IoT FOR BUSINESS

IoT FOR BUSINESS

Distributed in
THE TIMES

raconteur reports

Publishing manager
Chloe Johnston

Associate editor
Peter Archer

Deputy editor
Francesca Cassidy

Managing editor
Benjamin Chiou

Digital content executive
Taryn Brickner

Head of production
Justyna O'Connell

Design
Joanna Bird
Sara Gelfgren
Kellie Jerrard
Harry Lewis-Irlam
Celina Lucey
Colm McDermott
Samuele Motta
Jack Woolrich

Head of design
Tim Whitlock

@raconteur /raconteur.net @raconteur_london
raconteur.net /iot-business-2020

CHALLENGES

Hype and buzzwords hold back IoT potential

Widespread hype around the internet of things continues to promise great things, but adoption and the pace of delivery has underwhelmed

Josh Sims

Not all is well. "The problem," says Andrew Dunbar, "is that 'internet of things' is such a broad, almost meaningless term. What's more, the whole idea of IoT has been massively oversold, more in emphasis than in inaccuracy. It's all connected underwear and connected bathmats, and that bores people because they can't see the application."

Dunbar is general manager of digital consultancy Appnovation and just the sort who should be singing the praises of IoT, the prospect of interconnecting computing devices embedded in everyday objects including, yes, your pants. But he thinks the story of the potential utility of IoT has been pushed too hard, with wild-sounding predictions that it will, according to Ericsson, be worth some $619 billion to telecom operators within the next six years, and in a way that misses the point.

"The emphasis should be on the goals it might help achieve rather than the processes," he argues. "I'm interested in losing weight, for example. Through monitoring food consumption, minimising food waste and so on, IoT can help me do that. But I'm not interested in the mechanism. I'm interested in the end-result. That's what has been missed: it's about digital means of meeting human needs."

It's certainly true for consumers. But even businesses, given a chance of cost-savings and improved systems, need to see the point. Michelle McKenzie, IoT principal analyst at digital research firm Analysys Mason, concedes that the pace of delivery has been considerably slower than anticipated too, also slowing IoT adoption. All talk and no tech has perhaps been the cause of a surprising lack of awareness of IoT among 25 per cent of small and medium-sized enterprises (SMEs) especially, according to an Analysys Mason survey conducted last year, with 9 per cent of large businesses still not engaged with the idea either.

"One major IoT challenge is there's been too much hype and a lot of discussion of what IoT can do for industry without much proof that it actually can," McKenzie explains. "Frankly, it's hard to see how companies that have deployed IoT have benefited from it, in terms of cost-savings or advantages, even with them understandably not advertising any benefits they've found."

This in part stems from the fact that, once investigated, it becomes quickly clear IoT is, as McKenzie stresses, more a complex ecosystem of hugely variable technology rather than the singular, manageable entity it sounds like it is. It's not just about connectivity, but requires data analytics, cloud services, IoT security products and overcoming a skills gap in handling all these things. And if you have the data, it's not always clear what to do with it. No wonder IoT adoption has faltered.

"Certainly a lot of companies are still coming to terms with what IoT actually is and are reluctant to admit their ignorance," says Martin Franzen, director of digital training company Apis. "But then look at companies that have embraced it and often their systems are entirely internal. There's no real use of the internet at all, so the name itself is confusing. And I'm not sure this is an unusual pace of change for new tech; a couple of years ago everyone was bemused by the cloud too."

Those companies that have already invested in IoT have typically taken a highly customised approach. But it's another IoT challenge that without volume, and the price reductions that come with it, such an approach is also highly expensive and out of the reach of most SMEs. Large companies are almost twice as likely as SMEs to be planning IoT adoption. And that's even with acknowledgement of IoT being a long-term project, with most companies intending to start small, connecting maybe a few thousand devices, and growing from there, with most initially using it to cut costs rather than develop new services.

There are companies well down the path in arranging their IoT readiness. The Weir Group, supplier of engineering solutions for the minerals, oil and gas industries, is already providing smart products to provide real-time equipment monitoring, with the future likely to see such boons as predictive maintenance and autonomous operation.

"How to get enough traction in the near term to demonstrate the potential; how to put infrastructure in place; how to integrate IoT into established infrastructure. We've worked through these questions and think a lot of businesses will be doing the same," says Weir Group's IoT product management director Alasdair Monk. "But it takes significant commitment, a leap of faith. As tends to happen with digital disruption, businesses that don't commit tend to get left behind by the market."

Analysys Mason's McKenzie adds: "It helps that we're starting to see more IoT suppliers raising awareness through trials and proofs of concept, but we still need more simplification and fewer buzzwords. Success will be about a lot more of these suppliers bringing all that's needed together on behalf of industry, both to raise awareness and make deployment much easier."

This would quickly raise confidence, but it needs to come soon to maintain momentum. Security is a particular IoT challenge. "The impact of IoT will, eventually, be massive," says Dan Wolff, IT security expert, formerly of IBM and McAfee. But right now there's a "huge black hole in understanding" quite what a challenge security alone will be, for both consumer and industrial uses of IoT, added to which "there's a dearth of tech available to deal with it".

It's a classic chicken and egg: once the market is there, the products will come. And, without wishing to add to the hype, the market is on its way. Between 2018 and 2028, the number of global IoT connections is expected to grow sevenfold to 5.3 billion, according to Analysys Mason, outpacing the growth rate for smartphones over the same period. Seeing this as a positive would be more assured if, as Appnovation's Dunbar underscores, the IoT industry, such as it is, stopped talking big in terms of value, or of gimmicks, and started focusing on the provision of solutions to problems. But that will come.

"I think it's inevitable there will be a teething process while the new ideas IoT proposes are bedded in," he says. "But once that phase is over, it will be exponential how things will then connect."

127 new IoT devices connect to the web every second
Leftronic 2019

25bn
estimated IoT connections by 2025

$619bn
total revenue opportunity for telecom operators by 2026
Ericsson 2019

Commercial feature

AI helps protect endpoints in the IoT age

The internet of things has multiplied opportunities for cybercriminals to hack companies, but in this increasingly difficult threatscape, artificial intelligence can proactively protect data, assets and individuals

The number of connected devices is exploding as the internet of things (IoT) plays an increasingly influential and transformational role in nearly every walk of life, at home, in the workplace, on the streets and production lines around the world. There will be 75 billion connected devices by 2025, Statista predicts, and this will help drive huge efficiencies for businesses as well as eliminating mistakes from manual processes.

As the number of devices continues to increase, so does the sheer weight of unstructured data within enterprises. Cybercriminals seek to manipulate such data for malicious purposes, intercepting IoT communications, from a sensor to a server, user to user or sensor to user, and altering its flow for their own personal gain. This could mean modifying the data to steal information, changing a value for financial gain or even industrial sabotage and state-funded cyberterrorism.

The wide influence and availability of IoT, and opportunities for malicious actors to intercept communications, poses a major risk to businesses. However, cybercriminals don't always try to attack inside the businesses themselves because that's hard to do. Though many prevention methods within organisations are not as effective as business leaders would like, 95 per cent of companies do nonetheless have a formal security policy in place that is shared with employees, according to an IDG study.

It is therefore far easier for hackers to concentrate on a business user that is working remotely, such as behind a personal firewall at home where the connection and devices are far less secure.

The rise of digital personal assistants, such as Google Home and Amazon Alexa, has exacerbated this threat and widened the attack surface. By targeting these kinds of sensors, hackers have new opportunities for stealing sensitive information. Last year, Security Research Labs claimed malicious apps could be designed to listen in on people's conversations through Amazon's Echo and Google's Nest devices.

"We're seeing a very different kind of threat," says Adam Enterkin, senior vice president of sales, Europe, Middle East and Africa, at BlackBerry. "It's not just the data itself in its rawest form that's under threat, but also voice information, certainly from a remote attack point of view. Anyone has been able to use a microphone for many years, but not had access to it unless it was right in front of them. That's definitely something we see has changed."

With flexible working only set to rise further, enterprises need to ensure they are secure. Yet while companies are surely investing in cyber-prevention, the frequency with which high-profile breaches are exposed in the media is not slowing. The recent attack on foreign exchange giant Travelex is just the latest in a long line of large companies whose customers expected more robust cyber-processes from them. Often, hackers aren't concerned about whether it's a mobile, server or desktop, they're just trying to get in by whatever means they can.

