SPECIAL REPORT

Sensor'd enterprise: IoT, ML, and big data

ZDNet

TechRepublic

TABLE OF CONTENTS

ENTERPRISE IOT PROJECTS: KEY FACTORS FOR SUCCESSFUL DEPLOYMENTS

BY CHARLES MCLELLAN

The collection and analysis of data from sensor-equipped devices in order to achieve a business or organisational goal—a.k.a. the Internet of Things, or IoT—is a key component in the wave of digital transformation underpinning the Fourth Industrial Revolution.

Although the IoT has been discussed and analysed for many years (ZDNet's first special report on the subject was in January 2013), there's a widespread sense that the pieces are now falling into place for it to begin delivering real value for businesses of all kinds, and not just early adopters. Business value will flow from real-time information about operations, supply chains and customers, which (if analysed properly) should translate into lower costs and increased revenues. Better information about business processes should also lead to lower environmental impact and wiser investment decisions.

A TRILLION IOT DEVICES

The scale of the upcoming IoT disruption was the subject of a white paper published in June 2017 by chip designer Arm, entitled The route to a trillion devices: The outlook for IoT investment to 2035. By 2035, according to Arm's analysis, the IoT's boost to global GDP will be $5 trillion, the annual spend on IoT hardware and services will be $1 trillion, the cumulative spend on IoT connectivity modules from 2017 will be $750 billion, and 1 trillion IoT devices will have been built since 2017.

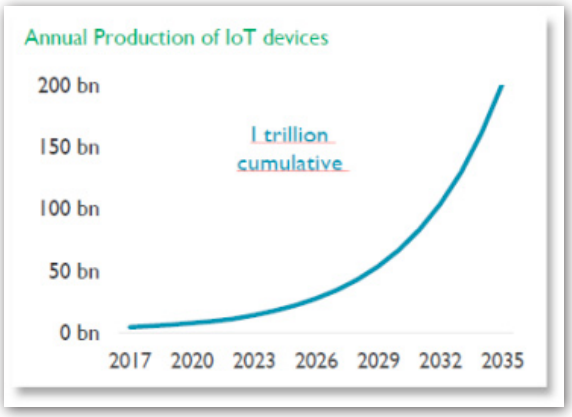
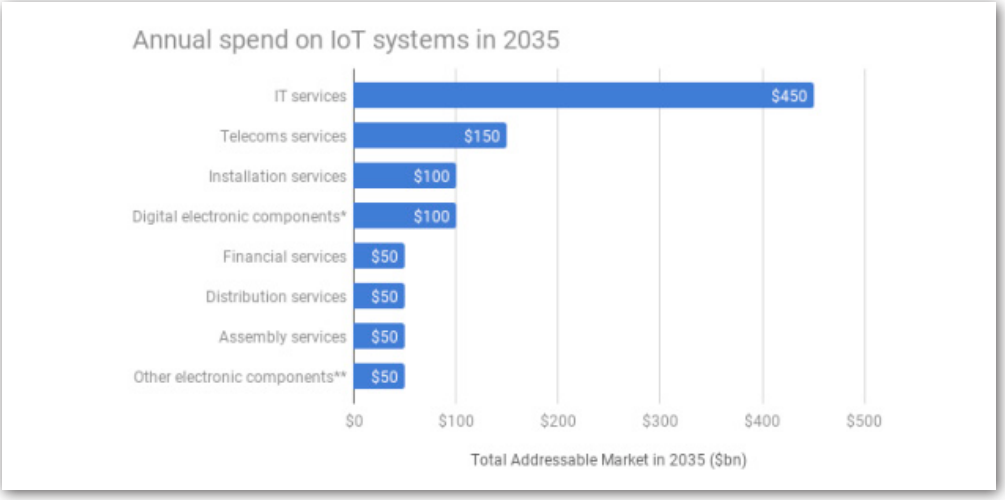


IMAGE: ARM

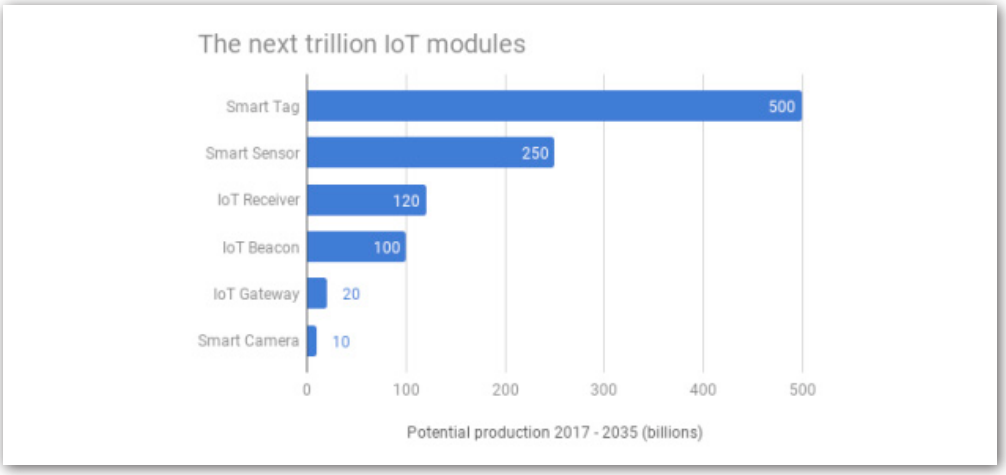
Here's Arm's projected breakdown of that $1 trillion annual IoT spend in 2035:



MICROCONTROLLERS, APPS PROCESSORS, RADIO CONTROLLERS, MEMORY; ** SENSORS, BATTERIES, SOLAR CELLS, ANTENNAE, CIRCUIT BOARDS, ETC. (DATA: ARM / CHART: ZDNET)

With $100 billion a year potentially on the table for digital electronic components alone in 2035, the reason for Arm's interest in the IoT is very clear. Firms involved in IT services ($450bn/yr), telecoms services ($150bn/yr) and installation services ($100bn/yr) also have a lot to play for.

Here's Arm's projected breakdown of the 1 trillion IoT devices that it predicts will be built between 2017 and 2035:



DATA: ARM / CHART: ZDNET

Different IoT modules have different connectivity and power supply requirements, which will affect their unit cost: the cheapest (with a BOM of around 40 cents in 2017) will be a smart tag powered by RF energy harvesting with NFC or RFID connectivity, for example, while the most expensive (BOM around $8 in 2017) will be an IoT gateway powered by mains electricity with internet access via an unlicensed radio connection.

And where will that $5 trillion global GDP boost come from? Prominent sectors in Arm's breakdown are: food production and distribution (food waste reduction, water/fertiliser/pesticide reduction, yield increases); manufacturing (throughput increase, preventative maintenance, after-market revenues); wholesale and retail (targeted advertising, inventory management, supply-chain management); transport and logistics (fleet management, asset utilisation, fuel savings, paperwork elimination); healthcare and social assistance (preventative medicine, drug research, home care, patient monitoring); and government, education and defence (improvement in traffic monitoring, crime prevention, pollution control, waste management).

FOG AND EDGE: DATA PROCESSING FOR THE IOT

If this kind of IoT expansion comes to pass, the amount of data available for analysis will be enormous, and much of it will require processing in real time—or at least with low latency. This has prompted the realisation that the traditional data-processing model—sending all data to centrally located (on-premises or cloud) data centres—will need retooling. Two contenders have emerged: 'fog' computing and 'edge' computing, both of which bring processing capabilities closer to the data sources, thereby reducing traffic to core data centres, decreasing latency and accelerating response times for critical applications.

Fog computing is a Cisco idea, backed by the OpenFog consortium (founding members Arm, Cisco, Dell, Intel, Microsoft and the Princeton University Edge Laboratory), whose mission statement reads (in part):

> Our efforts will define an architecture of distributed computing, network, storage, control and resources that will support intelligence at the edge of IoT, including autonomous and self-aware machines, things, devices, and smart objects. OpenFog members will also identify and develop new operational models. Ultimately, our work will help to enable and drive the next generation of IoT.

Edge computing is a similar idea, promoted by (among others) the EdgeX Foundry, an open-source project hosted by The Linux Foundation. EdgeX Foundry's goals include: building and promoting EdgeX as a common platform unifying IoT edge computing; certifying EdgeX components to ensure interoperability and compatibility; providing tools to quickly create EdgeX-based IoT edge solutions; and collaborating with relevant open-source projects, standards groups and industry alliances.

