WAYS TO COMBAT NEW IOT SECURITY THREATS AT THE FIRMWARE LEVEL

BY MARY SHACKLETT

Telepresence robots enable physicians to administer care to patients in remote and rural areas, extending the reach of healthcare to those who otherwise might go without it. The use of telepresence in healthcare isn't new; it has operated for more than 10 years and is an accepted part of medical practice in many care networks.

What **has** changed for telepresence is the emergence of a new set of security vulnerabilities that attack telepresence robots at the firmware level—where standard IT security practices often don't extend.

"Robotic telepresence is a next-generation technology that allows a person in one location to replicate himself in another," wrote Dan Regalado, security researcher at IoT security provider Zingbox in a 2018 report. "The remote person can see you, hear you, interact with you, and move all around your location. But what if the person behind the robot is not who you think he is? What if the robot gets compromised, and now the attacker is watching you and your surroundings?"

SECURITY VULNERABILITIES

Zingbox conducted research on a widely adopted telepresence robot and found several areas of security vulnerability:

- Attackers could intercept firmware updates for the robot by penetrating the network.
- Once the firmware was intercepted, hackers could extract files from the telepresence file system.
- Access to the telepresence robot could be gained physically by plugging a USB device into the USB port of the robot and stealing the robot's WI-FI credentials, giving remote hackers an entry point into the robot.
- Malicious code could be injected into the telepresence robot and then propagated throughout the network that the robot is attached to.
- Hackers could steal pictures, images, records of conversations, and doctors' instructions.

"The danger is that hackers can get into the robot through firmware and then steal sensitive information, logs, and video streams because they can penetrate the firmware," Regalado said.

In healthcare, this is a major threat to security and privacy. However, these threats aren't limited to healthcare—other industry sectors are at risk, too.

How do you combat new IoT security threats at the firmware level, which traditional IT security is not designed for? Here are four best practices.

1. SECURE PHYSICAL PREMISES

Security measures for visitors to a patient or a hospital are not extreme, and equipment isn't always locked down. That means it's possible for nonauthorized personnel to access a telepresence robot that is sitting idle in a patient's room or in a treatment area.

To deal with this threat, firms using telepresence robots should address the physical aspect of IoT equipment security since it's easy for anyone to pull out a USB device, insert it into a USB port on a robot, and obtain the machine's Wi-Fi credentials so that the machine can later be accessed from a remote location.

One way to tighten up physical security is to track all IoT assets, like telepresence robots, so that they can be monitored for secured physical access at all times.

2. ENGAGE IN CONTINUOUS SECURITY DIALOGS WITH VENDORS

"Too many vendors of IoT equipment execute firmware updates but fail to notify customers when updates to firmware are available," Regalado said. The best way to address this is to maintain communications with your vendors on software and firmware updates. By keeping software and firmware updated you lower your risk of an unwanted intrusion, which often occurs in earlier versions of software and firmware.

3. DURING THE RFP PROCESS, EVALUATE PROSPECTIVE IOT VENDORS FOR BEST PRACTICES

Take time to select the best vendor for security. "There are security best practice checks you can perform, such as verifying that the vendor equipment doesn't allow any unencrypted data to pass in or out of the machine," Regalado said.

4. PERFORM BENEFICIAL HACKING ON YOUR OWN

By regularly testing your machine with "friendly hacks," you can probe for security holes and fix what you find. In this way, you give yourself the best possible chance of proactively preventing a hack that could be devastating to your company and your customers.

SIX WAYS GOVERNMENT PROJECTS WILL INFLUENCE BIG DATA AND IOT IN 2019

BY MARY SHACKLETT

The inspiration behind new technologies comes from an assortment of variables, including nature, science fiction, and product demand, to name a few. More specifically, innovations and developments found in aerospace and defense often trickle down to the commercial market as products and new capabilities for big data and IoT.

Dr. Mike Barrett, manager of the Power and Propulsion Element effort at NASA's Glenn Research Center, echoed these sentiments.

"In the early days of the Apollo flights we built most of the technology that was needed for space ourselves," he said. "But now we prefer for our commercial partners to do most of the innovations and development. In return, our industry partners can leverage these new technologies into breakthrough commercial applications for other markets."