"Some are now even chucking a USB key onto porches for kids to pick up and then put into the home computer or laptop. The hacker then has access to the families' systems," says Enterkin. "On top of that, an awful lot of people will have similar passwords for personal devices and their corporate systems. So, once a home laptop has been infiltrated, hackers can decipher passwords and get into corporate systems that way."

A mentality shift is required among IT security professionals to ensure greater protection in the IoT age. Chief information security officers have spent years implementing policy-driven ways of protecting their assets, data and individuals, but enforcing the same rules and controls on everyone results in very inflexible ways of working.

Traditionally, companies will deploy their IT services, acquire policy-driven devices and security measures, and then see what's happening in their environment. Based on information they see around threats and vulnerabilities, they then retrospectively try to fix the issues that exist.

This reactive approach cannot survive for long in the fast-changing world of IoT. Instead, BlackBerry is advocating beginning with a "left shift", which requires a full review of security measures before deploying anything, rather than the other way around. It involves implementing a secure development life cycle and ensuring software is already at a certain security standard before it is deployed.

Crucially, it also means looking at more adaptive ways of applying security, driven by artificial intelligence (AI) and machine-learning algorithms which learn from all the data and behaviour that is monitored across an enterprise environment. In the IDG study, seven in ten IT professionals said it's only a matter of time before the window of vulnerability has a negative effect on their business continuity.

By feeding AI-driven insights back into their systems, businesses can close the window of vulnerability and constantly evolve their approach to security. The transformative effect AI has on security was the key driver behind BlackBerry's acquisition last year of cybersecurity firm Cylance.

"There's a huge amount of data collated in the IoT. We can analyse that data and start to build mathematical algorithms which we then apply to an AI process," says Enterkin. "Based on this information, we can start to predict what's happening. We can look at every single thing that's happened in malware and viruses over the last 30 years and predict how a virus or a piece of malware in the future will react and respond.

"By using AI and machine-learning models, we also end up in a position where not only are we more secure, but there is fundamentally a better user experience. Based upon set metrics and an analytical view, we can decide whether something is normal or requires action. BlackBerry is championing the user experience and enabling IT to be as frictionless as possible for employees, while providing robust security at the same time.

"There is no other company in the world that's better positioned to protect data through the internet than BlackBerry because we've been doing it for the best part of 40 years. We can provide security at any level, including mobile devices, desktop and IoT. There are 150 million cars around the world today using BlackBerry software to communicate. We are even operating on the International Space Station. So BlackBerry is much more than just a mobile company. We provide security with a seamless touch."

> "There is no other company in the world that's better positioned to protect data through the internet than BlackBerry

For more information please visit blackberry.com

BlackBerry.
Intelligent Security. Everywhere.

Bailey Torres/Unsplash

SECURITY

Peering through the world's webcams

The so-called 'search engine for the internet of things' exposes which connected devices are at risk, and is being used by the good and bad guys alike

Clive Thompson

There's something deeply unsettling about peering into other people's insecure webcams.

It was a January evening and I was hanging on Twitter with Luke Stephens, an ethical hacker, who was sending me links he'd found to webcams open online. The devices didn't have password protection turned on by default and their owners apparently didn't realise this. Like so many internet of things (IoT) devices, the cameras were an insecure mess.

I saw one camera that looked out in the lobby of a building in India and another in a Spanish plaza. Then, most alarmingly, I found one in a house in Germany showing a clear view of what appeared to be a bedroom, with a cabinet half open and a small table with a few bottles of water on it. Nobody was in view. I immediately closed the browser window, feeling like a creepy voyeur.

How had Stephens and I found all these open, insecure webcams? Not through any nefarious hacking. We were using Shodan, the "search engine for the internet of things".

Shodan is a tool that lets anyone search for IoT devices online. If you hunt for a particular piece of hardware – a new voice-controlled thermostat, say – it will provide you with a list of them anywhere in the world. Or if you type in the IP address of your firm or house, Shodan will show you whether you have any public devices online.

Much as Google "crawls" the internet, pinging every webpage to create a massive list of them, Shodan crawls the universe of internet-connected devices. It doesn't actually log on to them; it just records any metadata they publicly broadcast.

You might imagine that Shodan would be a choice tool for black-hat hackers. A search engine, ripe with possibly vulnerable targets.

But in reality, it's mostly used by white-hat security professionals, to help them keep their companies safe. Shodan and other sites that have blossomed in the wake of its success have become a crucial way to figure out whether any of their online devices are accidentally insecure.

"Hackers will find vulnerabilities," as Shodan creator John Matherly says. "What's important is that you respond in a timely manner and fix the bugs." He launched the tool ten years ago and now 80 per cent of his customers are security professionals within Fortune 100 firms.

What types of things do white-hat hackers find on Shodan? A dizzying array of leaky devices. US-based security researcher Nate Warfield has found devices that were vulnerable to ransomware attacks and even Monero mining attacks when botnets hijack a business's devices and use them illicitly to mine cryptocurrencies.

Plus, new vulnerabilities are discovered daily, so whenever Warfield hears of some new leaky, piece of software or hardware, he can quickly use Shodan to check if his clients are exposed. "It's extremely useful when you need to quickly assess the risk," he notes.

Having even one IoT device that's vulnerable can become a critical weak point for a firm. Recently, Tom Lawrence, founder of security firm Lawrence Systems, ran a test to show how this works. Using Shodan, Lawrence found an exposed port on a device at the firm and discovered an employee's name on it. Using the name, Lawrence says: "We found some records on them. We found their LinkedIn." This led to the employee's mobile number, which allowed Lawrence to generate "a phishing attempt through a password reset that you send to a fake link on there". Thus he demonstrated how you could break into a firm through one leaky device.

Many firms use Shodan to set up a monitor, a sort of Google alert, which pings if Shodan finds a vulnerable IoT device suddenly alive on their network. Nathan McNulty, who works in security for a school district in Oregon, recently had one such alert ping when an employee put a server online and, through a single typo, left it exposed. "Fortunately, it had no data on it yet when we found out," says McNulty, "but it could have been very bad."

Other white-hat hackers use Shodan to hunt for so-called bug bounties, checking major companies for vulnerabilities, then alerting the firm in the hope of a reward. Stephens was recently prospecting for bug bounties when he found a company with a device so insecurely configured that it "allowed any hacker to gain full control of that system", he says. "This level of access also would have made it easy to read from a database, which contained personal details of all customers."

Sometimes security professionals, just for curiosity's sake, will go on a Shodan safari, poking around to see what unprotected devices are around. They quickly stumble across alarming stuff. Personal webcams may be the least of the world's problems, but governments worldwide are leaving mission-critical systems lying around utterly exposed, according to Matherly.

> "I saw something that allowed you to change the flow of water through a city. It was wide open

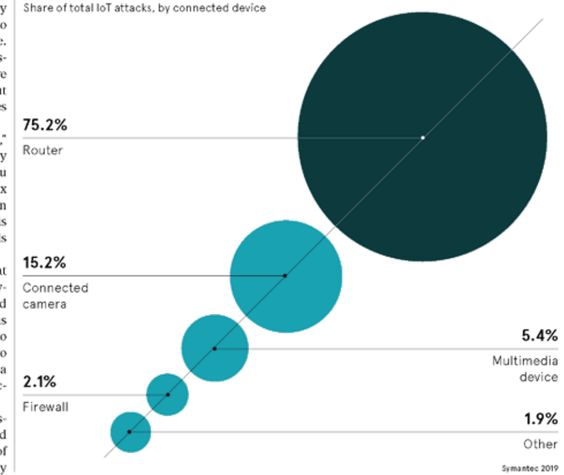
Security expert Daniel Miessler says: "I saw something that allowed you to change the flow of water through a city. It was basically opening and closing the ports that control the dam structure. It was wide open." He's also found exposed "power control systems, water control systems, manufacturing plant controls: the nastiest stuff you can imagine".

Warfield adds: "I could write a novel on the interesting and terrifying things I've found." These include an insecure air-conditioning system for an Asian skyscraper and a remote-controlled fire-suppression water cannon at a port in the South Pacific.