According to EdgeX Foundry, "The project's sweet spot is edge nodes such as embedded PCs, hubs, gateways, routers, and on-premises servers to address key interoperability challenges where 'south meets north, east, and west' in a distributed IoT fog architecture":

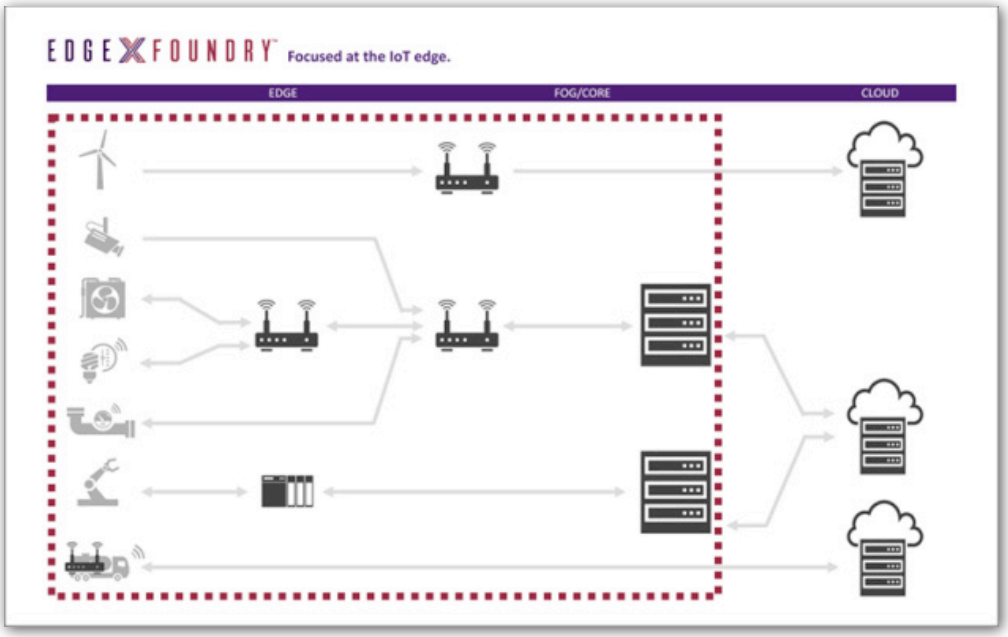


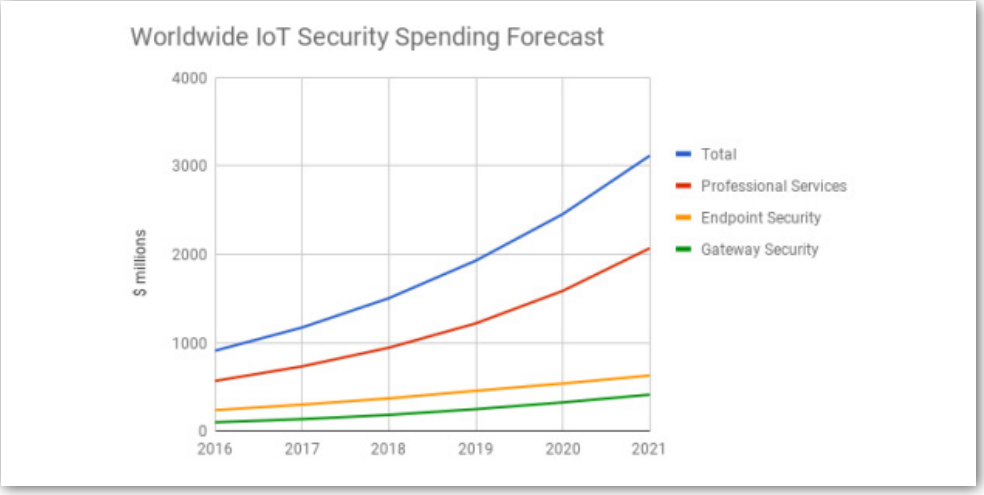
IMAGE: EDGEX FOUNDRY

EdgeX Foundry's technical steering committee includes representatives from IOTech, ADI, Mainflux, Dell, The Linux Foundation, Samsung Electronics, VMWare and Canonical.

IOT SECURITY AND THE RISE OF BLOCKCHAIN

The biggest worry with the rise of the IoT is security: what kinds of havoc could bad actors wreak with billions of internet-connected devices—in homes, offices, factories and other critical infrastructure—at their mercy? We don't have to use our imaginations, as serious IoT-based cyberattacks have already happened. Perhaps the most notorious was the 2016 attack that used Mirai malware to recruit hundreds of thousands of poorly secured Linux-based IoT devices into a botnet, which then launched large-scale DDoS attacks on high-profile websites and service providers.

The likely growth in the number of IoT devices and the pressing need to secure them has led analyst firm Gartner to predict that spending on IoT security will total $1.5 billion in 2018 (up 28% from 2017) and reach $3.1 billion by 2021 (up 107% from 2018):



DATA: GARTNER / CHART: ZDNET

"Although IoT security is consistently referred to as a primary concern, most IoT security implementations have been planned, deployed and operated at the business-unit level, in cooperation with some IT departments to ensure the IT portions affected by the devices are sufficiently addressed," said Ruggero Contu, research director at Gartner in a statement on 21 March. "However, coordination via common architecture or a consistent security strategy is all but absent, and vendor product and service selection remains largely ad hoc, based upon the device provider's alliances with partners or the core system that the devices are enhancing or replacing."

A widely discussed solution to the problem of securing IoT devices, and the data they generate, is blockchain—the distributed ledger system that's best known for underpinning cryptocurrencies like Bitcoin. While blockchain technology might not prevent the factory-default credentials of cheap IoT devices being accessed by botnet-creating malware, it can help to create networks of trusted devices that exchange data securely and trigger automated actions via 'smart contracts'.

That's the goal of the Trusted IoT Alliance (TIoTA), a consortium comprising blockchain technology companies, enterprises (including Bosch, Cisco and Gemalto) and IoT technology providers, which launched in September 2017. The TIoTA notes that "Thus far, the Internet of Things has been deployed without much trust in the provenance of device identities, integrity of device software, or verifiability of device data," and

defines as its primary purpose "to leverage the blockchain and other security technologies to introduce trust into IoT, to leverage the automation potential of trusted IoT sensors with smart contracts, to evaluate the ROI of use cases enabled by trust, and to create common open source methods in the smart contracts as a system of lego blocks."

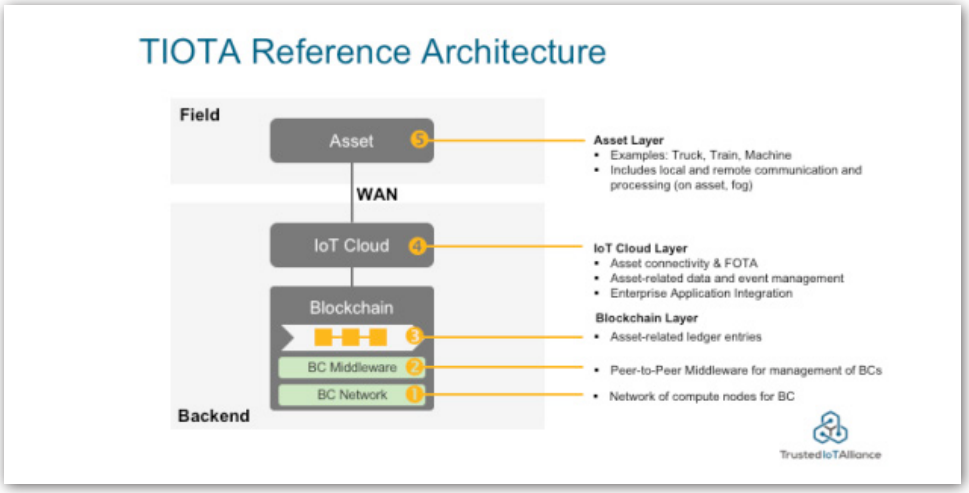


IMAGE: TRUSTED IOT ALLIANCE

In February this year the TIoTA published its Trusted IoT Reference Architecture, following this up in March with the Trusted IOT Alliance Testnet, a global private IP network with member-managed endpoints where any protocol can run and connect to both the internet and the private network.

All this sounds promising. However, in its predictions for 2018, specialist IoT market research company IoT Analytics sounded a cautionary note: "At this point, we believe that it could easily take 5+ years before the [blockchain] technology gets used to secure individual end-to-end IoT applications in the field or before a significant number of devices autonomously engage in a smart contracts-based data exchange."

IOT AND AI/ML

Exponential growth in the number of IoT devices will require new data-processing architectures and serious attention to security. But perhaps the key link in the value chain will be the application of artificial intelligence (AI) and machine learning (ML) algorithms to extract actionable insights from the resulting flood of IoT data. These algorithms could be deployed at the edge (flagging up and transmitting anomalous data patterns, for example), or at the core (analysing medium/long-term trends, for example).

IoT data will come in different volumes, varieties and velocities, and, as the authors of this February 2018 research paper note, the broad goal is to use data mining and AI/ML algorithms to uncover patterns and generate insights in the most efficient manner possible.

In their paper, Mahdavinejad et al provide a listing of the 14 most common supervised, unsupervised and reinforcement ML algorithms for classification, regression, clustering and feature extraction. These algorithms range from K-Nearest Neighbours and Naive Bayes to One Class Support Vector Machines and Feed Forward Neural Networks, via Linear Regression and Principal Components Analysis, and are matched to typical IoT and smart city use cases.

The main takeaway from this study is that different IoT applications involve different numbers of devices and types of data, which generate specific features that will be best characterised by applying the most appropriate ML algorithm—turning 'big' data into 'smart' data in the process.