Here are six examples of new technology developments coming out of NASA and the Department of Defense (DoD) that you should keep an eye on in the months to come.

1. REAL-TIME DATA CLEANING

With IoT, the ETL (extract, transform, and load) process that IT laboriously executes to clean big data could radically change. As an example, drones in military operations are programmed with machine and deep learning algorithms that enable them to determine which pieces of data are critical to a mission and which are not. During the in-flight real-time data collection process, these drones assess all incoming data and automatically discard irrelevant data, dramatically shrinking data payloads.

2. HARDENED SENSORS

In both the Lunar Lander and Mars projects, NASA wants hardened sensors that can withstand extreme heat, cold, high radiation levels, and other harsh environmental conditions found in space. These new hardened sensors are more reliable than what companies presently use in their IoT and will go far in preventing IoT sensor failures in space and elsewhere.

3. MACHINE LEARNING AND AI

In military operations, commercial sector contractors and the DoD are working on self-healing formations of drones, where each drone executes its own machine learning and artificial intelligence (AI) as it flies a mission. Using this machine learning and AI, a drone fleet on a mission can detect when a member has failed and then communicate with other drones to regroup and continue the mission without interruption.

This type of self-healing failover can easily be used on manufacturing assembly lines, with machines interoperating and communicating together—and devising alternate production paths if a single machine fails.

4. SYMBIOTIC HUMAN-MACHINE WORK PROCESSES

In military operations, a technology that symbiotically teams humans and drones on missions is designed so an unmanned vehicle can fly as a teammate with a manned aircraft.

"Effective manned/unmanned teaming can reduce the high cognitive workload, allowing warfighters to more exclusively focus on mission planning and management," said Mark Cole, Business Strategy and Development, Intelligence Surveillance and Reconnaissance (ISR), and Unmanned Aircraft System (UAS) programs at Lockheed Martin Skunk Works, a DoD contractor.

This human-machine symbiosis can work just as well for a logistics provider with a 1,000-vehicle fleet.

5. SOLAR POWER

In NASA's Lunar Lander project, the energy source of choice is solar, which is limitless in space and does not require transport. NASA plans to take advantage of the limitless space solar supply by applying logistics to its vehicle lunar orbits. The plan includes keeping an orbiting craft away from the dark side of the moon, so that the craft can continuously replenish its fuel supplies because it's always exposed to the sun's solar energy.

Look for data centers to seek out ways to maximize their energy use through logistics as well as through technology.

6. LEGACY SYSTEMS

In space and defense and in the private sector, there is a desire to keep legacy systems in place that continue to perform well. Substantial investments have already been made in these legacy platforms, and no one wants to waste them.

Accordingly, vendors working on military projects are asked to develop technologies that are backward compatible with existing technology bases. This is exactly what enterprise IT wants.

HOW IOT MEDICAL DEVICES SAVE YOUR LIFE AND THREATEN YOUR PRIVACY

BY MATT ASAY

The good news: People are figuring out how to scale IoT systems, pulling real-time analytics to deliver better healthcare, fleet tracking, and more. That's also the bad news.

It's bad because, as Derek Kravitz and Marshall Allen have detailed, the way sensitive personal data is increasingly being used will almost certainly upset even the most "I bare the buttocks of my life on Facebook" person. While IoT promises a utopian future, we're starting to see some of its dystopian present.

GETTING PERSONAL IN REAL TIME

As Avenade's Maria Muller has stressed, "No longer are analytics teams thinking about their daily, weekly, or quarterly reports. The demand for data, and understanding of it, needs to happen in real time." This is particularly true in IoT, which almost by its very nature demands real-time response to external triggers.

This may be even more true in healthcare, where a blood glucose monitor or implanted pacemaker can not only monitor patient health, but react in real-time to keep a heart beating regularly, for example. Over time, device manufacturers will almost certainly increase the range and criticality of such IoT devices, even as we move from "near real-time" to "true real-time."

They'll also keep pushing that data to places most consumers won't want.

WHO WATCHES THE WATCHERS?

For the price of reimbursement by an insurer, many consumers are shoveling their data to those insurers, among others. Or as Kravitz and Allen point out, "Children undergoing genetic testing are sometimes outfitted with heart monitors before their diagnosis, increasing the odds that their data is used by insurers."

