TechTarget | IoT Agenda

E-guide

PRO+ Content

Internet of Things in the Enterprise

Your expert guide to getting started with IoT

In this e-guide

In this e-guide:

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

In this new era, business professionals need expert assistance in order to make the leap to IoT. In this e-guide, find out:

- **What you *need to know* before you get started on an enterprise IoT initiative**
- **Seven key IoT risks to prepare for before implementing an IoT policy**
- **How to address new data center security concerns brought on by IoT**
- **How to leverage data analytics to get the most out of your IoT investment**

In this e-guide

Delving into an enterprise IoT initiative? Read this first

Nicole Laskowski, Senior News Writer

From the business problem to the technology, here's what CIOs need to know to get started on an enterprise IoT initiative.

The Monsanto Co. wants to help farmers solve a major problem: How to feed the additional 2.3 billion people we will have on earth by 2050, according to projections from the Food and Agriculture Organization of the United Nations. Throw in shrinking farmland and an industry that's traditionally slow to market, and the problem, it appears, becomes a crucible.

Monsanto, the world's largest seed company, has turned to the Internet of Things (IoT) in search of potential solutions. For Monsanto IT, the push has required upending tried-and-true protocols for the uncertain and the experimental. And they're not alone. According to experts, CIOs who decide to delve into IoT will be exploring new territory that includes new platform choices, new concepts such as edge computing, and new relationships with vendors that look and feel more like partnerships.

In this e-guide

But the old problems don't go away either. Among the most important IoT issues facing CIOs is how to forge better relationships with the business where, according to experts, IoT opportunities often begin to take shape. The same cultural, language and trust issues that CIOs have been negotiating for years come to the fore in IoT. That's because many business people see IoT as extremely strategic and, according to Gartner analyst Paul DeBeasi, they can be almost secretive about it. "Even when IT folks found the business problem and began to understand the business problem, a lot of times, the business just put up a wall, and pushed them back and didn't allow them to get engaged," DeBeasi said of IoT initiatives at the recent Gartner Catalyst event.

Paul DeBeasi

Still, CIOs should make inroads now rather than later, if only for the sanity of their IT departments. "The business needs to get you involved, because they're only going to go so far," DeBeasi said. "Eventually, it's going to be dumped in your lap, and, eventually, you're going to have to run it."

How IoT works

For the uninitiated, IoT is a network of physical objects that have unique identifiers capable of producing and transmitting data across the Web automatically. While the technology itself isn't new, components such as

In this e-guide

sensors that used to be prohibitively expensive are now more affordable than ever, resulting in a wave of "smart" products flooding the market -- everything from bathtubs to baby monitors.

Monsanto's enterprise IoT strategy started as a way to reduce inefficiencies in its supply chain, such as preventing seed loss. Seeds that experience heat stress, for example, are unlikely to germinate. By outfitting the semi-trucks that transport seed from fields to processing facilities with sensors that measure temperature and geolocation, Monsanto's IT department was able to build a virtual window into the transportation environment.

Doing so gave the business an advantage: "Now, with IoT, if our grain gets heat stressed, we can dynamically route it to cooling centers or route it to the front of a receiving line to get the grain processed," said Fred Hillebrandt, infrastructure architect at the agro-chemical and technology company in St. Louis.

Hillebrandt and Monsanto were held up as a model IoT example during the recent Gartner Catalyst event, where more than one analyst remarked at how quickly the IoT trend is moving. "You started to hear about it a little a few years ago, but all of a sudden, it's here," said Lyn Robison. If Gartner predictions of 25 billion sensors generating $1.9 trillion in global economic value by 2020 play out, interest in the IoT won't fade anytime soon.

In this e-guide

Drue Reeves

Put another way: CIOs need to start thinking IoT strategy, which begins by understanding how IoT works. According to Gartner, there are three components of any IoT service: the edge, the platform and the user. Here's how the three components break down:

- **The edge:** Where data originates or is aggregated, pared down and, in some cases, analyzed, according to experts. At Akamai Technologies Inc. in Cambridge, Mass., for example, edge computing plays a crucial role in real-time operating systems. Rather than transmit every signal from a sensor to a centralized data warehouse and bog down the network, Akamai collects the data at an aggregation point close to the user and transmits in real time only the data points that require immediate attention. Aggregation points aren't always necessary, according to Gartner analyst Drue Reeves, but the more IoT devices a business is gathering information from, the more critical they become. "When you have thousands of turbines or thousands of washing machines, you're going to want some aggregation in the middle or you're going to overflow your IoT platform with data," he said during his presentation at Catalyst.