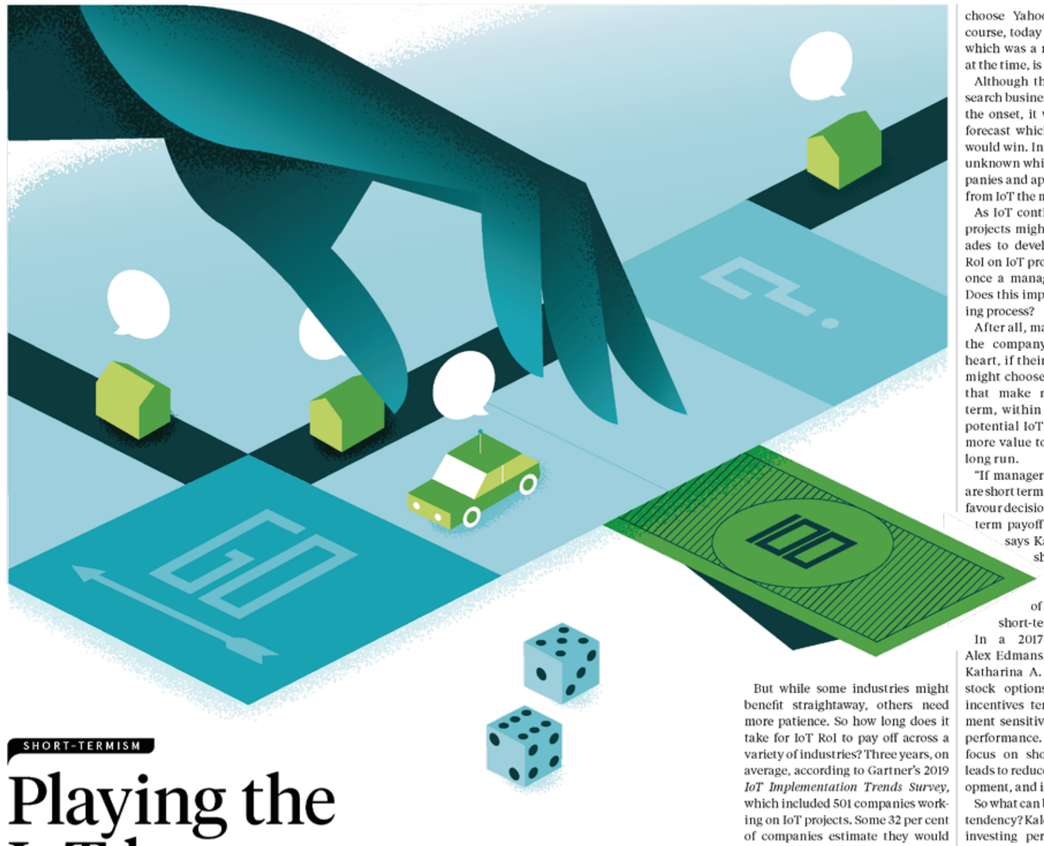
As Matherly concludes: "We live in a crazy world." Most white-hat hackers seem resigned to the fact that firms, and individuals, aren't going to stop putting IoT hardware online. So they offer this important advice: if you buy an IoT gadget, immediately change the password, update the software and put it on a separate network. That way, if it gets hacked, it won't be a stepping stone to your email, financial databases or other personal details.

IoT DEVICES MOST VULNERABLE TO ATTACK

Share of total IoT attacks, by connected device



Symantec 2019



SHORT-TERMISM

Playing the IoT long game

How quickly will managers see a return on investment from the internet of things? And how much is short-termism holding back IoT's potential?

Marina Gerner

The internet of things (IoT) has huge potential. According to one forecast, there will be a trillion connected computers in the world by 2035, built into everything from cars to toasters. Collectively, such IoT devices, which record, monitor and communicate data, herald what some call the "second phase of the internet".

Companies at the forefront of IoT are set to be the winners of the future. But we have yet to see what industries and uses will benefit the most. In many cases, IoT projects might take years, and even decades, to come to fruition. At the same time, the decisions of executive managers are increasingly shaped by short-term concerns.

Given that IoT projects involve significant funding, a meaningful return on investment (RoI) is crucial. So how long should it take for companies to see an IoT RoI? Does this vary across industries? And how can we ensure the long-term thinking needed for IoT projects is not hampered by managers' egos and short-termism?

IoT projects can take many forms from optimising the performance of equipment on the factory floor, to utilising workspaces more efficiently and improving patient health through wearable technology. "I've observed a few cases of successful IoT application to improve production processes," says Vitali Kalesnik, director of research for Europe at Research Affiliates. Multiple sensors are placed around the production line to provide engineers with real-time information, collect data and then apply machine-learning algorithms to improve production.

> **If managers' evaluation and pay are short term in nature, they tend to favour short-term payoff**

"What is interesting about IoT is how quickly you can see RoI," says Jon Forster, manager of the investment trust Impax Environmental Markets. "For instance, industrial companies often adopt software to make their operations more efficient and, indeed, tend to see RoI pretty much from day one; reduced labour costs, the benefits of predictive maintenance, for example."

But while some industries might benefit straightaway, others need more patience. So how long does it take for IoT RoI to pay off across a variety of industries? Three years, on average, according to Gartner's 2019 *IoT Implementation Trends Survey*, which included 501 companies working on IoT projects. Some 32 per cent of companies estimate they would achieve financial payback for their IoT projects in one to two years, with 10 per cent estimating this would take less than a year. Only 8 per cent estimate they would have to wait for more than five years.

At the same time, we have yet to see the full potential of IoT. Kalesnik compares the evolution of IoT to the introduction of Internet companies in the nineties. "If we were to invest in search businesses back in the late-nineties, we would probably choose Yahoo! and AltaVista. Of course, today we know that Google, which was a really geeky company at the time, is the winner," he says.

Although the potential of online search businesses was obvious from the onset, it was really difficult to forecast which particular business would win. In the same vein, it's yet unknown which technologies, companies and applications will benefit from IoT the most.

As IoT continues to evolve, some projects might take years and decades to develop. What happens if RoI on IoT projects is only expected once a manager has left the role? Does this impact the decision-making process?

After all, managers may not have the company's best interests at heart, if their egos interfere. They might choose to invest in projects that make money in the short term, within their tenure, even if potential IoT projects could bring more value to the company in the long run.

"If managers' evaluation and pay are short term in nature, they tend to favour decisions which favour short-term payoff over the long term," says Kalesnik. Research has shown that executives tend to sacrifice the long-term value of companies to meet short-term earnings targets.

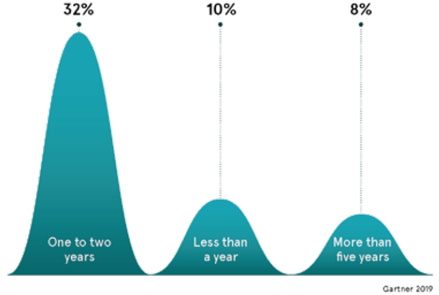
In a 2017 study, researchers Alex Edmans, Vivian W. Fang and Katharina A. Lewellen found that stock options used as executive incentives tend to make management sensitive to short-term stock performance. They found such focus on short-term performance leads to reduced research and development, and investment.

So what can be done to counter this tendency? Kalesnik suggests a longer investing period for management stocks of about three to five years to ensure managers have incentives to look after the long-term value of the company. What's more, he points out that startups, where managers' profits tend to be tied up with the equity they own for a long time, naturally align with the long-term thinking needed for IoT projects.

For companies to succeed with IoT, the right managerial incentives are key. After all, the second phase of the internet promises to be a long game.

HOW LONG WILL IT TAKE TO ACHIEVE FINANCIAL PAYBACK FROM IoT PROJECTS?

Survey of companies working on IoT projects



Gartner 2019

Commercial feature

IoT is gamechanger in net-zero emissions

If renewable energy and green technology are saviours in the drive towards net-zero emissions by 2050, the great enablers are those bringing the internet of things to life

Smart connectivity is now enabling some of the UK's most intensive energy users to monitor what they use, drastically improve energy efficiency and slash consumption at a time when all eyes are on carbon neutrality.

"Winning businesses will be increasingly defined by their ability to reduce their carbon footprint. Advances in cloud and edge-based technology are a real gamechanger because they transform energy-consuming assets into intelligent, automated devices that can boost efficiency," explains Jordan Appleson, chief executive of Hark, a producer of real-time, cloud-based monitoring and control systems.

Digital technologies under the internet of things (IoT) umbrella are predicted to reduce global emissions by up to 15 per cent in the next decade. This will be critical in tackling climate change and meeting the Paris Climate Accord goals. Retail food outlets alone are responsible for 3 per cent of all electricity consumed in the UK and 1 per cent of greenhouse gas emissions.