What about users of continuous positive airway pressure (CPAP) machines? "The data may be transmitted to the makers or suppliers of the machines. Doctors may use it to assess whether the therapy is effective. Health insurers may receive the data to track whether patients are using their CPAP machines as directed. They may refuse to reimburse the costs of the machine if the patient doesn't use it enough."

The day is coming (it may already be here) when someone's medical procedure won't be covered by that insurer because the insurer finds the patient wasn't walking enough, using their blood glucose monitor consistently, or

committing some other infraction. Or as Rakesh Agrawal has offered, "What's next? If you're involved in a car accident, a lawyer subpoenas your sleep records from the night before." Yes, we have HIPAA to protect patient privacy, but insurers are finding ways to work around this by going directly to our devices.

In theory, patient data can be used only if it's "donated," meaning that the patient consents to its collection and use. Most of us, however, don't fully understand that, as Kravitz and Allen write, our data "... can be packaged and sold for advertising. It can be anonymized and used by customer support and information technology companies. Or it can be shared with health insurers, who may use it to deny reimbursement."

We need better privacy protections from our governments—or at least, we need more vendors to be like Apple and make privacy a top concern.

HOW TO LEVERAGE THE INDUSTRIAL INTERNET OF THINGS

BY BOB VIOLINO

The Internet of Things (IoT) can deliver benefits for companies in a variety of industries: retail, healthcare, logistics/supply chain, etc. In the manufacturing sector, it's the Industrial Internet of Things (IIoT) that's garnering lots of attention in terms of potential value.

IIoT incorporates big data/analytics and machine learning technologies to glean insights from data gathered from production equipment, products, and sensors in industrial settings. Manufacturers can use the data to discover inefficiencies, cut costs, and improve customer service. IIoT can provide better quality control, more efficient supply chains, and sustainability.

One company that's banking on IIoT is Rexnord Corp., whose Process and Motion Control (PMC) platform designs, manufactures, and services highly engineered mechanical components used within complex systems where customer reliability requirements and the cost of failure or downtime are extremely high.

The company's bearings, couplings, and gears are used at facilities such as power plants and mining operations, and its conveyer components help customers in manufacturing make everything from cars to food.

Rexnord provides a range of smart-connected products that offer a way to monitor critical parameters of its customers' equipment, providing operational analytics that help them improve the performance of their systems and anticipate the failure of key components. That way they can prolong the useful life of equipment and avoid catastrophic failures that result in costly unplanned production downtime.

Last year, the company began using the IoTium Edge-Cloud Infrastructure-as-a-Service offering from IoTium Inc. to support rapid and scalable deployment of IIoT by connecting legacy machinery to the cloud. This provides rapid access to data analysis and insights, combined with the benefits of remote asset management for preventive maintenance and predictive analysis.

The diverse deployment and critical nature of its products made it imperative for Rexnord to find a maintenance platform that could be implemented in a scalable way, said Rick Morse, vice president of digital solutions for Rexnord's PMC business.

The IoTium service solves the fundamental industrial connectivity problem of brownfield environments, giving Rexnord secure, remote connectivity and the ability to deploy edge computing. It provides the ability to securely manage a growing global installed base of networked devices, while ensuring that customers' information is secure.

Rexnord can now connect legacy machines—running in facilities such as power plants, mining operations, wind farms, food manufacturing plants, and aerospace and automotive manufacturing plants—to the cloud so it can easily manage all these machines and remotely pull critical data for real-time data analysis and insights.

A major benefit is the remote access of information. For example, in a conventional mining scenario, there are many physical locations that operations personnel have to manually go to in order to get information and compile data. With remote access, mining operators can save significant time in collecting data that helps them operate more efficiently. They can obtain more accurate, timely information that may help improve business results, and they can reduce risk to personnel who no longer need to go into hazardous environments to manage assets.

In the past, Rexnord couldn't offer its customers an efficient way to access their mechanical power transmission assets to collect data to perform preventive maintenance.

The company is still in the early stages of applying IoTium's technology to its products, Morse said, but it's clear that IIoT will be central to Rexnord's future operations.

"Our customers have confirmed to us they improve their productivity from the capabilities we provide to them via our IIoT-smart products," he said. "Specifically, our customers have realized business-impacting results from extended mean-time-between-failure, shortened mean-time-to-replace, and optimized asset management."