- **The platform:** Where data is ingested -- typically in the cloud, analytics are performed and an often internally developed algorithm takes an action, according to Gartner's DeBeasi. Incoming data is sent to a real-time stream processing engine, which decides if an action needs to be

In this e-guide

taken right away or if the data can be tucked away for future use, according to Reeves. The platform also performs big-picture analytics by, say, integrating historical data with real-time data to look at trending analysis; it also contains a policies engine and an orchestration engine to manage the platform, Reeves said.

- **The user:** Where data drives a business action. According to Reeves, data that's been analyzed can move from the IoT platform to a user in one of three ways: The user can use an API to "call" or query the data, the IoT platform can call out or signal to the business user when it finds a predetermined set of events, "or you can do both of those over an API bus," Reeves said.

An IoT strategy

The recommended steps to bootstrap an enterprise IoT initiative will be familiar territory to many CIOs. Gartner suggested they build a team, find a business opportunity, build a prototype and decide if the project is worthwhile enough to invest in. But several of the finer points are worth highlighting.

For example, DeBeasi recommends CIOs start by appointing what he calls an IoT architect -- someone who:

In this e-guide

- understands IT and has a basic understanding of IoT technology;
- has a deep curiosity, as well as a willingness to learn and share; and
- understands operational technology and how IoT will impact business operations.

That last trait is what makes IoT so different, according to DeBeasi. "It's not enough to be technically savvy; this person must be business savvy as well," he said. "They understand the business process; they're a good communicator."

Fred Hillebrandt

At Monsanto, Hillebrandt, who works for both the strategy and architecture organization as well as the supply chain organization, has taken on the role of IoT architect (not his official title). Last February, he was tasked with leading an IoT initiative for the company. "I'm still focused on supply chain, but I was asked to put together an enterprise strategy around IoT -- a platform strategy," he said. (For the record, Hillebrandt's first step was also people-focused: He put together a small team of influencers who were already tinkering with IoT or had expressed interest in aspects of it and had credibility with senior management, he said.)

In this e-guide

IoT platform vs. point solution

Another aspect CIOs will want to focus on is the platform itself. When deploying, CIOs have a couple of options, according to DeBeasi: They can either select a point solution or a more general purpose solution.

How to bootstrap your enterprise IoT initiative

1. Build a core team. Gartner analyst Paul DeBeasi said to start with an IoT architect who has a keen understanding of IT, but also understands operational technology and how IoT will impact business operations. DeBeasi also recommended that the IoT architect partner with an IoT analyst, someone with an even deeper understanding of the business.

2. Discover the opportunity. DeBeasi used the word "discover" rather than "find" to convey how difficult of a challenge this might be for IT departments. Since IoT initiatives are starting in the business, figuring out how to build strong partnerships will be key.

3. Create a data model. DeBeasi suggested three steps when creating a data model: Define your data streams; define how your platform will process the data; and define the business action you want to take.

4. Build a prototype. Businesses will need to be developing and testing algorithms and automated responses, according to DeBeasi. "In the Monsanto example, this is where they have the action of prioritizing the seed coolant or the processing of the seed," he said.

5. Invest in the project. Verify the business value, assess the feasibility of the project and consider the scope, DeBeasi said.

Source: Gartner Inc.

In this e-guide

IoT point solutions like BigBelly Solar trash compactors are a low, initial investment, can be deployed quickly and can provide rapid innovation, according to DeBeasi. "You're not defining any of the data, you're not building the sensors, you're not building the dashboard," he said. But there are drawbacks, such as the inability to integrate a point solution with a larger enterprise IoT initiative, thereby creating IoT silos, and that's the last thing CIOs want, according to Monsanto's Hillebrandt.