Yet the UK government has said its energy targets for commercial buildings will not be met, the market isn't delivering change fast enough and a step-change is needed.

Refrigeration and lighting are just two of the high costs retailers can control through industrial IoT

"Deploying IoT at scale, nationwide, could help. It's one thing to monitor and adjust a single refrigerator or a bank of lights, it's another to do this across an entire chain of supermarkets or offices, at thousands of locations. Then you realise what adding intelligent controls achieves. The efficiency gains are impressive, making a real difference to the bottom line," says Appleson, whose Hark Platform is used by the biggest names in retail.

"Existing sensors in old assets can be connected and overlaid with data from new machinery, creating a unified data feed. Machine-learning algorithms help make predictions on energy use, detecting anomalies, say a refrigerator using more energy than it should, or a high-energy asset that could be automatically turned off when not in use. It's about knowing where the high-value, low-hanging fruit is when it comes to efficiency gains."

Connected IoT devices feed information from the edge to the cloud in real time and the challenge is knowing how to analyse the sheer volume of data intelligently. Standardisation is difficult as there's no cookie-cutter model and no two companies are the same. This is where case studies and experience are crucial, as is understanding the end-to-end picture of energy use.

"You have to be agile, start off in one location, with a couple of problems, and scale up. Forward-thinking companies get it. It's a journey with our clients. When it becomes a shared challenge for everyone, we achieve great things," says Appleson, whose award-winning, plug-and-play Hark Platform is deployed by life science and manufacturing companies, logistic firms and smart building operators.

"Changing human behaviour is the biggest issue. You need to articulate energy efficiency in peoples' everyday lives. By using push notifications to politely nudge people, we can notify facilities' managers by text to switch off devices, manage energy use or operate machines efficiently, with feedback from connected devices."

IoT is driving more automation, especially with building heating and cooling systems, which are huge energy consumers. If the system knows how many people are in there in real time, then this can be used to automatically turn off the system when everyone's left, conserving power. This is useful during peak times when energy costs are highest.

"We need to get a lot smarter about how we use energy. IoT has so much to offer. We can also predict when a machine is likely to break down, pre-empting maintenance. Algorithms now automatically analyse use patterns, sending real-time alerts if something changes. We then prioritise callouts for engineers; this has an indirect effect on fuel consumption for the person sent to fix the asset. Every little counts," Appleson concludes.

IoT RESULTS FROM ONE OF THE TOP FOUR UK SUPERMARKETS

24,000
assets monitored

100,000
sensors connected

200m+
daily readings

600+
store rollout

£1m+
saved in 12 months

For more information please visit www.harksys.com

Hark

CLIMATE CHANGE

A silver bullet for climate change?

The internet of things promises greater efficiency across a range of industries, but the technology could have adverse effects if managed incorrectly

Alexandra Leonards

Teetering on the precipice, countries across the world are desperately seeking a resolution for the ongoing and hastening threat of climate change. But with technologies such as the industrial internet of things (IIoT) already reducing carbon emissions and boosting energy efficiency across industries, the bigger picture could start to look a little more promising.

IIoT measures the impact of industrial processes and human activity through sensors that can monitor a whole range of factors, including everything from air and water quality, to assessing pollution levels around factories, rivers and cities. The technology can also identify the more indirect impacts of climate change by measuring things such as flood and river levels, wind speed, land erosion, the activities of bees and beehives, and tracking animals or vegetation in impacted areas.

"The internet of things is the digital skin of our planet," says Alex Gluhak, head of technology (IoT) at Digital Catapult. "By measuring the real state of the world through sensors, we become aware of existing issues and can track them over time as we use specific interventions to combat these issues."

IIoT can also have a significant impact on reducing the carbon footprint of processes. It does so by minimising the use of natural resources, including raw materials, electricity, fossil fuels and water. Alongside this, the technology can reduce production waste and plays a key role in the tracking of material flow in the emerging circular economy.

Susanne Baker, associate director climate, environment and sustainability, at techUK, says: "IoT is increasingly recognised as an essential element in our transition to a net-zero economy."

> **IoT is increasingly recognised as an essential element in our transition to a net-zero economy**

When combined with other digital applications, such as 5G and artificial intelligence (AI), IoT could help cut carbon by 15 per cent, according to the World Economic Forum.

"IoT can help make sense of the raw data produced every minute by the thousands of connected devices that make up business operations, supply chain and connected products," says Andy Stanford-Clark, chief technology officer at IBM, UK and Ireland. "IoT technology, especially when paired with AI, can improve resource efficiency, reduce pollution, and stimulate new thinking and innovation."

In farming, precision agriculture is used to minimise the use of water, fertiliser and pesticides. The technology monitors soil minerals, temperature and moisture. This helps improve and increase yields, and minimises the use of both resources and land. IoT sensors in the soil and environment, alongside the use of algorithms, or "grow recipes", can improve the management of farm resources.

IIoT could also help reduce the harmful impact of greenhouse gases produced by livestock. "There's potential for reduced methane from ruminants through livestock health monitoring, for example monitoring dietary health and temperature of animals to identify and treat animals, which helps to reduce greenhouse emissions," explains Dr Nilufer Tuptuk of the Department of Computer Science, University College London.

In the manufacturing industry, sensors are used to order products autonomically, thus optimising production. IIoT is also being used to monitor the energy consumption of manufacturing equipment, enabling operators to identify inefficient equipment. Further precise monitoring of external factors can reduce errors, resulting in less waste and more efficient use of materials.

"Logistics companies can shorten delivery routes through intelligent route planning, tracking can shorten delivery times through new insights into the supply chain, products can be located, fewer products are lost, which ultimately has a positive effect on the climate by reducing total direct and indirect energy consumption," says Pascal Vögeli of the ZHAW Zurich University of Applied Sciences, Switzerland.

In the energy and utilities market, smart street lighting is being used to reduce consumption, and leakage sensors in water and gas pipes are used to detect and repair losses caused by leaks.

Extension of the lifetime of goods can also be attributed to the introduction of IoT solutions. Predictive maintenance of goods, including cars, electrical goods and construction equipment can enable longer utilisation cycles. This means fewer breakdowns and replacements, and ultimately a reduction of waste.

On the surface, IIoT appears to generate only benefits. But the technology itself can contribute to product waste. That's because millions or even billions of sensors, and their batteries, will need to be disposed of once their lifespans end.

"There's the consideration that building IoT components themselves requires resources that might have an adverse effect on the planet," says Digital Catapult's Gluhak. "There is already a lot of research on energy harvesting for IoT devices to get rid of batteries completely or replace them with biodegradable materials."

Gluhak believes that it's only a matter of time before enough breakthroughs are made to minimise these potentially harmful environmental impacts.

However, there is also an argument to say that more efficiency, stimulated by emerging technologies like IIoT, can result in more production and therefore more consumption.

"Any technology that supports efficiency and productivity improvements could in turn potentially drive higher levels of production and consumption," says techUK's Baker. "It is important therefore that these risks are properly understood in the context of our national and sector planning to move to a post-fossil-fuel society."

The ability to cut waste, make better use of resources and reduce carbon emissions makes the deployment of IoT across industries a largely positive step towards combating climate change. But alone, the technology is certainly no silver bullet. It must be aligned with the right policies and actions to maximise its potential and be managed closely to ensure its benefits are not offset by lurking environmental flaws.

84%

of existing IoT deployments can address the UN's Sustainable Development Goals

25%

of these focus on industry, innovation and infrastructure

19%

of these focus on affordable and clean energy

World Economic Forum 2018

Creating smart-city infrastructure and a connected world

How Trilliant's end-to-end platform technology is connecting the world of things

Ever since the phrase "fourth industrial revolution" was coined by Klaus Schwab, founder of the World Economic Forum, in 2015, much has been written about the industrial internet of things (IIoT), a system which uses big data and machine-learning to connect cities, machines and people.

A cursory glance at the internet, for example, reveals a myriad of benefits for the industrial sector including increased safety, compliance, flexibility and agility.

But what a quick internet search doesn't reveal, says Peter Asman, an IIoT and communications expert working for Trilliant, is just how many IIoT projects fail.

"You can't just deploy an IIoT programme without having a systematic and scalable architecture to aid you in achieving an end-goal," he explains. "Nor is it possible to utilise the IIoT without also utilising a multi-layered, end-to-end platform, which enables the secure and frictionless exchange of data. This is the secret to connecting the world of things and this is what Trilliant does, and does well."