What does all this look like in practice? IoT platform provider C3IoT offers a good example in the nuts-and-bolts area of inventory optimisation, where the disparate data sources include "demand, supplier orders, production orders, bill of materials (time-varying), change history of re-order parameters, and inventory movement data". Using the company's AI-driven C3 Inventory Optimization application, a global manufacturer of complex equipment achieved a 30 percent reduction in inventory levels and projected annual savings of $100-$200m:

IMAGE: C3IOT

"Thanks to the intersection of today's elastic cloud, big data and IoT technologies, combined with the application of powerful AI methods, manufacturers can now finally realize the promise and benefits of dynamic, adaptive inventory optimization," the blog post concluded.

IOT DEPLOYMENT: THE STATE OF PLAY

Cisco

At the Internet of Things World Forum (IoTWF) in May last year, Cisco presented the results of a survey covering 1,845 IT and business decision-makers in enterprise and mid-market companies from the US, UK and India. Six industry verticals were represented: retail/hospitality, energy, transportation, manufacturing,

local government and healthcare. All respondents worked in organisations that had already completed or were developing IoT initiatives, and all were involved in the strategy and direction of at least one IoT initiative.

The resulting report, The Journey to IoT Value: Challenges, Breakthroughs and Best Practices delivered a surprising headline finding, given the amount of hype surrounding the IoT in recent years: only around a quarter (26%) of surveyed companies were successful with their IoT projects—although as Cisco's IoT marketing chief Inbar Lasser-Raab noted in her IoTWF presentation, only 15 percent were "truly failing".

That leaves around 60 percent of companies who were neither succeeding nor 'truly failing' with their IoT projects, so it's no surprise to see statements such as these emerge from Cisco's survey:

- 60% believe that IoT initiatives look good on paper, but prove more complex than expected
- 64% agree that learning from stalled or failed initiatives help accelerate their IoT investments
- 61% believe they have barely begun to scratch the surface of what IoT can do for their business

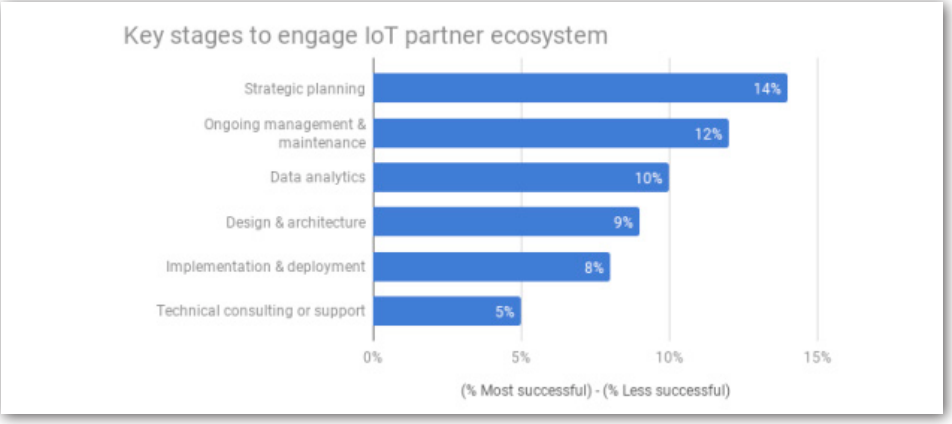
What did Cisco learn from the 26 percent of companies that did achieve IoT success? Key factors here were: good collaboration between IT and the business; a technology-focused culture; and IoT expertise gathered via internal and external partnerships.

Generally, IT executives were more positive, with 35 percent considering their IoT initiative a complete success, compared to 15 percent of business executives. There were differences in emphasis too: IT types stressed the importance of technologies, organisational culture, expertise and vendors; meanwhile, business execs were more interested in strategy, business cases, processes and milestones.

On the partnerships front, successful organisations were more involved with the partner ecosystem at every stage of their IoT projects:

IMAGE: CISCO

If we look at the 'delta' between most successful and less successful organisations, it seems that partner involvement at the strategic planning stage of IoT projects is currently most important:



DATA: CISCO / ANALYSIS & CHART: ZDNET

When it comes to 'blockers' holding up the progress of IoT projects, the key factors in Cisco's survey were time to completion, quality of data, internal expertise, IoT integration, and budget overruns.

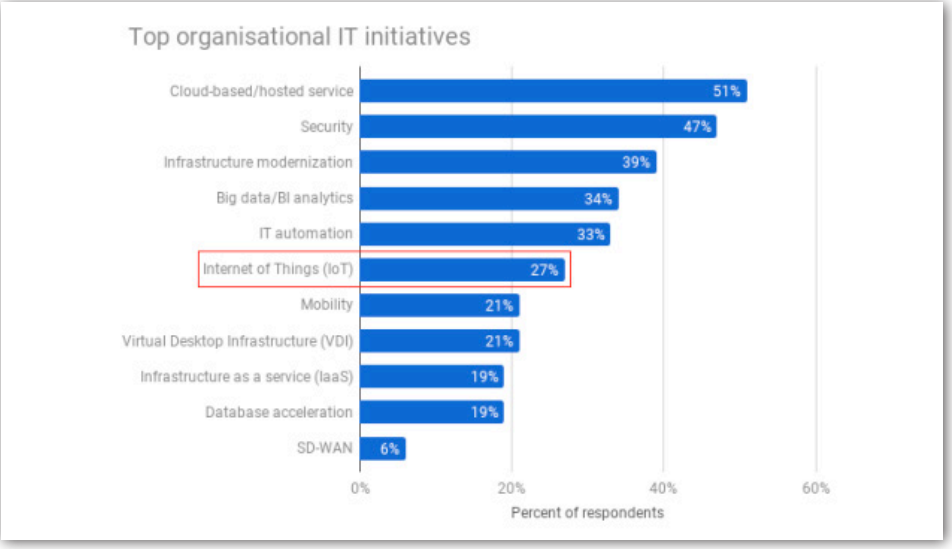
Despite the relatively low overall percentage of successful projects in its survey, 73 percent of Cisco's respondents felt that IoT data was benefiting their businesses in areas such as: improved product quality or performance; improved decision-making; lowered operational costs; improved or new customer relations; and reduced maintenance or downtime.

Cradlepoint

With help from Spiceworks, Cradlepoint—a provider of cloud-based WAN networking solutions for enterprises—surveyed 400 IT professionals in the US, Canada and the UK for its State of IoT 2018 report. Respondents were all involved in some capacity with IoT strategy, and worked for companies with at least 500 employees. Industry sectors represented were: manufacturing, education, IT services, healthcare, government, retail/wholesale, financial services, construction, telecommunications and energy/power/utilities.

In Cradlepoint's survey, only a third (32%) of organisations said they currently used IoT, although more than two-thirds (69%) had adopted or planned to adopt IoT solutions within the next year. As with Cisco's survey summarised above, the broad-brush picture here is one of a technology area that's on the cusp of lift-off.

Supporting that interpretation is the fact that just 27 percent of respondents identified IoT as a top initiative for the coming year:

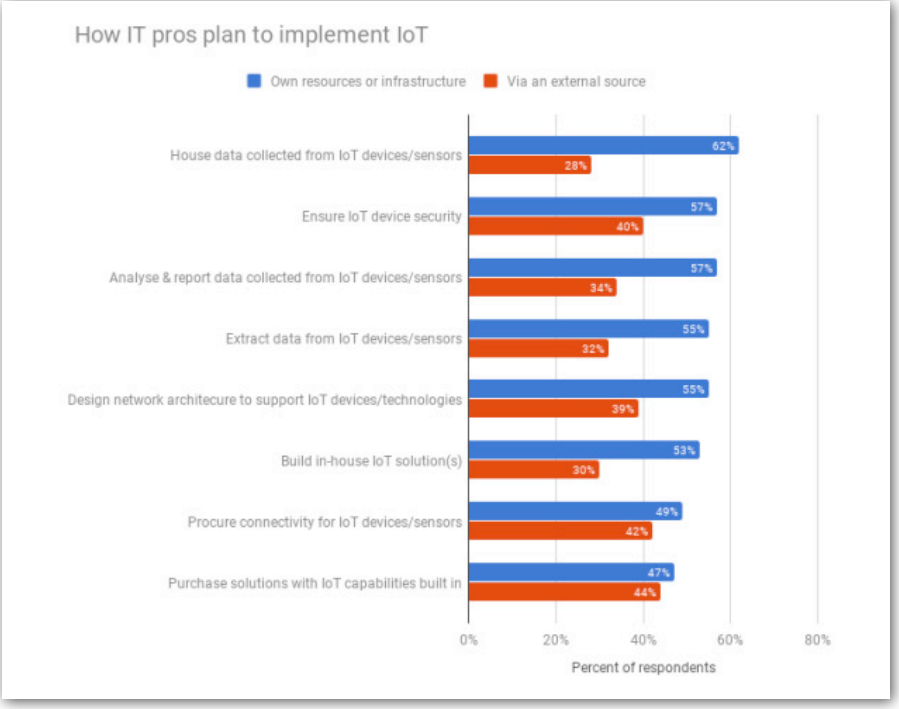


DATA: CRADLEPOINT & SPICEWORKS / CHART: ZDNET

Given that IoT projects require considerable re-engineering of IT infrastructure and for security and analytics to be in place, it's no surprise to see these initiatives ahead of IoT in the IT priority queue. In fact, when evaluating IoT projects, the main factors considered by Cradlepoint's respondents were security (41%) and return on investment (35%).