He compared it to the 10 instances of Salesforce that Monsanto currently supports. "Every time we stand up a CRM for a region, we're building it all from scratch," Hillebrandt said. "That's not what we want to happen with IoT. We really want to have one platform, because that's going to get us the agility -- the innovation through sharing the data to build these higher-value applications."

To avoid silos, CIOs can either build an IoT platform internally, like Monsanto did, or follow Gartner's recommendation of deploying a "universal IoT platform" from Amazon Web Services, IBM Bluemix, Microsoft Azure or Google Cloud Platform. By getting all lines of business on the same platform, IT departments "can begin to then do federation or integration of information," DeBeasi said, as well as build additional capabilities into the platform -- another characteristic point solutions lack.

In this e-guide

Business/IT mojo

Selecting a universal IoT platform over a point solution won't happen without the business. And, unlike Monsanto's case, IoT opportunities won't normally start in the IT department, according to experts. (And even in Monsanto's case, one of Hillebrandt's goals is to build a self-service platform for the business. "It's our intent to deliver business value by deploying an IoT platform that lets the business chase after cost optimization and bring new digital products to market," he said.)

Jonathan Reichental

For most CIOs, the process will reflect something closer to what Jonathan Reichental, CIO for the City of Palo Alto, Calif., is experiencing. IoT initiatives, such as deploying a smart grid or implementing smart traffic signals, are coming out of different departments -- utilities or traffic -- in a fragmented way. But unlike what Gartner analysts observed at other businesses, Palo Alto departments aren't hiding IoT initiatives from Reichental. "I'm pulled in occasionally for discussions with vendors," he said. "Or, when we have to issue an RFP, my advice is sought."

The relationship between IT and city departments operates like this for a couple of reasons. Technology these days almost demands it, Reichental said. "In today's hyper-networked environment, no department can really go

In this e-guide

rogue without having to plug into the network, and get ports open, and conform to things like backup strategy and archiving," he said.

More pragmatically, Palo Alto has adopted a governance process, supported by the city manager, on steps that need to be taken before a technology project moves forward. Reichental described it as a funnel. "It goes through and we evaluate it for architecture, security, data backup, staffing, budget, and what capacity and skills we have," he said. In some cases, projects are deemed "not a good idea," and that conclusion is supported by the data gathered.

In the case of IoT initiatives, Reichental sees the practicality that a project like digitized parking meters could have for Palo Alto. By this time next year, he hopes to have a more centralized IoT vision for the city, but in the meantime, he doesn't want department efforts to live in the shadow. "I'm fully supportive of a partnership between a centralized IT and the needs of the departments," he said.

Besides, he said, if the relationship between business and IT isn't strong, the work doesn't get done. "You've got to have really good credibility and trust," he said. "And then you've got to have a governance process in place, endorsed by the CEO or the city manager downwards."

In this e-guide

Building trust is easier said than done, so here's a basic piece of advice Gartner analysts provided to get started: Scrub the term IoT out of existence when talking to the business.

"Business units won't call it IoT," Reeves said. "They'll call it something else, like digital business or the digital oil field or the connected car." In fact, scrub the tech talk out altogether. "Learn the business language," DeBeasi said. "Learn what's happening in the business; learn how to communicate."

Next article

In this e-guide

Internet of Things (IoT): Seven enterprise risks to consider

Ajay Kumar, Contributor

The Internet of Things is a growing enterprise threat. Learn about the seven key IoT risks to prepare for before implementing an IoT policy.

The day when virtually every electronic device -- from phones and cars to refrigerators and light switches -- will be connected to the Internet is not far away. The number of Internet-connected devices is growing rapidly and is expected to reach 50 billion by 2020.

However innovative and promising it seems, this so-called Internet of Things (IoT) phenomenon significantly increases the number of security risks businesses and consumers will inevitably face. Any device connecting to the Internet with an operating system comes with the possibility of being compromised, in turn becoming a backdoor for attackers into the enterprise.

In this article, we will discuss the proliferation of the Internet of Things and explore what enterprises can do to manage the security risks associated with IoT devices.

In this e-guide

What is the IoT? Why is it growing in popularity?