In fact, Trilliant is unique in this respect. With a presence in 20 countries, it provides more than 75 of the world's largest companies with one of the most advanced hybrid wireless communications platform on the globe.

In the UK alone, several large organisations have benefited from Trilliant's data-driven networking solutions.

In May 2009, for example, a large UK energy and home services provider enlisted Trilliant's help to lay the digital foundations that have enabled the company to better link millions of datapoints from disparate assets such as smart meters, gas meters and smart thermostats.

Asman, who is Trilliant's vice president of IIoT and smart cities for Europe, Middle East and Africa, says: "When the organisation approached us, it had no way of gathering and harmonising that data. Over the course of many months, we worked in concert with the company to build a secure and robust platform, which today connects over six million smart meters that communicate with their datacentre in real time.

"The benefits for company and customer are that the organisation can monitor the amount of gas being used nationally, while consumers are guaranteed accurate billing."

But it's not just large energy companies that are profiting from Trilliant's leading-edge technology. Trilliant's hybrid wireless solutions technology is also helping data-driven water companies to unlock their potential.

In South Africa, for instance, where drought almost left Cape Town's four million people without access to water, Trilliant is using its technology to help cities in the region to understand how to reduce water leakages, while also ensuring the quality of drinking water remains high.

Although Asman is unable to disclose the client's name, he says Trilliant is working with a water provider to detect leakages in real time. "This is achieved through the use of a series of sensors, which enable greater efficiency and control of an already limited water supply," he explains.

But this transformation also relies on digital harmonisation, something which Trilliant excels in. Working in tandem with some of the world's top sensor providers allows the Trilliant IIoT Platform to surface data from many different types of sensors and collect it all in a "single pane-of-glass view". For water providers like those in South Africa, this single view into their entire system provides them with the ability to take swift and accurate action when needed.

Asman explains that this high level of digital integration provides water companies with the ability to manage leakages, as well as pressure flows, proactively. He notes that it also helps them to manage change quickly, adding that the ability to connect a multitude of different sensors to the network is an absolute prerequisite.

So how does the so-called single pane of glass translate into efficiency savings? With acoustic sensors fitted across pipe infrastructure, Trilliant's data platforms can integrate all the information in real time, enabling the water management company to identify a leak within a range of 20 metres.

"The sensors can also monitor water pressure and flow, and check the levels of chlorine are always safe. What's most important though is that the platform is able to adapt to the ever-changing needs of the customer, whatever the use-case and wherever they may be," says Asman.

And it's this flexibility that he says "gives Trilliant's technology platforms a vital edge" over its rivals.

Asman, who joined Trilliant from Spanish multinational communications giant Telefonica, points to the fact that Trilliant's data networks utilise both 2.4GHz and 5.8GHz to serve every international region.

Of course, it wouldn't be impossible to build this variable system bandwidth into its network, without industry-leading standards and world-class security credentials.

Take agility, for instance. All of Trilliant's hybrid wireless communications conform to the latest industry standards. But why does this matter? Asman explains: "With developers bringing out new sensors every day, Trilliant's platforms are designed to be as flexible as they are robust. For example, when a company chooses to partner with us, it's our job to create an interoperable platform infrastructure where sensors, no matter how new to the market they are, can communicate effectively and powerfully with each other through a single pane of glass."

But accessibility means nothing without leading-edge security. With Trilliant providing mission-critical communications to a host of large organisations, utility-grade security standards are an absolute necessity.

"Keeping our customer's data safe lies at the heart of everything we do. All Trilliant's software utilises the Federal Information Processing Standard, which provides a secure bedrock on which our technologies are deployed and maintained," says Asman.

Indeed, with more than 500 million end-users benefiting from its platform, Trilliant is using its vast knowledge and experience to build the smart cities of the future. It is currently working with partners in the United States, Europe and Asia to connect people and cities to the world of things.

But it's perhaps Trilliant's dedication to their customers that is most eye catching. By working in collaboration with cities, utilities, energy companies and even universities, Trilliant is seeking to create not just a smart city infrastructure, but an entirely connected world.

"Our projects are ambitious and are often trailblazing in their scope and possibilities. Our infrastructure provides a living, breathing template for the connected world of the future," Asman concludes.

That Trilliant, a company made up of just one person in 2008, is playing an instrumental role in shaping the world's future is as empowering as it is remarkable.

> **Our infrastructure provides a living, breathing template for the connected world of the future**

53%

of Trilliant's customers use the platform for multiple applications

34%

of Trilliant's customers use multiple Trilliant technologies

500m

the number of end-users under reach of the Trilliant platform

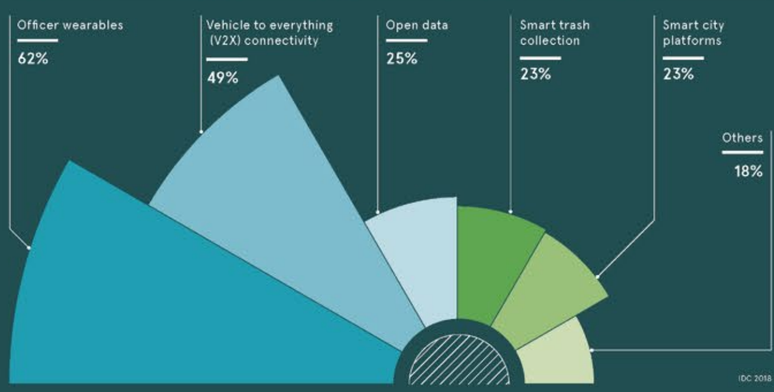
Learn how Trilliant can help connect your world of things by visiting trilliant.com/thetimes

Trilliant

SMART CONNECTIONS

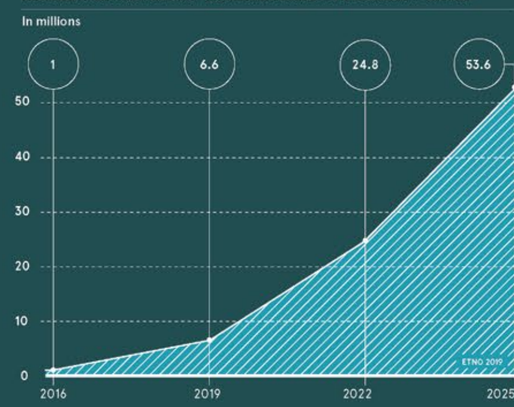
However important the internet of things will be for business, its impact is transformative when it comes to our cities. Around the world, IoT-enabled smart cities are changing the way we live, using technology to increase the speed and efficiency of urban services. The results are wide-ranging, from greater safety on our streets to valuable time shaved off our daily commutes, as well as cleaner air and water, and, in some regions, more disease-free years of life

GLOBAL GROWTH RATES FOR SMART CITY SPENDING FROM 2017-2022, BY USE CASE



IDC 2018

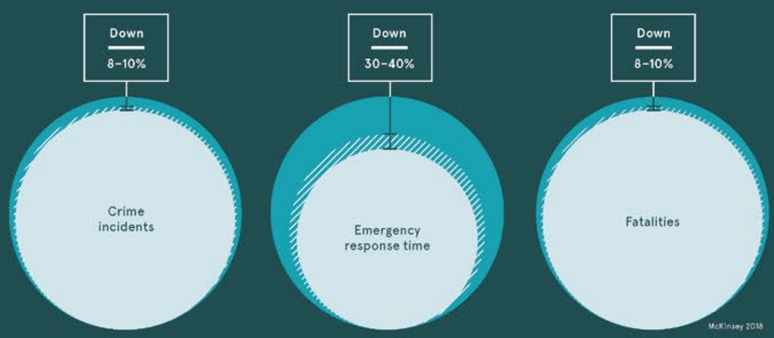
NUMBER OF ACTIVE IoT CONNECTIONS IN EU SMART CITIES



01 EMERGENCY SERVICES/SAFETY

Predictive policing, real-time crime mapping and gunshot detection - these IoT-enabled processes could save up to 300 lives a year in cities such as Rio de Janeiro.