HOW TO BECOME AN IOT DEVELOPER: SIX TIPS

BY ALISON DENISCO RAYOME

The Internet of Things (IoT) industry is booming, with the number of connected devices in use forecast to reach almost 31 billion worldwide by 2020. And as connected homes, cars, and offices become more mainstream, more developers are needed to ensure that devices operate properly and securely.

The term "IoT developer" remains broad, said Greg Gorman, director of the IoT Developer Ecosystem at IBM. "There are a lot of discipline areas that are in play, including security, networking, systems engineering, cloud programming, and hardware device programming," he said. "It pays to be multilingual so that you can be flexible and play many different roles on the team."

There are four stages in developing an IoT device, according to Kornilios Ampatzis, a software developer at InfoLearn:

- **Assembly of the physical hardware** requires engineering skills and is usually not completed by a developer. Most IoT devices use primarily preassembled boards and sensors connected on them.
- **Programming the device** requires programming skills to read the data from the sensors connected on the IoT device and send them to the server.
- **Programming the server that will receive and store the data from the device** requires the use of server-side languages, like PHP, ASP.NET, or Node.js, and database queries based on MySQL or some other SQL derivative.
- **Displaying data to the device user** involves creating the web page or app that will depict the collected data to the user, which requires web development knowledge of PHP, JavaScript, HTML, CSS, MySQL, or another framework.

"Usually a developer is not responsible for all those stages," Ampatzis said. "So in order to specify how to get started on a career in the field, first they have to decide which stage of the development process they want to get aboard."

Here are six tips from IoT experts on how to break into a career developing connected devices.

1. GAIN A DEEP UNDERSTANDING OF SENSORS

Unlike other developers, those who work in the IoT space must have a deep understanding of sensors and wireless communication, said Karen Panetta, an IEEE fellow and professor of electrical and computer engineering and dean of graduate education for the School of Engineering at Tufts University.

It's recommended that IoT developers have a background in computer science or electrical engineering, she said. However, IEEE and other professional organizations offer online courses on sensors and development in which you can make a project to show employers. And a number of inexpensive sensors and maker kits are available to practice skills on your own.

"Beyond computing, IoT will take you into the world of mechanical and civil engineering as sensors gather physics data," said Bryan Kester, corporate director of Concrete Sensors. "It's very difficult to be a 'deep' IoT technologist—you have to be naturally curious about the world and a renaissance person at heart."

2. FOCUS ON USER INTERFACE

When developing a commercial IoT product, it's important to hold yourself to high quality standards for user experiences, said Kit Klein, product line manager – smart home at Ubiquiti Networks. "Many customers depend on these products for critical tasks in their daily lives and are understandably intolerant of failures," Klein said. "As an industry, we need to ensure products delight a rapidly growing base of users who aren't necessarily tech savvy. Quality and reliability are paramount to this experience and need to be part of any developer's mentality."

Panetta recommends performing usability studies with customers to determine ease of use. "It all comes back to user interface. "You can have the best control for your thermostat, but it needs to be simple to use."

3. LEARN JAVASCRIPT OR PYTHON

Suz Hinton, cloud developer advocate at Microsoft, recommends learning JavaScript before pursuing an IoT developer career. "Using a web-based language for both the data processing backend and the code running on the device itself makes a lot of sense," she said. "JavaScript is a very event-driven language, and this makes it ideal for reacting to new data from devices and triggering actions on the devices themselves."

Working with new technology often means being motivated to work without documentation, code samples, or guidance other than the scant information provided by hardware manufacturers, said Rob Lauer, senior manager of developer relations at Progress. IoT developers tend to use common languages, including Python and JavaScript, with some Windows IoT-compatible devices using C#/.NET, he said.

4. PLAY WITH A RASPBERRY PI

For those without a computer science or electrical engineering degree, Elliot Schrock, founder and lead developer at Thryv, Inc., suggests demonstrating your aptitude to employers by completing projects on a Raspberry Pi.

"Raspberry Pi's are very inexpensive, tiny computers and are often employed in proof of concept IoT projects," Schrock said. "They're also a great way to learn how to solder together simple circuits and link those circuits with software. Putting together some simple demo projects and then coming up with, and executing, some projects of your own is a great way to show that you have the initiative and know-how to work in IoT."