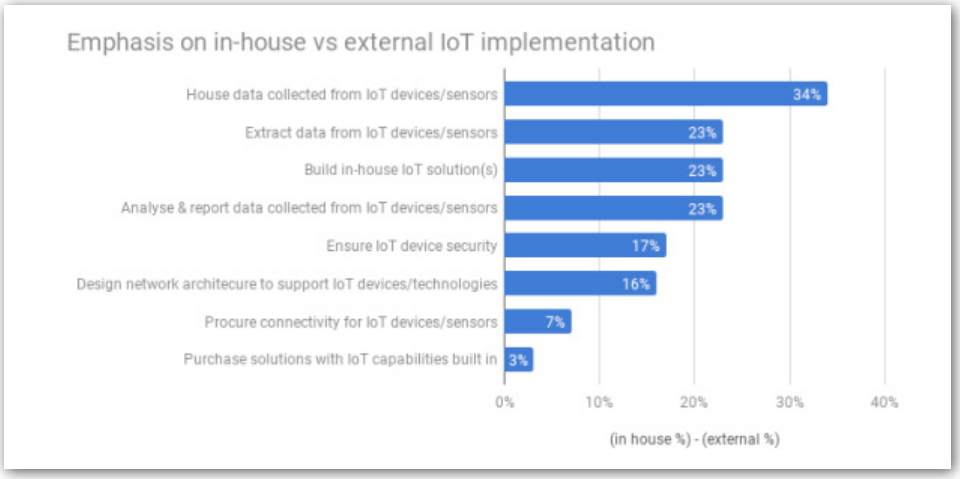
Ironically, although security is a major worry with the IoT it's also a top driver for IoT adoption (along with improved operational processes, reduced OpEx, simplified management, reduced IT complexity and improved flexibility): in Cradlepoint's survey, 71 percent of respondents said they were using IoT for building security applications. Yet it was insecure IP cameras (and other IoT devices) on internet-facing networks that allowed attacks such as Mirai to occur, fuelling fears about the IoT. Even so, nearly half (49%) of Cradlepoint's respondents said their IoT systems would reside on core enterprise networks, rather than a separate network dedicated to IoT technology (40%).

Another concern raised by Cradlepoint is the extent to which companies plan to implement IoT systems in-house, rather than partnering with external providers. In all eight stages covered by the survey, in-house implementation trumped external partnership:



DATA: CRADLEPOINT & SPICEWORKS / CHART: ZDNET

Looking at the 'delta' between these numbers, IoT data storage emerges as the most in-house-biased stage, followed by data extraction, solution building and data analysis:



DATA: CRADLEPOINT & SPICEWORKS / ANALYSIS & CHART: ZDNET

"Organizations that plan to implement, house, and manage IoT in-house are taking a back-to-the-future approach," concluded Cradlepoint, echoing the finding of Cisco's survey that IoT projects are more likely to succeed if companies involve the partner ecosystem rather than try to go it alone.

Cradlepoint concludes with some best practices that, it says, "will allow companies to mitigate the potential for a massive security incident and increase the odds of achieving ROI on IoT systems":

- Treat network security as a foundational consideration from the inception of the planning process, not as an afterthought.
- Do not try to implement IoT applications using only in-house resources and IT generalists. Work with one or more trusted partners/vendors with IoT expertise to drive initiatives forward effectively.
- Consider whether legacy network infrastructure—which requires manual, error-prone, and time-intensive network segmentation and policy orchestration—can really meet the needs of this fundamentally different technology.

OUTLOOK

The Internet of Things has been hyped, discussed and piloted for years, but is now beginning to deliver real business benefits. However, with surveys revealing only moderate success rates for IoT projects, there's clearly work to do in deploying suitable edge computing architectures, setting up trusted (blockchain-mediated) data flows, and applying the most appropriate AI/ML algorithms to extract actionable insights. The IoT is a complex area and, it seems, businesses would do well to look beyond their in-house resources in order to maximise the chances of a successful result.

SURVEY SHOWS THAT MOST BUSINESSES ARE TAKING STEPS TO SECURE IOT DATA

BY AMY TALBOTT

IoT devices can be a valuable source of data that would otherwise be difficult to obtain. Two use cases recently reported by ZDNet sister site TechRepublic include measuring restroom traffic at busy airports and detecting early warning signs of natural disasters, like earthquakes and avalanches.

With providers like Amazon and Microsoft offering new solutions for deriving business value from IoT data, this space is becoming more accessible to companies of all sizes.

Tech Pro Research wanted to find out how companies are taking advantage of IoT capabilities. In a survey of 104 professionals, 85% said their company was using, or considering using, the technology in some way. Most said their company was using IoT devices as part of business operations or was considering doing so.

Security can be a big concern when working with anything connected to the internet. There have been a number of high-profile stories about IoT security incidents in recent years, and as reported recently by ZDNet, IoT security spending is projected to reach $1.5 billion this year.

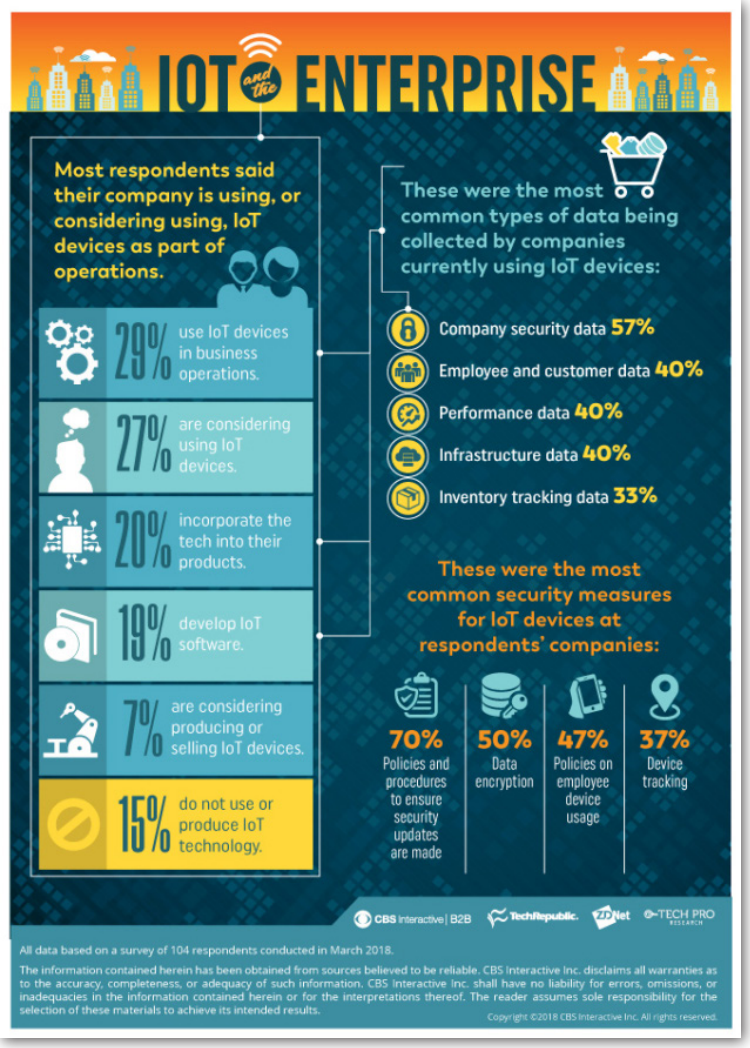


IMAGE: ERIK UNDERWOOD

The sample size from Tech Pro Research's survey was small, but 97% of respondents from companies where IoT devices were in use said their organization takes some security measures. Many indicated that their company used more than one method to secure IoT devices.

Our infographic contains selected results from the survey. The **full research report**, containing all survey data plus analysis, is available to Tech Pro Research subscribers.