ESTIMATED IoT-RELATED BENEFITS TO PUBLIC SAFETY/CRIME LEVELS



McKinsey 2018

10–15% improvement on emergency service arrival time

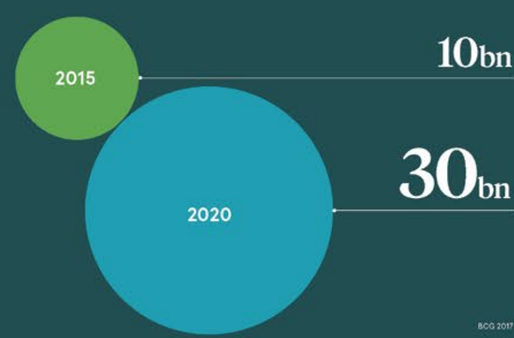
10% decrease in street crimes with IoT monitoring of public safety

PwC 2018

02 TRANSPORT

New smart roads and technologies can shave up to 30 minutes of the daily commute

GLOBAL IoT TRANSPORTATION AND LOGISTICS SPENDING



BCG 2017

10% increase in road traffic capacity with smart parking

30% decrease in passenger waiting time with connected public transport

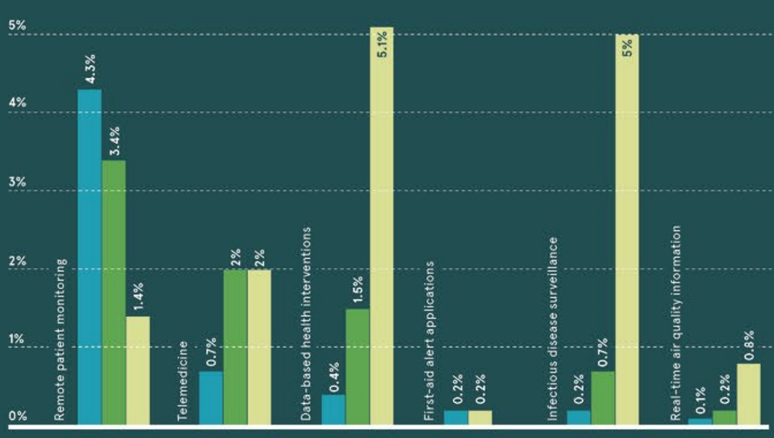
PwC 2018

03 HEALTH

Using a range of technological applications, smart cities can cut emissions, reduce waste and save up to 80 litres of water per person per day

IoT TECHNOLOGY IMPROVING URBAN QUALITY OF LIFE

Percentage reduction of disability-adjusted life years, the WHO's primary metric for conveying the global burden of disease, by different cities



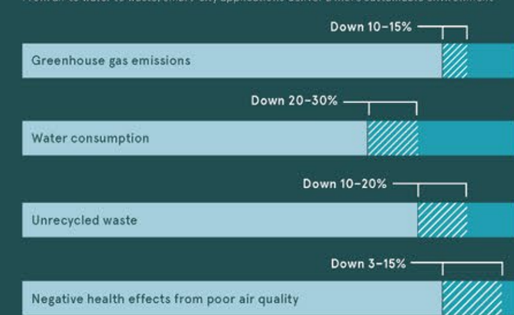
McKinsey 2018

04 ENVIRONMENT

Smart cities can help tackle chronic diseases, using data to fight preventable disease and improve patient engagement

CLEANING UP OUR ACT

From air to water to waste, smart-city applications deliver a more sustainable environment



30% reduction in street lighting costs by using smart lights

20% reduction of waste collection costs with smart waste systems

PwC 2018

INNOVATION

Innovations that will change your life

Interested in never buying vegetables, missing deliveries or losing your keys again? These five internet of things innovations from this year's Las Vegas Consumer Electronics Show, CES 2020, could help

Mark Frary


Plenty Cube

1 Modular farm for the smart city

Planty Cube was one of the top internet of things (IoT) solutions on view at CES 2020, winning an innovation award in the smart cities category.

Conceived by South Korea's n.thing, Planty Cube is a 40ft container that has been reimagined as a modular vegetable farm. IoT devices in the container monitor environmental factors such as temperature and humidity, and control feeding and watering.

Vertical farms, where crops are grown in layers, are an increasingly popular way to feed urban populations. Planty Cube's modular approach means such farms can easily scale as demand grows for their produce. The company says the technique can increase yield up to ten times and grown locally can help reduce carbon emissions.

Crops grown in Planty Cube have the advantage of being free from harmful substances as they are cultivated in a non-agrochemical environment and can be eaten without washing.

2 Home security for the sharing economy

Another top IoT innovation revealed at CES taps into the unstoppable rise of the sharing economy and short-term rentals in particular. Igloohome announced the Smart Mortise 2+ lock which works with a mobile app to generate unique PIN codes to let people access properties in real time without a physical key.

The technology used means smart home owners can create time-sensitive PIN codes with start and end times to ensure their property is secured after each renter departs.

Users can also unlock the Smart Mortise 2+ with a high-security fingerprint ID using a concealed biometric sensor, Bluetooth keys and RFID (radio-frequency identification) devices.

Owners can access activity logs which show dates and times of visitor access. Smart Mortise 2+ also features keypad security lockout, a panic exit system, child and pet safety function, fire and tamper alarms, and auto-relock.


Igloohome

3 Intelligent gardens for smart homes

Agricultural IoT innovation that turned heads at CES included the Agrove, a personal smart garden for growing your own produce.

The Agrove has sensors which detect the microclimate specific to each urban environment and proposes plant varieties to grow. An app then gives advice on how to plant and maintain the plants. Watering is fully automated and the application predicts the doses of water to be released according to the humidity level and needs of the plant.

Agrove founder Quentin Rousselot, a farmer's son, came up with the idea after moving to the city and being surprised by the difficulty of finding tasty fruit and vegetables at a reasonable price.

He says: "To simplify maintenance as much as possible, I had the idea of putting technology at the service of my vegetable garden by integrating all the knowledge of experts in a mobile application and creating a vertical, modular and intelligent planter."

Agrove


Innowave

4 Track your stuff anywhere

Over the course of our lives, we lose an average of 200,000 things, according to technology company Innowave. Their answer, unveiled at CES, is the LEAP, a tiny, multi-sensor wearable device that uses a range of different tracking technologies to make sure you don't misplace stuff ever again.

The LEAP is 42mm in diameter, 11.5mm thick, weighs 22gm and is water resistant. It can be tracked through 5G mobile networks, but also using direct communication with the Globalstar satellite network, so belongings can be tracked even in the most remote locations. It has very low power requirements and can last for months on a single charge.

The device can be used to see the last time an object moved and whether it has gone into or out of a specified area known as a geofence. Suggested use-cases include tracking vehicles, expensive equipment, children and pets.

5 No more missed packages

Online shopping continues to increase and with it the number of "while you were out" cards. Go Nok Nok, showcased at CES, aims to cut down on the number of missed deliveries and reduce the problem of stolen packages. A recent C+R Research study showed that more than one in three US online shoppers have had packages stolen from their doorsteps.

Go Nok Nok is like a sophisticated cat flap with an integrated video camera and two-way speaker. When a courier presses your doorbell, you are notified in real time on your smartphone or Alexa device, allowing you to unlock the flap remotely.

The software also has an integrated label scanner. The courier shows the label to the camera and, if the app recognises the package is for you, it will unlock the flap automatically.

Company founder Rez Gachcar says the Go Nok Nok is also useful for vulnerable and elderly people who do not wish to open their front doors.

Commercial feature

IT and OT come together to drive digital transformation

Data is the lifeblood of the internet of things and connecting tissue of the manufacturing industry, but creating truly scalable value means seamlessly bridging OT and IT at all levels

Since the rise of computing in the 1960s and '70s, advancements in IT have been paralleled by developments in operational technology (OT). Yet, while manufacturing kept at the forefront of automation on the factory floor, it fell behind other sectors in digitising paper-based processes at the plant level. Companies may have deployed numerous systems – enterprise resource planning (ERP) and the like – to drive improvements, but many struggled to leverage the data collected in their manufacturing plants because it was such a large human undertaking.

Emergence of the internet of things (IoT) in the last decade, however, has accelerated their digital transformation journeys. New solutions incorporating advanced analytics have enabled manufacturers to identify and anticipate the failure of a machine based on data insights generated through the use of low-cost sensors and analytic programs that can interpret factors such as vibration, temperature or throughput. By being able to predict quality with IoT, and also to prescribe what to do through insights driven by artificial intelligence, the potential is there for manufacturing organisations to transform from a position of making improvements based on past learnings to being able to prepare proactively in the best way.