Hinton agreed. "Using a device like the Tessel 2 or the Particle Photon or even the humble Raspberry Pi can get developers fast on their way to learning how hardware ticks and the new skills required," Hinton said. "Writing for IoT is really just learning how to write for smaller, slower computers."

5. FIND A COMMUNITY

Involvement in the surrounding communities of makers, inventors, and entrepreneurs with whom you can explore, develop, and refine your ideas into reality is an important factor for becoming an IoT developer, said Emily Rose, a developer advocate and technical content creator. "The world of IoT is still so nascent and nebulous; there are few well-defined paths into the industry. This may seem like a daunting prospect, but it can also be a tremendous advantage to those with an eye for exploration beyond the bounds of convention."

David Middlecamp, head of solutions architecture at Particle, suggests looking to Hackster and Instructables for communities of makers and project ideas.

6. KEEP YOUR SKILLS CUTTING EDGE

Learning one platform or skill set isn't enough, according to IBM research scientist and master inventor Eli Dow. "The platform you write for this week will often be obsolete within six months to a year," Dow said. "Sensors will change, single board computers or other embedded platforms will continue to evolve, and you have to have the flexibility to adapt as platforms change at a blistering pace."

Becoming an IoT developer means being "obsessed" with technology, said Erin Essex, product design manager and senior product designer at Shutterstock. "Successful IoT developers must be tech news junkies—they should know everything that is going on in the industry, what's hot, what's old news, and what could be the next great thing," she said. "This will provide the foundation needed to tinker with technology and make whatever is being built the best it can possibly be."

THE FIVE INDUSTRIES LEADING THE IOT REVOLUTION

BY ALISON DENISCO RAYOME

As the Internet of Things (IoT) continues to spread across the home and the enterprise, various industries are leading investments in the revolutionary technologies that are changing how we live and work. Here are the top five industries that experts say are leading IoT investments and adoption.

1. MANUFACTURING

IoT is "evolutionary," according to Peter Middleton, a Gartner market research analyst focusing on IoT. It emerges out of a history of using networked automation systems in industries such as manufacturing and transportation. "Over time, as networking technology improves through phenomena such as Moore's Law and advances in processing technology and sensors, the idea of monitoring and optimizing use of physical assets extends to all industries," Middleton said.

IoT's manufacturing origins continue, as the largest investments in the technology remain in that space. These investments fall into two categories: inward facing (those concerned with optimizing systems and saving costs) and outward facing (those that make improvements in customer usage).

In terms of internal investments, manufacturers are using IoT to optimize their processes, monitor equipment, and do preventative and predictive maintenance on that equipment. Manufacturing operations was the IoT use case that saw the largest investment in 2016 across all industries, at $102.5 billion, according to IDC.

In the outward-facing arena, those in this industry use IoT devices to examine how their products are used by customers by maintaining a networked link to those products and sampling usage data and sensor measurements. This way, manufacturers can analyze results and see broad patterns in terms of how the product is used, which can inform the next generation of the product or help diagnose problems early.

2. TRANSPORTATION

The transportation industry is also investing heavily in IoT. Freight monitoring drives much of the IoT spending in this sector, representing the second-largest IoT use case across all industries.

Increasing numbers of freight and public transportation vehicles are equipped with sensors that help schedule maintenance, optimize fuel consumption, and train drivers, Middleton said. These vehicles can also monitor operating or driving behavior for insurance purposes. Some vehicles have digital data recorders that are

programmed to take video samples under conditions of heavy acceleration that might be indicative of a serious traffic accident. That video could then be used in an investigation, Middleton said.

3. UTILITIES

In the utilities industry, investments in the smart grid for electricity and gas totaled $57.8 billion in 2016, according to IDC. Smart grid meters are now widely deployed in the US and in several European countries, Webb said. "It's relatively simple: Electricity meters have power, so they don't have to worry about batteries and are static. And the business case is straightforward—you don't have to pay someone to read the meter."

The oil and gas industry has also taken advantage of IoT solutions. "These [industries] are spread across large areas and have lots of pipes and valves and pressure gauges to monitor," Webb said. "The loss of revenue from just a few minutes of an oil pump breaking down is huge, so it's worth installing IoT systems."