SOUTH KOREA'S IOT IN FULL SWING: FROM WATER METERS TO AI-POWERED SMART BUILDINGS

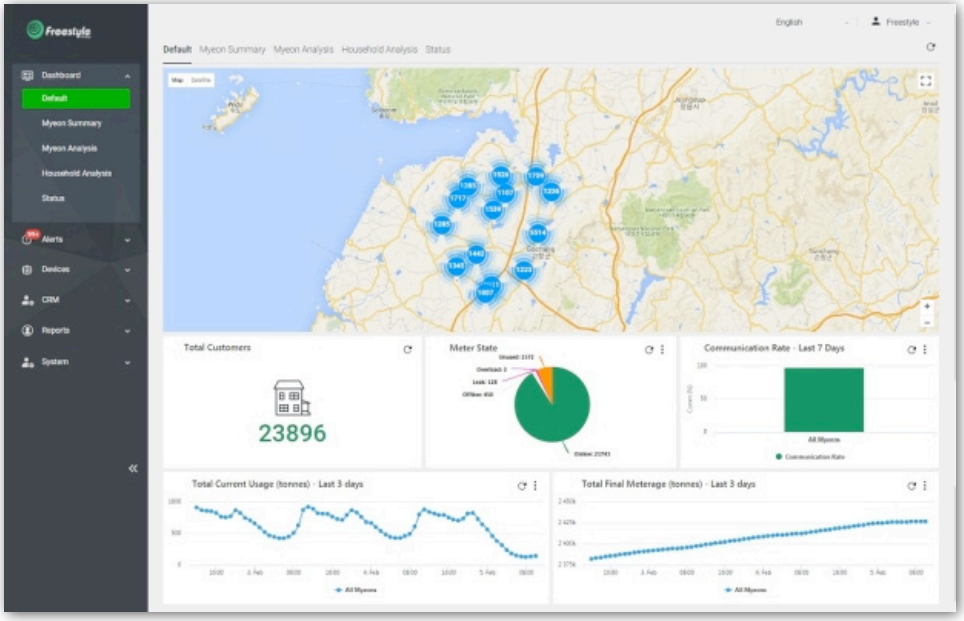
BY CHO MU-HYUN

Gochang is a relatively small, rural county in South Korea in North Jeolla Province, 260 kilometres south of the capital Seoul. It borders the Yellow Sea to its west with a 70-kilometre coastal line, and, by all accounts, it's quite a sight. The county has a very small population of just 58,181, as of March 2018, according to the Ministry of Interior. But it has an area of 606.90 square kilometres, slightly larger than Seoul, which has a population of 9.86 million as of 2017, around 20 percent of the country's 50 million.

It's not easy for county officials and sensors, especially metermen checking water usage via monthly home visits, to get around. If there is water leakage, it takes one to two months to confirm. The problem is exacerbated by the delayed response. And then there is the occasional dispute over the bill with residents.

Enter smart water meters: digital meters that allow the county to monitor and read water usage remotely in real-time without the need to send personnel.

Gochang is the first in South Korea to deploy smart water meters county-wide in one go. Deployment began last year in collaboration with Australia-based IoT firm Freestyle Technology, which supplied all the necessary equipment, from the smart meters to repeaters. Installation was completed in 24,104 homes in December.



GOCHANG CAN NOW VIEW WATER USAGE BY HOMES IN THE WHOLE COUNTY. (IMAGE: FREESTYLE TECHNOLOGY)

"We approached it as a welfare project for residents," said Kim Sang-ah, manager at Gochang Waterworks, the water and sewage enterprise of the county, and manager of the project. "The meters allowed us to accurately relay information to residents on their usage and bill, which were one of the main complaints we received previously.

Another is preventing damages from leakages. Cost stemming from water leakages fell 19 percent in March from a year ago."

It wasn't just about convenience; there were also social benefits.

"The biggest gain, we think, is increased safety for the residents, especially the elderly. Water is always being used, daily. We find households that have not used water for 48 hours and we contact them or their relatives. Residents gave the greatest positive feedback for this," Kim said.

South Korea has one of the highest suicide rates in the world; the elderly and socially marginalised are especially vulnerable. In April, a 41-year-old mother and her 4-year-old daughter were found dead in their apartment at neighbouring Jeungpyeong County, North Chungcheong Province, in a double suicide. It was later revealed that the pair died months ago, with their water bills unpaid for months.

A remote water reader solution like those now in Gochang could have prevented the tragedy, Kim said.

Younger generations move to the cities for better jobs; their elderly parents usually stay behind in their rural hometowns. The distance is a cause of worry for many families.

"We see, going forward, more and more IoT projects being deployed all over the county, which will be good public policy," he said. "We are mulling over a smart streetlamp project that will use the same repeaters that we use for the water meters."

'IOT IS AN IRREVERSIBLE TREND IN UTILITIES'

South Korea's towns, counties, and cities are increasingly eyeing IoT adoption in infrastructure and unities, especially in water, which along with roads, require local governments to build, manage, and supply by Korean law. That provides an incentive in a democracy for municipalities to do good public work.

Gimje City, a North Jeolla Province neighbour of Gochang, has also begun deployment of smart water meters supplied by Freestyle Technology. The city will start with two towns numbering 2,290 households.

"We had some problems with old buildings with outdated water pipes that are especially vulnerable to leakages in the winter," said Song Jin-hee, officer for accounting at Gimje City's water and sewage department.

"We are taking a step-by-step approach, run annually, in installation. Today, technologies and cost are changing so fast. We want to keep our options open," Song said. "IoT, we think, is an irreversible trend. In the long-run it will especially contribute in alleviating the burden of cost for residents, because we can use the same equipment network, base stations, and repeaters that we use for water to control other utilities and public services, driving down the cost."

It was the municipalities in the mountainous and high-altitude Gangwon Province, the northeastern most region of South Korea, that first eyed smart water meters. Pyeongchang, which hosted the Winter Olympic Games earlier this year, was one of the first to deploy smart water meters in the country.

GIMJE IS ALSO DEPLOYING SMART WATER METERS LIKE GOCHANG SEEN HERE. (IMAGE: GOCHANG COUNTY)

There was real demand due to random pressure depending on area. A myriad of altitudes has made water and sewage management much more difficult compared to other counties and cities. Starting in 2007, Pyeongchang deployed the meters block by block and achieved 80 percent coverage by 2014.

Taebaek City and Yeongwol County of the same province are also moving to install smart water meters, county officials said. Jaecheon City of North Chungcheong Province was also an early adopter, installing digital water meters from 2009 to 2012, which cost $3 million. The equipment used is likely not as sophisticated as recent products, officials said.

Besides water, electricity and gas are also seeing more IoT applications. The most ambitious so far, however, is likely the state-run Korea Electric Power Corporation (KEPCO)'s Advanced Metering Infrastructure project. The corporation began the 1.7 trillion won—around $1.5 billion—project in 2013 and the goal is to install around 22.5 million intelligent electricity meters in households with complete national coverage by 2020. KEPCO's regional offices will monitor electricity usage in real time.

SCALING UPWARD: FROM LOCAL TO GLOBAL

Advances in transmission technology and computing power in the past decade have been instrumental in increased application of IoT in utilities and infrastructure areas, according to Song of Gimje.

"These concepts are not new, and have been attempted years ago, but many were canned because the low transmission accuracy rate. If you remember back in the feature phone days, sometimes you would get texts minutes or hours later than when they were sent. It was the same with this equipment," Song said.

"But today, on average vendors have very high accuracy rates. Tests for our smart water meter showed an accuracy of 98.9 percent, above the 98 percent we required for the order."

South Korea is one of the most wired places in the world and boasts the best networks, making it an attractive test-bed for IoT for both local and global firms. The country rolled out a 4G LTE network in 2011, and completed national coverage in 2012. The rollout of IoT-dedicated networks by telcos with more competitive costs has also made IoT projects more alluring for local governments.

SOUTH KOREAN TELCOS LIKE SK TELECOM HAVE DEPLOYED LORA NETWORKS, LOCALLY AND ABROAD, ALLOWING IOT COMPANIES TO LEVERAGE THEM FOR MORE INTEGRATED SERVICES. (IMAGE: SK TELECOM)

The networks have allowed deployment to scale. Daegu, Korea's fourth-largest city with a population of 2.5 million, has been one of the most ambitious in adopting IoT. SK Telecom invested 90 billion won to build a city-wide LoRa network. The city already boasts smart LED streetlamps, smart crosswalks, CCTVs, smart parking that checks parking availability, and number plates that capitalize on the infrastructure. It also allowed new businesses: SK Telecom launched a solar power usage reading service based on its LoRa network.

DIVERSE APPLICATIONS

High Tech is an IoT company specialising in protecting cultural heritage. Based in Gangwon Province, the firm last year worked with the local government to install low-power displacement sensors that detect displacements, humidity, temperature, and tremors on four cultural sites. It provides its own LoRa network and does not require the installation of electric and communication wires on the ancient buildings. This is important, as most ancient buildings are a fire hazard due to a large prevalence of wood.

HIGH TECH'S SENSORS DETECT ANGLE OF CULTURAL HERITAGE TO MONITOR DISPLACEMENTS. (IMAGE: HIGH TECH)

The sensors are not mains-powered, but have batteries that last one to two years depending on usage. Data is sent to the command centre every five to 30 minutes for monitoring. The data allows inspectors to find damage and detect possible damage from natural disasters or ageing in order to apply appropriate measures to protect the sites.

"Most detection tools used in cultural heritage sites use wired detectors that damage them directly over time, or may inadvertently do so," said High Tech CEO Choi Jong Un. "By applying IoT, governments can protect their sensitive cultural heritage sites as well as save cost in maintenance."

NTELS is an IoT firm that offers an integrated building management system that allows the monitoring of energy consumption and safety status of buildings. The company is partnered with Suwon City and the

solution is applied to 100 public buildings. Suwon's city hall can manage the entire roaster while individual buildings can also monitor their own. Access is divided to three security clearance levels.

Artificial intelligence (AI) was applied to the monitoring system so that it can predict energy usage and become more efficient as more data is collected. The tenants of the buildings themselves, not just the IT managers, can access the system within their designated areas to turn on or off lights, gas, and other utilities.