The IoT sensation is rapidly embracing entire societies and holds the potential to empower and advance nearly each and every individual and business. This creates tremendous opportunities for enterprises to develop new services and products that will offer increased convenience and satisfaction to their consumers.

On the user side, Google Inc. recently announced that it is partnering with major automakers Audi, General Motors and Honda to put Android-connected cars on the roads. Google is currently developing a new Android platform that will connect cars to the Internet. Soon, car owners will be able to lock or unlock their vehicles, start the engine or even monitor vehicle performance from a computer or smartphone.

The promises of IoT go far beyond those for individual users. Enterprise mobility management is a rapidly evolving example of the impact of IoT devices. Imagine if suddenly every package delivered to your organization came with a built-in RFID chip that could connect to your network and identify itself to a connected logistics system. Or picture a medical environment in which every instrument in the exam room connected to the network to transmit patient data collected via sensors. Even in industries like farming, imagine if every animal were digitally tracked to monitor its location,

In this e-guide

health and behavior. The IoT possibilities are limitless, and so are the number of devices that could manifest.

However, despite the opportunities of IoT, there are many risks that must be contended with. Any device that can connect to Internet has an embedded operating system deployed in its firmware. Because embedded operating systems are often not designed with security as a primary consideration, there are vulnerabilities present in virtually all of them -- just look at the amount of malware that is targeting Android-based devices today. Similar threats will likely proliferate among IoT devices as they catch on.

Enterprises and users alike must be prepared for the numerous issues of IoT. Listed below are seven of the many risks that will be inherent in an Internet of Things world, as well as suggestions to help organizations prepare for the challenge.

1. Disruption and denial-of-service attacks

Ensuring continuous availability of IoT-based devices will be important to avoid potential operational failures and interruptions to enterprise services. Even the seemingly simple process of adding new endpoints into the network -- particularly automated devices that work under the principle of machine-to-machine communications like those that help run power stations or build environmental controls -- will require the business to focus its

In this e-guide

attention on physical attacks on the devices in remote locations. This will require the business to strengthen physical security to prevent unauthorized access to devices outside of the security perimeter.

Disruptive cyberattacks, such as distributed denial-of-service attacks, could have new detrimental consequences for an enterprise. If thousands of IoT devices try to access a corporate website or data feed that isn't available, an enterprise's once-happy customers will become frustrated, resulting in revenue loss, customer dissatisfaction and potentially poor reception in the market.

Many of the challenges inherent to IoT are similar to those found in a bring your own device environment. Capabilities for managing lost or stolen devices -- either remote wiping or at least disabling their connectivity -- will be critical for dealing with compromised IoT devices. Having this enterprise strategy in place will help mitigate the risks of corporate data ending up in the wrong hands. Other policies that help manage BYOD could also be beneficial.

2. Understanding the complexity of vulnerabilities

Last year, an unknown attacker used a known vulnerability in a popular Web-connected baby monitor to spy on a two-year-old. This eye-opening incident goes to show what a high risk the IoT poses to enterprises and consumers

alike. In a more dramatic example, imagine using an IoT device like a simple thermostat to manipulate temperature readings at a nuclear power plant. If attackers compromise the device, the consequences could be devastating. Understanding where vulnerabilities fall on the complexity meter -- and how serious of a threat they pose -- is going to become a huge dilemma. To mitigate the risk, any project involving IoT devices must be designed with security in mind, and incorporate security controls, leveraging a pre-built role-based security model. Because these devices will have hardware, platforms and software that enterprises may never have seen before, the types of vulnerabilities may be unlike anything organizations have dealt with previously. It's critical not to underestimate the elevated risk many IoT devices may pose.

3. IoT vulnerability management

Another big challenge for enterprises in an IoT environment will be figuring out how to quickly patch IoT device vulnerabilities -- and how to prioritize vulnerability patching.

Because most IoT devices require a firmware update in order to patch vulnerabilities, the task can be complex to accomplish on the fly. For example, if a printer requires firmware upgrading, IT departments are unlikely to be able to apply a patch as quickly as they would in a server or

In this e-guide

desktop system; upgrading custom firmware often requires extra time and effort.