IoT devices are also used within power generating plants to monitor equipment over time, to do predictive maintenance, and to provide additional safety oversight, Middleton said.

4. HEALTHCARE

Healthcare is seeing the fastest spending growth in IoT. Middleton said IoT's use in the healthcare field is broad, ranging from medical machines that share images with a patient's other caregivers, monitoring and troubleshooting problems with equipment, and real-time location systems that can track equipment, dispensation of medicine, and staff and patients. Advances in implants, prosthetics, and wearables also take advantage of IoT, streaming data back to medical providers.

Connecting pacemakers and other medical devices to the internet benefits patients by reducing errors and providing more data to doctors to improve diagnosis and quality of care, said Valorie King, IEEE member and program chair of the undergraduate cybersecurity management and policy program at University of Maryland University College. But it also puts these devices at risk for cyberattacks.

"Security should be part of the design requirements of the system," King said. "Software security is the biggest area of vulnerability."

5. CONSUMER ELECTRONICS AND CARS

Consumer IoT purchases represented the fourth-largest market segment in 2016, according to IDC and are projected to become the third-largest segment in 2020. Over the past couple of years, we've seen a major rise of home and office automation systems and digital assistants such as the Amazon Alexa and Google Home.

Webb predicts that while digital assistants have gained popularity, it will be some time before most people invest in fully connected homes and offices. "The biggest problem is the inertia of needing to buy a new refrigerator or home security system that has these capabilities," Webb said. "We don't tend to think, 'Let me get a new refrigerator that's internet connected,' unless the old one breaks. It's a slow process of introduction in that space."

Connected cars are also an IoT industry leader in the consumer space, said Theresa Bui, IoT cloud strategy platform director at Cisco Jasper, which operates the company's IoT connectivity management platform. It has 17,000 enterprise customers worldwide—including General Motors—using the platform to manage connectivity of millions IoT devices.

For example, every General Motors car produced today has IoT capabilities that allow drivers to gain diagnostic information and connect to the internet, among other features.

Connected vehicles and smart buildings are predicted to rank among the top industry segments for IoT adoption throughout the next several years, according to IDC.

ADVICE FOR ENTERPRISES

As more industries invest in IoT, it's imperative to ensure that these devices have strong security systems built in, Webb said. "We've seen [an increase in] denial-of-service attacks from IoT devices that have been hijacked," Webb said. "It was unexpected, but in hindsight, we should have thought of that. Many more of these kinds of things will happen."

The cost of building a product that connects to a network continues to fall, Middleton said. But someone architecting a low-cost product, such as a smart light bulb, still needs to pay attention to network security, because it would be possible for an attacker to enter a network through that one inexpensive IoT device.

For companies beginning their IoT journey, "we recommend that operations or engineer departments strive to work more closely with IT departments," Middleton said. "It will enable a more cohesive plan in the use of technology across a given enterprise, as opposed to having islands of usage where people don't communicate and leverage best practices."

Middleton also recommended forming a team within your organization that coordinates the selection of technologies, considers possible use cases, shares best practices, and provides security oversight. This group can start with pilot projects and use lessons learned from those to develop more detailed return on investment calculations and justify scaling up to a full initiative.

CREDITS

Senior Director, B2B Editorial
Jason Hiner

Editor in Chief, UK
Steve Ranger

Senior Managing Editor
Bill Detwiler

Associate Managing Editor
Mary Weilage

Senior Editor
Alison DeNisco Rayome

Editor, Australia
Chris Duckett

Senior Features Editor
Jody Gilbert

Senior Writer
Teena Maddox

Chief Reporter
Nick Heath

Staff Writer
Macy Bayern

Associate Editor
Melanie Wachsman

Multimedia Producer
Derek Poore

Cover image: CNET

TechRepublic

ABOUT TECHREPUBLIC

TechRepublic is a digital publication and online community that empowers the people of business and technology. It provides analysis, tips, best practices, and case studies aimed at helping leaders make better decisions about technology.

DISCLAIMER

The information contained herein has been obtained from sources believed to be reliable. CBS Interactive Inc. disclaims all warranties as to the accuracy, completeness, or adequacy of such information. CBS Interactive Inc. shall have no liability for errors, omissions, or inadequacies in the information contained herein or for the interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.