Despite the huge potential of IoT, many of the schemes thus far have been limited to pilot projects whereby manufacturers pick a certain problem area and concentrate on the technology required to solve specific issues. Typically that means putting sensors in and getting some IoT gateways. They'll collect data, combine information from their ERP system and optimise processes to drive improvements. While this provides value to that individual use-case, the real challenge for a multinational company is standardising and spreading improvements across all sites.

"What is often lacking is the capability to capture the knowledge you've gained from that pilot in one individual plant and then extend it across multiple plants," says Steve Garbrecht, technical product marketing director for IoT at Hitachi Vantara. "You want to take the best practices from one site and reinstitute them in another. There's this need for scalability, but the experience and resources out there to do it are lacking. There are people who know OT technology, but they lack knowledge in how to institute some of the more advanced IT architectures to really take IT to the shop-floor environment."

Hitachi Vantara is seeking to bridge the gap between IT and OT, bringing to manufacturing the production process benefits that Toyota, another Japanese giant, brought to the automotive industry. Hitachi is in the unique position of having vast experience in both OT, from 110 years as a manufacturer in its own right, and IT, when for 60 years it has developed data management architecture, products and solutions. The company creates systems for use within its own plants, but also the manufacturing plants of its customers.

Earlier this year, Hitachi Omika Works, which manufactures automation control systems for industrial operations, was inducted into the World Economic Forum's Global Lighthouse Network of advanced factories leading the way in applying Industry 4.0 technologies to drive efficiencies and operational impact. The Omika Works factory showcases Hitachi's Lumada solutions, combining OT and IT technologies, and has reduced the lead time of core products by 50 per cent without impacting quality.

"We're bringing OT and IT together, and it's a really powerful combination," says Garbrecht. "What the Japanese and Hitachi have found is that by being able to improve the processes, which include the people, materials, production processes and the approach from a manufacturing point of view, you can gain competitive step-changes within the marketplace. By making improvements overall within not just Hitachi but the industry and society as a whole, we can make things better for everybody. A rising tide raises all ships."

Factories generate an enormous volume of captured production data which could be used to drive transformation, but 70 per cent of it goes unused today, according to the World Economic Forum. Until manufacturers adopt new practices to manage and derive insights from the data, and apply those insights to business outcomes, its potential will remain untapped.

Approaching data management and data analysis in a consistent way is imperative. Being able to compare results and operations from site to site requires data management at both the edge and the site factory-floor level, and all the way up the enterprise. There are two different groups using the data. On one side are the on-site operations and engineering teams that require visibility and a quick analysis capability of the data. On the other are data scientists, data engineers and IT people doing more advanced analytics and designing machine-learning models.

Between these two groups, manufacturers need a way to manage the data so it can be shared in a timely and correct way, or sometimes not shared at all if regulatory or security policies dictate so, or if it's not worth the costs of transmitting and storing it in enterprise or public-cloud platforms. Manufacturers, therefore, need to be more curated at the local level to ensure data is cleansed, corrected and in a suitable format before it reaches the enterprise.

Traditionally, manufacturers look at four possible root causes of poor quality or performance on shop floors – man, machine, material and methods – and attempt to isolate problems to increase efficiency and productivity through continuous improvement. In the IoT age, they have the chance to digitise *kaizen*, the Japanese word for improvement, and adopt advanced technologies to generate insights that identify where particular defects in quality can be traced.

"Industry 4.0 is about bold changes that enable not just continuous improvements but real transformation," says Sath Rao, director of digital solutions for manufacturing, industry solutions marketing, at Hitachi Vantara. "Leveraging a system of insights can drive transformative outcomes. Historically there's been this monolithic legacy system of records and then islands of automation on the shop floor. What was missing is the focus on return on data. The fourth industrial revolution is all about the focus on cyber-physical systems that can drive business agility. Establishing the digital innovation foundation is core to accelerating the digital transformation journey."

> We're bringing OT and IT together, and it's a really powerful combination

For more information please visit hitachivantara.com

HITACHI
Inspire the Next

SKILLS GAP

Cultivating the internet of talent

Fear of losing your job to a robot is nothing new, but is it time the conversation shifted?

Nick Easen

For as long as there have been robots, there have been fears they will take people's jobs. The rise of the internet of things (IoT) echoes these concerns. An engineer no longer has to monitor a machine or switch on a bank of lights, IoT sensors can do it instead. Smart devices may not be an answer to the global talent shortage, but they're starting to impact the work employees do.

The likes of heating, lighting and maintenance are already being automated, reducing routine tasks and eliminating others, in offices and factories around the globe. Demand for IoT is changing the role of facilities managers in a way that mirrors how self-service checkouts disrupted customer services in supermarkets or automatic doors and monitoring systems have affected guards and train drivers.

"The increased deployment of data-driven technologies is raising social, legal and ethical questions about the impact on people and their everyday lives. It's vital that we find ways to engage with employees and the public, as well as identify the issues so they can be addressed," says Julian David, chief executive of techUK.

Thought leaders are keen to highlight the strong demand for IoT isn't going to lead to mass redundancies or answer post-Brexit talent shortages, an ageing demographic or lead to less work for humans. Instead the focus is on IoT helping people do jobs better, with more productive and added-value tasks, empowered by data, redefining employment in the process.

"It's about giving people more time to use their expertise where it is more critically needed. With predictive maintenance, teams work in new, more impactful and proactive ways rather than reactively dealing with disruptions, which means this also minimises employee stress," says Belen Moscoso del Prado, group chief digital and innovation officer at Sodexo.

Ironically there is less worry about job losses with the rise of IoT and more concern over talent shortages, as well as how to fill new roles created by its increasing deployment. IoT networks need new levels of expertise focused on data analytics and data science, but knowledge is thin on the ground.

"IoT requires a set of information and operational technology skills that are often hard to find in combination. Businesses face a skills shortage, particularly in digital engineering capabilities, and are hindered by a fragmented skills system and a lack of systematic engagement between education and industry," says Pat Nash, managing director of InVMA.

Innovation in IoT has focused on areas where machine-learning easily beats humans, these are the tasks that are first to digitalise, and in the process retraining and filling the skills gap becomes crucial.

"There will be a reshuffling of the tasks that we typically do and ones we will do differently because we interact with machines," explains Ernst Ekkehard, chief macroeconomist at the International Labour Organization. "The risk we currently face is that many jobs across different sectors are changing quickly and simultaneously; anticipating such changes is not an easy task."

Ndoolindela/Shutterstock

> It's about giving people more time to use their expertise where it is more critically needed

This is also because organisations are now deploying a "smart ecosystem" approach. The key to success is not confining demand for IoT to one part of the business, but doing it at scale and selectively where it makes the most difference; this also has implications for the workforce.

"IoT is not a fire extinguisher and should not be applied to solve everything, but used to enhance, add value and improve the workplace. It should ultimately bring more benefits to workers, not eliminate them," says Johan Carstens, private sector chief technology officer at Fujitsu.

Those deploying IoT solutions talk of empowering employees, not disempowering them, allowing workers to do more, not less, upskill not deskill. On the employee side, absorbing all this change in the workplace is a big issue. "It will become increasingly challenging to stay relevant," says Thomas Frey, futurist and executive director of the DaVinci Institute.

When it comes to talent shortages, the good news is IoT plays to the strengths of a new cohort entering the workforce, Generation Z and beyond. "They grew up alongside technology and expect it in their work. From Minecraft to Instagram, they know how to use data in ever-more creative ways to add value," says Jonathan Bridges, chief innovation officer at Exponential-e.

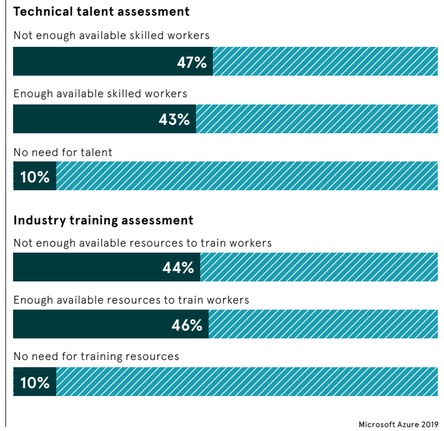
Such creativity could in turn be used to focus IoT sensors on employee activity, defining a worker's every move and how they operate. Companies are now increasingly using IoT to gather data about workforce movements, often anonymised in this post-General Data Protection Regulation world. For instance, facilities managers are sent text messages if they don't turn off lights or machines.