"In smart building business, connectivity is no longer a differentiator, because that is a given," said Park Chang-soo, general manager at NTELS' IoT development team. "So there needs to be added value such as AI atop high integration. We also differ in that we also offer tenants control over their workspace IoT."

THE ISSUE OF COST, REGULATION, AND PRIVACY

Despite the increased adoption and innovation, hurdles remain. The relatively successful deployment and coverage of Gochang relied largely on the cost benefit ratio. According to county officials, the project cost some $5 million. Larger municipalities find the cost less attractive as they attempt to scale. Network costs have declined as well over the years, thanks to IoT-dedicated networks, but for many municipalities it is still a strain on their budgets.

"No one disputes the benefits of deploying IoT for utilities. But the biggest obstacle is and remains cost," said Kim Jong-hoon, an officer of Korea Environment Corporation (K-eco), a subsidiary agency to the Ministry of Environment, working in its regional office at Pyeongchang and collaborating with the local government.

K-eco, in collaboration with the local government and telco LG Uplus, has been testing 100 units of water leakage sensors since last year.

"Among officials there is an expectation that prices will fall as early as the second half of this year or the first half of next year. But it remains to be seen," he said.

Individual municipalities also look for IoT portfolios specific to their needs, and the right product wasn't easy to find, Kim added.

"Market demand will automatically lead to competitive prices" said High Tech CEO Choi.

The biggest obstacle for the companies has been regulations that limit spectrum use depending on industry. Government buildings, and agencies such as the fire department, use their own networks and frequencies.

BUSAN METRO HAS INSTALLED A IOT-BASED EVACUATION SYSTEM. SIGNS LIKE THESE TELL WHICH ROUTE IS THE FASTEST AND SAFEST FOR EVACUATION. (IMAGE: MINISTRY OF SCIENCE AND ICT)

"It would be easier to deploy smart building solutions like ours if we had access to those networks," said NTELS' Park.

Standardisation was also an issue.

"What constitutes IoT can be very different country per country," said Park. "We wish there was more coordination between governments. There also needs to be more dialogue between governments and companies."

Privacy, or security, is more complicated picture. For example, Gimje cited the privacy as one of the main reasons of rolling out smart water meters. There are concerns that these devices are vulnerable to hacking; KEPCO last year faced intense scrutiny for their digital electricity meters that allegedly had incompetent security within the chips.

But the overall outlook remains optimistic for many.

"I can't say whether it will be one year, or three years, or 10 years from now," said K-eco's Kim. "But we are getting to a place where IoT will be massively deployed eventually."

SUCCESSFUL IOT DEPLOYMENT: THE ROLLS-ROYCE APPROACH

BY MARK SAMUELS

There is a lot of hype when it comes to delivering value from advanced technologies, such as the Internet of Things (IoT), artificial intelligence (AI) and big data, but Rolls-Royce is using a combination of these to create business benefits for its customers.

Late last year the engineering firm announced its R² Data Labs initiative, which aims to use machine learning, AI and data analytics to create new services.

At the heart of the labs are what Rolls-Royce calls 'Data Innovation Cells'; groups of data experts who work with teams from across the company's operations. These groups use DevOps principles to explore data, test new ideas, and turn those ideas into new innovation and services in areas such as asset availability, efficiency and maintenance or safety and compliance.

"The way you get to something that's worth doing well is via rapid iteration. We collaborate with our customers, whether internal or external, using a design thinking approach to identify a business opportunity."

—Caroline Gorski

By the end of this year, the company said, it will receive more than 70 trillion data points from its in-service fleet each year and has plans to use this to develop an engine which is "connected, contextually aware and comprehending", it says.

Caroline Gorski, director of the global ecosystem at Rolls-Royce's R² Data Labs, says the company has 30 years of data integration experience.

The R² Data Labs team, which includes 200 data architects, engineers, scientists and specialist mangers, has helped Rolls-Royce deliver more than £250m in value through engine health monitoring activities in the past 12 months. These activities run on 90-day sprints. During that process, Gorski says the team moves from an ideas phase right through to minimum viable product creation.

"The way you get to something that's worth doing well is via rapid iteration," she says. "We collaborate with our customers, whether internal or external, using a design thinking approach to identify a business opportunity. We rapidly release proof of concepts to demonstrate the validity of that approach."

MAKING THE UNKNOWN VISIBLE

Gorski, who joined Rolls-Royce in October 2017, has a broad range of experience when it comes to the implementation of advanced technology. She was previously head of IoT at accelerator Digital Catapult and head of business development for IoT at Telefonica.

"The IoT is useful when you know you can derive business benefit by making unknown processes visible," she says.

"If you try and use sensors everywhere, you will get nowhere because it's too expensive and it's too imprecise. Rolls-Royce picks the places where its IoT solutions can make data visible, and which will create significant operational benefits. That, for me, is the key to a successful IoT deployment."

Gorski advises other digital chiefs to analyse their business operations and understand where a lack of data transparency creates a headache. She has seen big-bang instrumentation projects happen and, for the most part, these are difficult to justify.

"They end up being expensive to implement," says Gorski. "It's costly to transmit data and the business ends up with a patchwork quilt of information. It's important to remember there isn't a single solution for IoT instrumentation and you must bootstrap technology together from lots of different suppliers. All that bootstrapping adds costs and creates complexity."

Her experiences lead her to conclude that spotting areas were it's hard to find the right data is key.

"I think if you're going to really make the most of the IoT, the first question you must ask is where in your organisation is a lack of transparency creating you issues. Because that is where you're going to get the value back to pay for your investments," says Gorski.

FINDING THE RIGHT SKILLS AROUND THE GLOBE

Gorski, who spoke with ZDNet at the recent Big Data World event in London, says R² Data Labs works with customers, such as private jet operators and shipping companies to come up with new services.

"It's a balance between what gives you pain today and what represents a potential answer—and there isn't always a sequential step between those points," she says. "The good news is once you have great business cases, you can use that evidence as proof points of your successful approach."

Gorski runs a specialist team within R² Data Labs that scours the world for partners—be that entrepreneurial individuals or leading-edge companies—to work with Rolls-Royce.

"We recognise within R² Data Labs that in a world of data innovation, particularly around AI and advanced analytics, it's not possible to build all of those skill sets internally," she says. "It takes too long, it's incredibly expensive and the individuals with those capabilities are in high demand."

Gorski's team brings partners into the organisation to fill skills gaps, either as part of a specialist cell within R² Data Labs or through a joint venture agreement. This joined-up team of internal and external talent then focuses on four technology areas: industrial IoT; autonomy and sensing; blockchain and quantum computing; and AI and advanced analytics.

MAKING THE DATA WORK FOR YOUR CUSTOMERS

The best way to demonstrate how her team works, says Gorski, is through examples. She refers to the Engine Network, which is a tool that allows Rolls-Royce to extract IoT sensor data from engines and health-monitoring systems, and to combine those records into a social network for the individuals who develop and use an engine.

Rolls-Royce engineers and private jet management companies can exploit this data to analyse engine performance. The platform also includes an AI-based recommendation engine that presents issues proactively to engineers, so they are aware of issues before a problem exists.

"They can look at anomalies and compare performance indicators with other engines that perform in a similar way," says Gorski. "This proactive approach creates enormous benefits for our service community and for the end customers that buy our jets."

Gorski also points to pioneering work in the marine business, where R² Data Labs has been using IoT sensors to track ship performance. By combining this information with contextual data from the wider marketplace, the team has created a fuel-efficiency guidance portal for crews sailing Rolls-Royce powered-ships.

The portal was built through multiple iterations. The first deployment took about six months and further modifications were made post-launch. The portal now sits on a secure cloud and its data is available to Rolls-Royce owners.

"The captains piloting ours ships can have real-time messaging from us that tells us how to save fuel, how to sail efficiently and how to deal with challenging sea conditions," says Gorski. "That kind of insight is absolutely transformational when it comes to operating a marine fleet."

TEXMARK CHEMICALS DEPLOYS INDUSTRIAL IOT TO CREATE THE REFINERY OF THE FUTURE

BY TEENA MADDOX

Texmark Chemicals is a boutique chemical processing facility that manufactures hazardous materials that are part of the petroleum product supply chain. The company teamed with Hewlett Packard Enterprises (HPE) to deploy industrial IoT to create a safer environment for employees while saving money with uninterrupted productivity, increased up-time and better process analytics.

Texmark is in the third phase of a three-part IIoT project to combine HPE and Aruba solutions from HPE Pointnext to create the "refinery of the future." Phases one and two established the digital foundation by enabling edge-to-core connectivity. Aruba deployed a secure wireless mesh network with access points and ClearPass for secure network access control. Aruba beacons provide location-based services for plant safety and security purposes. The wireless solution cost about half of what it would have cost to deploy a hardwired network.

For its edge analytics, Texmark is using the HPE Edgeline Converged IoT platform, an industrialized solution that supports robust compute capabilities. HPE Pointnext implemented the system as an HPE Micro Datacenter. HPE also upgraded Texmark's plant control room to enable edge-to-core connectivity and high-speed data capture and analytics, and to meet Texmark's safety and security standards. The Edgeline system runs Texmark's Distributed Control System software, which integrates operations technology and IT into a single system. The third phase is adding predictive analytics, advanced video analytics, safety and security, connected worker, and full lifecycle asset management.