Also challenging for enterprises will be dealing with the default credentials provided when IoT devices are first used. Oftentimes, devices such as wireless access points or printers come with known administrator IDs and passwords. On top of this, devices may provide a built-in Web server to which admins can remotely connect, log in and manage the device. This is a huge vulnerability that can put IoT devices into attackers' hands. This requires enterprises to develop a stringent commissioning process. It also requires them to create a development environment where the initial configuration settings of the devices can be tested, scanned to identify any kind of vulnerabilities they present, validated and issues closed before the device is moved into the production environment. This further requires a compliance team to certify that the device is ready for production, test the security control on a periodic basis and make sure that any changes to the device are closely monitored and controlled and that any operational vulnerabilities found are addressed promptly.

4. Identifying, implementing security controls

In the IT world, redundancy is critical; should one product fail, another is there to take over. The concept of layered security works similarly, but it

In this e-guide

remains to be seen how well enterprises can layer security and redundancy to manage IoT risk. For example, in the health care industry, medical devices are available that not only monitor patients' health statuses, but also dispense medicine based on analysis performed by such devices. It's easy to imagine how tragic consequences could result were these devices to become compromised.

The challenges for enterprises lie in identifying where security controls are needed for this emerging breed of Internet-connected devices, and then implementing effective controls. Given the diversity that will exist among these devices, organizations will need to conduct customized risk assessments, often relying on third-party expertise, to identify what the risks are and how best to contain them. While an interesting recent example was the case of former Vice President Dick Cheney disabling the remote connectivity of a defibrillator implanted in his chest, unfortunately most enterprises won't have the luxury of taking these devices offline. In any event, organizations which embrace IoT must define their own information security controls to ensure the acceptable and adequate protection of the IoT evolution. As the trend matures, best practices will certainly emerge from industry professionals.

In this e-guide

5. Fulfilling the need for security analytics capabilities

The variety of new Wi-Fi-enabled devices connecting to the Internet will create a flood of data for enterprises to collect, aggregate, process and analyze. While certainly organizations will identify new business opportunities based on this data, new risks emerge as well.

Organizations must also be able to identify legitimate and malicious traffic patterns on IoT devices. For example, if an employee tries to download a seemingly legitimate app onto his or her smartphone that contains malware, it is critical to have actionable threat intelligence measures in place to identify the threat. The best analytical tools and algorithms will not only detect malicious activity, but also improve customer support efforts and improve the services being offered to the customers.

To prepare for these challenges, enterprises must build the right set of tools and processes required to provide adequate security analytics capabilities.

6. Modular hardware and software components

Security should be considered and implemented in every aspect of IoT to better control the parts and modules of Internet-connected devices.

Unfortunately it should be expected that attackers will seek to compromise the supply chain of IoT devices, implanting malicious code and other vulnerabilities to exploit only after the devices have been implemented in an enterprise environment. It may prove necessary to adopt a security paradigm like the Forrester Zero Trust model for IoT devices.

Where possible, enterprises should proactively set the stage by isolating these devices to their own network segment or vLAN. Additionally, technologies such as microkernels or hypervisors can be used with embedded systems to isolate the systems in the event of a security breach.

7. Rapid demand in bandwidth requirement

A study conducted by Palo Alto Networks Inc. revealed that between November 2011 and May 2012, network traffic jumped 700% on networks the vendor observed, largely due to streaming media, peer-to-peer applications and social networking. As more devices connect to the Internet, this number will continue to grow.

However, the increased demand for Internet will potentially proliferate business continuity risks. If critical applications do not receive their required bandwidth, consumers will have bad experiences, employee productivity will suffer and enterprise profitability could fall.

In this e-guide

To ensure high availability of their services, enterprises must consider adding bandwidth and boosting traffic management and monitoring. This will not only mitigate business continuity risks, but also prevent potential losses. In addition, from the project planning standpoint, organizations would need to do capacity planning and watch the growth rate of the network so that the increased demand for the required bandwidth can be met.

Conclusion

The Internet of Things has great potential for the consumer as well as for enterprises, but not without risk.