A GROWING MARKET FOR DCPD

Texmark is headquartered in Galena Park, a small town on the Houston Ship Channel. It produces dicyclopentadiene (DCPD), which is a polymer used in printer ink, boat hulls, insecticides, paint, varnishes, fragrances and rubber goods.

Worldwide demand for DCPD is growing at approximately 4% compound annual growth rate (CAGR) between 2017-2024 and the global market is anticipated to reach about $800 million by 2024, according to a research report by Global Market Insights, Inc.

The increased demand is one of the reasons the company was in a position to improve its operations.

UPDATING A FAMILY-RUN COMPANY

Texmark was founded in 1962 by the father of current CEO Douglas Smith.

Smith said, "Over the last 15 years we've made significant capital investment within the process facility to help us make DCPD and other chemicals better and more efficiently. But we did an analysis about three years ago and determined that there were some areas, one that we determined on our own and the other that was determined for us, in which we needed to make some changes. And one of these was what's called mechanical integrity, which is looking at the condition of the different pieces of equipment in your facility. We had been doing mechanical integrity, but we had been doing it in a non-linear way."

IMAGE: TEXMARK

The company was spurred into action when insurance deductibles doubled due to the need for the implementation of an updated inspection plan. Smith, working with Linda Salinas, the company's vice president of operations, realized they also needed to improve the company's technology base, "what we call our DTS, our control system. We knew that we needed to update it and we had built it also in bits and pieces over time and it was essential that we got moving on that."

PARTY BUS TO HPE'S IOT INNOVATION LAB

After talking to HPE about innovation, they decided to visit the company's IoT lab, even though IoT was a new concept for many employees.

Salina recalled, "We rented a party bus and put 13 Texmark employees in it. We all got matching Texmark shirts and we were going on a field trip. And it was exciting for these employees because they weren't part of the meeting. They didn't know what IoT was. They just knew that we were leaving the plant and we got to do this on company time. And it was a cross-section of people from the lab, engineering, operations, maintenance, admin folks. It was a good representation of the people that run the business for us."

"We got there and one of the representatives from HPE gave us mini-lecture and defined for us what IoT was. And even after that lecture it really just didn't ring clear for us what IoT meant," she said. "So then, we actually toured the lab. It's like an interactive science museum."

VALUES IN THE PROCESSING UNIT AT TEXMARK. (IMAGE: TEXMARK)

There was a centered pump on display in the lab that drew everyone's attention.

"The pump represents one of the cores of our business and it was familiar to everyone. We all gravitated towards that and it was a flowserve pump and it was just blowing green water in the pump and out of the pump," Salinas said. "We have pumps at the plant that move the product from the storage tank through the process, out of the process, into the storage tank, in a truck, the rail cars and so forth. So this was very familiar. So we go over and look at this demonstration and they have it set up so that you can make the pump be misaligned. You can make the pump operate in a way that is not optimal. And then on the handheld device, like an iPad, it would show on the screen that before, when it was running normally, the predicted life was maybe 600 hours. But then when you took the pump out of alignment and it started acting erratically, instead of running for the next 600 hours, it reduced the expected life to like 60 hours. And if you really mess with the alignment, something really radical, it might last only six hours."

After realizing the way that IoT sensors could help with maintenance and know when something was off before employees could even see it really hit home with the Texmark employees.

SAVING MONEY THROUGH INCREASED EFFICIENCY

"The pumps are the perfect example of saving money. And the reason why is for any piece of equipment, let's say any pump in the plant, if we are to connect it with wire, if we have to hardwire that pump and run it from the control center to the pump, it can cost anywhere from $2,000 to $7,000 to hardwire that pump. By placing $300 worth of [wireless] sensors on the pump and piping that information into those with widgets and Wi-Fi, there's a considerable savings," Smith said.

Texmark currently has wireless sensors on two pumps and will eventually put them on all of the pumps involved in production.

Currently, employees spend 35,000 hours each year monitoring the plan, which means more than $1 million in inspection program costs. Texmark is determining how many hours are saved by reducing hands-on inspections, but it is expected to be considerable, Smith said.

As a boutique chemical plant, Texmark has customers that bring them raw material and Texmark processes it on its equipment to create an end product that the customer receives. Right now, Smith is talking to a potential customer who came to them simply because they'd heard about the IoT sensors in the plant, and they were interested in the benefits and cost savings.

The vast amount of data that Texmark receives from the IoT sensors also helps, because it allows for assessments throughout the production process. "Having every inch of data along the way and how it impacts the quality of the product that we're making for them. All of that data is valuable to them because then we can tweak how we ramp it up," Smith said.

The safety aspect is also important. Salinas said, "the safety aspect really gets me excited. If you look at each one of these use cases that we're looking at: the sensor pumps, the video analytics, connected worker, and total asset management, in one way or another they touch and impact safety and reduce risk. So when we talk about the sensored pump, if a pump fails, not only does it mechanically break, there's risk that it will leak hydrocarbons, which are flammable, which will then potentially catch fire, potentially injure someone."

"We talk about sensored pumps as something that's to protect the assets, but in the end it reduces risk and improves safety," she said.

HOW TO CREATE A DATA STRATEGY FOR ENTERPRISE IOT

BY ALISON DENISCO RAYOME

Enterprises deploying Internet of Things (IoT) devices are collecting large amounts of data in hopes of gaining insights to improve operations, safety, and costs. However, many organizations lack a strong data strategy for these growing IoT projects, sidelining IT and potentially putting the company at risk.

"The best way to prepare for IoT data is to first make sure that your existing data is well managed, well secured, and that you're getting value out of it." —Mark Hung

When it comes to enterprise adoption of IoT, most deployments are still in a pilot or proof-of-concept phase, according to Forrester Research senior analyst Paul Miller. These projects are often driven by operational teams, and are not necessarily linked to enterprise-wide technology strategies for cloud or data.

"A lot of these deployments are early, small, and often under the radar of central IT," Miller said. "As they become more mission critical, there will be a very real need to ensure that they do comply with things like data policies, privacy policies, and security policies. But it's still early days, and there's relatively little formal policy around IoT deployment at the moment."

Most companies are examining how to manage their existing data, in terms of how to secure and extract value from it, said Mark Hung, a research vice president at Gartner. "Both the speed and scale of data that IoT brings is a new challenge," Hung said. With so many endpoints, companies need to prepare to manage a large influx of information that must be analyzed in close to real time to gain the greatest insights, he added.

CREATING AN IOT DATA STRATEGY

Before building an IoT data strategy, companies should ensure that they have a solid foundation for data management, security, and analytics, Hung said.

"The best way to prepare for IoT data is to first make sure that your existing data is well managed, well secured, and that you're getting value out of it," Hung said. Failing to do this means you're just collecting more data on top of the information you have you that you don't get any value from, which makes everything more complicated, he added.

The best data strategies are co-created by stakeholders including the business, the IT department, and the operations team working together, said Christian Renaud, research director of the IoT practice at 451 Research. That group of stakeholders should decide on business objectives and problems to be solved, and then talk to vendors about what is technologically possible. That way, the CFO can ask about costs and revenue, the CIO can determine where the data is stored and how it is handled, and other leaders can make sure their questions are answered too.

"The successful IoT deployments are the ones where they had broad stakeholder buy-in at the executive level," Renaud said. "It wasn't IT or the business going it alone."

In terms of creating a data strategy or policy, companies need to consider any regulations—particularly the upcoming General Data Protection Regulation (GDPR)—as it could impact IoT data, Miller said.

This strategy should also stipulate what data is being collected, where it is stored, and who can access it. For example, if a company uses a machine that offers an IoT-enabled service to analyze performance, you need to consider who has access to that data, and whether you or the manufacturer own it, Miller said. If the manufacturer does own it, then you need to determine if they can sell it to a third party.

"It's not about saying, 'You must collect this and this,'" Miller said. "It's about understanding very clearly what is being collected, where it's going, and who has rights to see it, reuse it, and monetize it."

Today, a lot of data management and analytics strategy involves storage on the enterprise platform level or cloud level, Hung said. "With IoT, just given the scale and the field data, you necessarily have to start pushing some of the costs of obtaining the storage out to the edge," he added. "I think edge computing is going to be one of the critical components to any kind of IoT management strategy."

Companies must also ensure that any IoT data strategy complies with broader data policies, including customer privacy and retention strategies, Miller said.

There is also a large difference between IoT devices used within the organization, and those that are potentially being used by customers, Miller said. In the case of the latter, there is more of a requirement for clear visibility. "The worst possible thing would be for an IoT sensor to be gathering data that no-one knows it's collecting, and sticking it in a cloud store that no-one knows is there," Miller said. "Then someone stumbles across it, and that's obviously bad news."

Finally, an IoT data strategy must consider the tools an organization may need to gain useful information from that data, Miller said. This is where analytics comes into play.

"Simply connecting a device and getting data off it isn't enough on its own," Miller added. "You need to go a step further and start using things like machine learning to actually extract some value from that."

HOW TO CREATE A SECURITY STRATEGY FOR IOT

BY CONNER FORREST

The Internet of Things (IoT) presents a major opportunity for collecting critical data that can be used to fuel digital transformation across the enterprise. Unfortunately, it's also one of today's biggest security risks to an organization.

The number of connected devices will top 20 billion by the year 2020, research firm Gartner predicted last year. These connected devices can help with an organization's automation and efficiency efforts, but they can be difficult to secure and often lack enterprise-grade controls.

However, with the proper security strategy in place, an organization can safely deploy IoT to meet their business objectives while protecting critical assets. Here's how IT and business leaders should go about building their security strategy for IoT.

THE STRATEGY

Businesses should work to develop a specific, standalone IoT security strategy, according to Merritt Maxim, principal analyst at Forrester Research. Taking an existing security strategy and assuming it will work for IoT can be a huge mistake, he said.

Another mistake is to assume that there is an all-encompassing security solution for IoT, according to Gartner research director Barika Pace.

"The first thing I tell people is: Don't keep IoT security in a silo," Pace said. "Often times, people look for an IoT security solution and there isn't one."

IoT integrates with all aspects of security—cybersecurity, physical security, and operational technology security, Pace said. So, business leaders must think about it in terms of a whole security ecosystem.

Because of the multiple layers involved with IoT security, it's also important to plan for unexpected challenges, Maxim said. "This means conducting risk assessments, simulating IoT-specific breaches, and building playbooks that prepare the organization to respond effectively but still maintain a positive customer experience," he said.

It's also key to remember that security pros are human, and can't possibly predict every threat against their IoT deployment, Maxim warned. Instead, "security teams need to forecast and document the most probable, highest-impact IoT security scenarios," Maxim said. This will help them be best prepared for a potential breach.

THE HARDWARE

IoT hardware security is very vertical-centric, Pace said. IT leaders in any market must consider the physical security of the device as well as its software, but one aspect is pertinent across all: The devices must be patchable.

"If you cannot patch those devices, that's where you become heavily at risk," Pace said.

Many legacy devices, like the CCTV cameras and baby monitors attacked by the Mirai botnet, had no means of pushing a security patch. Manufacturers are now thinking more about patchability, Pace said, but older devices should be given extra caution.

IoT security starts at the device purchasing decision, according to Patrick Daly, an associate analyst at 451 Research. At this point, a company must be able to determine if the device has the memory and compute necessary to support extra security. "If the answer is no, the company needs to weigh whether it still wants to move forward in deploying the device," Daly said.

Other red flags are the use of unchangeable, hard-coded passwords, and devices that cannot be updated over the air (OTA), Daly said. Strong authentication and encrypted communications are also key. "However, some devices are so resource-constrained that introducing encryption or cryptographic authentication would have a noticeable impact on performance," Daly said.

Additionally, enterprises should build visibility into their security strategy so that they have a clear view of the devices in their network, along with their "typical communication patterns," Daly said. This kind of information can help when inventorying devices or determining dangerous device behavior.

"The scale and distributed nature of the IoT device data increases the risk of data misuse, whether inadvertent or malicious."
—Merritt Maxim

THE DATA

Perhaps the most valuable result of an IoT deployment is the data collected, but if it isn't protected, it can't be used. Maxim recommends focusing security efforts on analytics, and not just the collection of data.

"IoT significantly increases the amount of available security-related data such as authentication and data usage," Maxim said. "While managing and collecting this scale of data can be challenging, it's an excellent intelligence source that will help identify potential IoT security events and allow your organization to respond quickly to new attacks."

When thinking about data, IT leaders and business executives must put their customer privacy concerns on par with their own. Many IoT devices can capture highly personal data, which can make its way to cloud-based systems and become difficult to assess, Maxim said.

"The scale and distributed nature of the IoT device data increases the risk of data misuse, whether inadvertent or malicious," Maxim said. "With new data privacy regulations such as GDPR coming in force next month, CISOs need to understand if the IoT device's data collection and use are consistent with all relevant legal, regulatory, and compliance requirements."

Compliance, overall, is one of the most difficult aspects of an IoT security strategy. "The landscape is so complex because there isn't a global standard," Pace said.

To determine what regulations apply to your IoT data, Pace said business leaders must understand the following three things:

- What data is being collected
- How that data is processed
- Where that data is stored

Understanding these three factors helps build the groundwork for a compliance strategy, Pace said. The organization can then work with its own legal team, or partner with someone in the region where they are operating to fully build it out.

HOW TO USE MACHINE LEARNING TO ACCELERATE YOUR IOT INITIATIVES

BY CONNER FORREST

As businesses flock to the Internet of Things (IoT), connecting everything in sight and adding new functionality to old hardware, they're all really after only one thing: Data.

Data is the new oil, and an enterprise IoT deployment is an easy way to get a lot of it from many different sources. But in the end, it is what a business does with its data that really matters. It is by putting that data to work that organizations can improve efficiency, boost the bottom line, and drive innovation.

That's where machine learning comes in. It's still a fairly nascent technology, but some companies are using machine learning to boost the value of their IoT initiatives.

For starters, machine learning algorithms can make IoT data better suited for processing and analysis. Businesses can use trained algorithms to help in the organization and tagging of data. Using machine learning, a company can determine data provenance and classification, as well as if it meets certain requirements for compliance. This could be especially helpful for IoT deployments in the highly regulated medical and financial services fields.

Machine learning can also be used for the analysis itself. The technology can "provide predictions, recommendations or potentially prescriptive actions" for enterprise IoT deployments, according to Dave Schubmehl, research director for cognitive and AI systems at IDC.

The core use case for this type of algorithm is predictive maintenance. This is done when sensors on complex machines send data back that is "used to predict when various sub-systems might fail and recommend when that machine should get preventative maintenance to keep failures from occurring," Schubmehl said. By using data to address maintenance issues before failure occurs, businesses can save time and money.

Predictive maintenance use cases represent about two-thirds of the IoT deployments that 451 Research sees, according to Christian Renaud, the firm's research director of IoT.

What typically happens, Renaud said, is that "there's a lot of real-time data that you're monitoring, but you don't really start capturing and analyzing until there's an exception case." One example would be a hospital with high-value refrigerators for organ transplants that need to stay at a constant temperature. No one really cares that they stay at a constant temperature until they don't anymore, and machine learning can (hopefully) keep them from failing.

Resource management is another way machine learning can be used with IoT initiatives. According to Schubmehl, companies like John Deere use "sensors on tractors and farm equipment to monitor the state of the soil, plants, insects, moisture, etc. in order to build predictive models to gauge exactly how much fertilizer, water and pesticides should be applied in order to maximize crop yield."

In the 2017 Gartner report AI on the Edge: Fusing Artificial Intelligence and IoT Will Catalyze New Digital Value Creation, an example was given of how Google uses IoT and machine learning to optimize the resources in its data centers. According to the report, sensors monitor temperatures, power, pump speeds, setpoints, and more. Using that data, and a specific algorithm, Google reduced its cooling bill by 40% and got 3.5x computing power from the same energy consumption.

Data collected from radio frequency identification (RFID) tags can also be used with machine learning to create business value. Schubmehl gave the example of RFID used in the shipping industry to optimize routes and logistics for supply chain. Renaud said this is seen a lot in trucking, where machine learning is used to determine which route impacts the engine the least and helps maintain the best fuel economy.

Currently, machine learning implementations in IoT are more prevalent in mature verticals like manufacturing and transportation that have been working with these kinds of technologies for some time, Renaud said. Most companies, however, are "still in a period of experimentation," where they don't know what the significant variables are yet, Renaud said.

IMAGE: ISTOCK/METAMORWORKS

As machine learning further comes into its own in the enterprise and in conjunction with IoT, other new use cases will present themselves. One of these use cases will be machine learning used to understand contextual customer data.

"You're going to get a lot of user intent from things like omnichannel marketing for retail—being able to tie you as a consumer and your online behavior to what you do in-store," Renaud said.

The Gartner report also mentioned contextual data in retail, specifically using in-store video cameras and machine learning to create intelligent video analytics.

Other integrations of machine learning and IoT include ingestible autonomous surgical robots, using manufacturing data and algorithms to autonomously trigger other specific actions in the manufacturing process, and using connected vehicle data and machine learning to create customized insurance offerings, Schubmehl said.

While it's impossible to predict all the ways that machine learning will impact IoT, it's nearly a foregone conclusion that machine learning will be the linchpin that drives real enterprise value in IoT.

CREDITS

Global Editor in Chief
Jason Hiner

Editor in Chief, UK
Steve Ranger

Managing Editor
Bill Detwiler

Editor, Australia
Chris Duckett

Senior Features Editors
Jody Gilbert
Mary Weilage

Senior Editor
Conner Forrest

Senior Writers
Dan Patterson
Teena Maddox

Chief Reporter
Nick Heath

Staff Writer
Alison DeNisco Rayome

Associate Editor
Amy Talbott

Multimedia Producer
Derek Poore

Associate Social Media Editor
Leah Brown

ABOUT ZDNET

ZDNet brings together the reach of global and the depth of local, delivering 24/7 news coverage and analysis on the trends, technologies, and opportunities that matter to IT professionals and decision makers.

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.