Information security organizations must begin preparations to transition from securing PCs, servers, mobile devices and traditional IT infrastructure, to managing a much broader set of interconnected items incorporating wearable devices, sensors and technology we can't even foresee currently. Enterprise security teams should take the initiative now to research security best practices to secure these emerging devices, and be prepared to update risk matrices and security policies as these devices make their way onto enterprise networks to enable machine-to-machine communication, huge data collection and numerous other uses.

This increased complexity within the enterprise shouldn't be overlooked, and threat modeling will be necessary to ensure basic security principal of

confidentiality, integrity and availability are maintained in what will be an increasingly interconnected digital world.

Next article

In this e-guide

In this e-guide

IoT device explosion challenges data center security

Robert Gates, News writer

The billions of Internet connected devices in the IoT wave introduce new data center security concerns that IT managers must head off at the pass.

Whether it is a sensor mounted on a rover inside a mine or a sensor inside a car, the connected world of the Internet of Things presents new security concerns that data center operators are starting to tackle.

The data center has evolved from connecting to PCs, then BYOD and now, "who knows who brought the device," according to Joe Skorupa, an analyst with Gartner Inc., adding that the number of devices is extraordinary.

This year, research firm Gartner Inc. estimates 1.1 billion connected things will be used in smart cities alone. That number will balloon to 9.7 billion by 2020.

In this e-guide

Much of the enterprise infrastructure is not configured or scaled from the Internet of Things (IoT) perspective, said Mike Sapien, an analyst with Ovum, an independent consultancy firm based in London.

The data center will process large quantities of IoT data in real time, which will increase as a proportion of data center workloads, Gartner said, leaving providers to face new security and capacity challenges.

IoT data security begins with the network

The IoT introduces, for the first time in a widespread way, devices without a human behind it. While the security challenges of BYOD presented similar concerns, the many connected IoT devices magnifies it in scale, Sapien said.

One solution is to have an IoT network connected at just one point to your corporate network, and even consider using a different provider, Sapien said. An age-old example is the ATM network of the bank.

But today's IoT introduces thousands of new machine-to-machine relationships. Take pay-as-you-go insurance, for example, where devices in a car tabulate the miles traveled or the areas where the car goes to calculate the insurance charge.

In this e-guide

"The insurance company is not going to put that on its data backbone," Sapien said.

Because many IoT devices will be owned by third parties, the control, risk assessment and mitigation will be outside of enterprises, according to Gartner, which will bring on a new set of vulnerabilities because many of the devices will be connected to enterprise networks.

Gartner recommends that data center managers understand that security must be integrated as part of IoT infrastructure and they should partner with industry device and platform manufacturers to succeed in this emerging marketplace.

Solutions to the security challenges of the IoT in the data center can be found for specific verticals, Sapien said.

Data center mangers should still be most concerned in coming up with a plan to respond to a breach from an IoT connected device.

"The ability to rapidly respond to a breach or threat is still a major challenge," Sapien said, adding that data center managers should develop a strong plan to isolate, remediate and remove the threat. "There could be hundreds of end user devices without a user that are attacking."

That's one of the big differences data center managers will face with the IoT -- unlike the mobile device management in a phone which can enforce proxy

In this e-guide

settings or remotely wipe the data on the device -- many IoT devices have nobody controlling the end point.

In addition to the connected city -- which will grow nine-fold in the next five years -- some of those connected "things" are in the data center itself. The security system for a data center which used to be secure and separate may now be connected. Tools to monitor the data center environment are, or can be, connected to other machines.

"Every point of entry will spark someone's imagination," said Jeff Wilson, an analyst at HIS Technology.

While the processing power of a sole IoT device may be limited, the devices could operate with a swarm mentality, according to Gartner's Skorupa.

"We are in the very early period of IoT," Skorupa said. "The security issues are there whether it is the IoT but the IoT just increases the security footprint."

Wilson suggests two solutions -- monitor traffic for attacks or obscure the security network. For example, Tempered Networks has a product that creates an encrypted overlay network that obfuscates the data center's control infrastructure.

In this e-guide

Most large data centers have been built in the past 10 years, Wilson said, noting that it is much simpler than a power plant, which may have a piecemeal security system built over the past 50 years, or longer.

Next article

In this e-guide

Analytics holds key to business value of IoT technology

Ed Burns, Site Editor

With all the hype about the Internet of Things, many businesses are wondering how they can get value out of IoT investments. One critical component is effective data analytics.

The Internet of Things is quickly becoming one of the most-hyped technologies in IT circles -- the big data term of the moment. But as the concept of the IoT becomes more familiar, how businesses can derive value from it is a question that needs to be answered. And increasingly, analytics is seen as the key to making investments in IoT technology worthwhile.

The futuristic example of the networked refrigerator has become a popular way for people to explain how the IoT works. The idea is that sensors embedded in the refrigerator will know when products that you typically keep on hand are running low or reaching their expiration date, triggering the refrigerator to automatically order more via its network connection. It sounds a bit like something from *The Jetsons*, though, and businesses outside of the home appliance or food delivery markets may wonder what's in the IoT for them.

In this e-guide

But IoT technology has potential applications well beyond the consumer space. For example, package delivery trucks, manufacturing systems and electrical grids all typically have sensors to monitor performance. More and more companies are now starting to collect and store data from such sensors. The next step is to analyze the data. Looking for patterns in it could illuminate ways to improve business operations, such as doing more preventive maintenance or designing more efficient delivery routes.

"The way I think of it is it makes things we deal with more addressable," said Joe DeCosmo, chief analytics officer at Enova International Inc., an online financial services provider based in Chicago. But DeCosmo, who previously worked as a consultant to public utility companies on projects to balance energy production with consumer demand, said that without the analytics piece, sensor data is just a lot of noise.

"The data combined with the analytics makes those addressable opportunities," he said.

High expectations for IoT tools

In its 2014 Hype Cycle for Emerging Technologies report, published in August, consultancy Gartner Inc. placed the IoT at the very top of what it calls the peak of inflated expectations. But many IT departments that are thinking about the IoT now are focusing primarily on the data collection

In this e-guide

aspect. In order to get to a point where IoT projects really deliver business value -- and avoid falling into Gartner's trough of disillusionment -- organizations need to have a plan for analyzing IoT data and acting on those analytics' results, said Steven Sarracino, founder of Activant Capital Group LLC, a Greenwich, Conn., venture firm that invests in technology companies.

Vendors marketing IoT products also need to emphasize data analysis capabilities, not just collecting sensor data, according to Sarracino. "There are a lot of [vendors] that will take the data and present it, and it will look pretty in a dashboard," he said. "But if they're not doing sensor-driven analytics, it's not useful."

Retail is one industry where Sarracino sees IoT technology having an impact today. His company recently invested in a software vendor called RetailNext Inc., which applies analytics to data from security cameras and Wi-Fi beacons to help retailers understand how customers are interacting with in-store displays.

Sarracino said retailers have been analyzing customers' Web activity data for years to identify opportunities to optimize their online services. Now, he added, they're looking to do the same kind of thing in their brick-and-mortar locations.

In this e-guide

Constructing an IoT analytics business case

But the opportunities aren't limited to retail. For example, Dan Hussain, a technologist who is founder and president of patent law firm American Patent Agency PC and investment company American Pioneer Ventures, has developed software designed to analyze sensor data from cranes being used to build high-rise towers to help identify potential structural failures in the cranes. Hussain said such machines have long had sensors to monitor their performance. What's new is that construction companies are now starting to ask how they can use that data to improve performance and avoid potentially dangerous safety issues.

This new strategic focus on IoT data collection and analysis can give organizations visibility into areas of their operations they've never had before. "We talked to many Fortune 500 companies and CEOs and found that many of their problems come from a lack of data coordination," Hussain said. "But once you get things connected, everything takes off."

Next article

In this e-guide

Getting more PRO+ exclusive content

This e-guide is made available to you, our member, through PRO+ Offers – a collection of free publications, training and special opportunities specifically gathered from our partners and across our network of sites.

PRO+ Offers is a free benefit only available to members of the TechTarget network of sites.

Take full advantage of your membership by visiting http://pro.techtarget.com/ProLP/

Images; Fotalia