"Some monitoring has serious 'big brother' associations, invading privacy and creating stressful working environments. Given the importance of data to machine-learning, there's intense scrutiny of the legal basis for the control of data and whether the law should change," says Matt Hervey, head of artificial intelligence at Gowling WLG. "The law does not cater well for the ownership of most data. Employees do not own data collected about them, but have rights affecting the data."

Certainly, without proper communication, scrutiny and education on the benefits of IoT, mistrust could grow. "There could be a backlash, especially if there are unions involved. It's really important to bring everyone along with this journey," Mike Jeffs, chief commercial officer at Hark, concludes. Maybe it's time to start having that conversation right now.

LACK OF TALENT AND TRAINING PRESENTS CHALLENGES FOR ALMOST HALF OF IOT ADOPTERS

Percentage of IoT adopters who selected the following challenges



Microsoft Azure 2019

Commercial feature

Protecting IoT in the age of remote working

With consumers and businesses adopting smart devices at a scorching pace, the need for security is a pressing concern for organisations, particularly with more and more remote workers accessing corporate networks from homes increasingly connected to the internet of things

The internet of things (IoT) is transforming the way we work and live. The ability to connect nearly any object to the internet, including lightbulbs, radiators, cars and refrigerators, means consumers and businesses are able to carry out all manner of tasks in a smarter way. As a result, IoT devices are being adopted on a huge scale around the world.

According to Cisco, 500 billion devices are expected to be connected to the internet by 2030. More often than not, however, this myriad of smart devices is completely unprotected, as consumers ignore the patches and updates they previously took notice of for their laptops and PCs, or the IoT device manufacturers just fail to issue them at all.

Four in ten digital households worldwide have at least one vulnerable device, according to the *Avast Smart Home Report 2019*. Apart from routers and network devices, media boxes, security cameras and printers are the most vulnerable and these are often the point of entry for hacks, from DDoS (distributed denial-of-service) attacks to data breaches, spying and blackmailing.

"Endpoint security on the IoT is pretty non-existent at the moment as nobody really thinks they need to install security measures for their smart devices, be it at home or in the office," says David Ryder, director of SMB (small and medium-sized business) and MSSP (managed security service provider) at security firm Avast.

"For the vast majority of IoT manufacturers, their main concern is selling products, designing them to work easily and making them addictive. Little thought is put into securing them or even recommending any security. They're worried about having the conversation about security risks because they believe it might deter people from buying their products."

With flexible working now widely adopted by organisations of all sizes, the security risks in people's increasingly connected homes is suddenly a very major consideration for the companies they work for. Their seemingly innocuous unsecured smart doorbell or lights could be a weak link and give cybercriminals access to the company network.

In one of the more high-profile cases, hackers infected millions of home IoT devices with malware to attack DNS (domain name system) provider Dyn and bring down sites such as Twitter and Spotify which rely on its services. These kinds of DDoS attacks now happen frequently and anybody who isn't actively securing their IoT devices is obliviously participating.

The grey area between office security and home security, and lack of understanding on how to tackle the problem, is creating significant challenges for organisations. Remote workers often resent BYOD (bring your own device) policies and try to find a way to work around them. It's crucial, therefore, for companies to acknowledge that the model of the traditional security perimeter is broken; it's now everywhere their workers, data and devices will be.

"A lot of the attacks don't happen against the hard outer shell. Sometimes they find the soft underbelly and the remote worker is an increasingly common source for attacking an organisation," says Ryder. "Frequently they have access to the most sensitive files, data and intellectual property in a company. It's important their security perimeter is treated with as much importance as the company's headquarters security perimeter.

"Organisations must secure remote workers and devices wherever they roam. The same security posture they have in their office environment needs to be applied to remote workers and implementing that is one of the biggest challenges they face.

"Avast Business has an always-on solution that wherever workers are, provides the same security they get in the office. Even when working on an insecure public wifi network, we provide two-factor authentication and ensure the worker is always behind a robust, cloud-based firewall. It's essential that this firewall is inspecting all SSL (secure sockets layer)/https (hypertext transfer protocol secure) traffic, otherwise they're close to useless.

"IoT devices are being adopted faster than the security postures that most organisations have put in place. We're going to be securing things we didn't think we'd have to secure. Security needs to be one of the foremost concerns in any IoT policy. Avast Business recognises this and we have put in place systems that ensure we are able to inspect traffic from all IoT devices.

"We provide a multi-layer security approach, at both the endpoint and network level, for remote workers and all IoT devices, from the smallest gateways to the large corporate centre."

Although security tools and technologies are vital to protecting companies in the age of IoT, one of the best defences, and indeed vulnerabilities, can often be the workforce itself. Remote workers with the right awareness are more likely to not only identify threats and alert the right people, but also prevent issues from occurring in the first place by ensuring they are doing all they can to keep their home IoT devices secure.

> We're going to be securing things we didn't think we'd have to secure

For more information please visit https://www.avast.com/en-gb/business

avast business

Four security tips for the remote worker

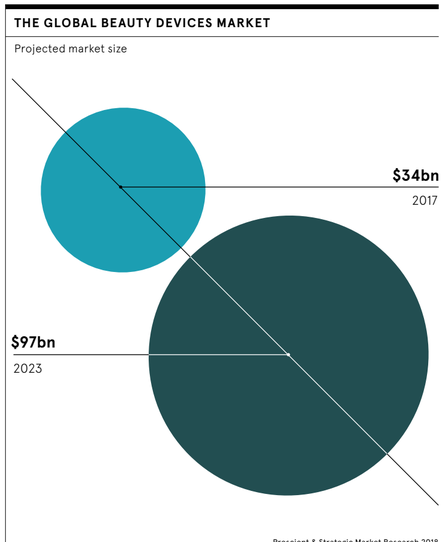
1 Secure your router
Household routers are central to IoT network security, yet Avast has found 60 per cent are vulnerable. They all come with a default password that should be changed immediately to something impossible to crack. Making sure the security protocol is WPA2 (wifi protected access II) is also critical and provides a strong foundation of basic security.

2 Change other default passwords
The router isn't the only thing you should be changing passwords on. No matter what the device is, when given the option you should always change the default password to something complicated. Two-factor authentication, if available, should also be enabled. Password managers are very handy and mean you don't have to remember them all.

3 Read the settings and connect only if necessary
IoT devices are created to be simple: take them out of the box, plug them in and away you go. However, each one is a possible gateway for a hacker. Take the time to purchase devices with an encryption standard, to read the security settings and only connect them at the times you need them. For example, if you only drink coffee in the morning, your connected coffee maker shouldn't be on all day.

4 Get additional security and always run updates
It's important that remote workers realise they are as responsible for cybersecurity as their company is. A strong antivirus protection product is a necessity and IoT devices must be kept updated with the latest versions available from the manufacturer. Updates often include security patches for flaws or bugs, which will help keep hackers at bay.

Plush Design Studio/Unsplash



BEAUTY

Do we really want connected beauty?

The beauty industry has been an unexpected player in consumer electronics, but are smart brushes and skincare apps really what customers want?

Katie Deighton

Back in 2015, L'Oréal jolted attendees at Dreamforce awake. Delegates at the annual Salesforce conference had endured days of pitches for digitalised sales pipelines and customer retention management systems. They hadn't banked on someone showing up and talking about technology in the beauty industry. They hadn't expected a "connected eyeliner".

Dreamforce 2015 was something of a marker for the multinational beauty company, which was one of the first to take the concept of the internet of things (IoT) and apply it to something as aesthetic as a mascara wand.

Until then, IoT had largely been spoken about in the context of businesses such as Google, Cisco and IBM. Now, here was a L'Oréal executive suddenly talking about tracking the behaviour of customers through their eyeliner or lipstick.

But behind the scenes, L'Oréal had been going through a business transformation. The year before it had launched its Make-up Genius app, which enabled customers to "try on" make-up shades through augmented reality (AR) before purchasing. It went on to acquire the company behind the tech, ModiFace, in 2018. L'Oréal then tasked head of its technology incubator Guive Balooch to start building a global team of engineers, user experience specialists and industrial designers.

Connected innovations began to roll out across L'Oréal's portfolio. Kérastase created a smart hairbrush, Vichy launched its SkinConsult AI and La Roche-Posay developed UV Sense, a wearable sensor that tracks exposure to damaging sunlight.

L'Oréal was by no means the only brand to welcome tech in the beauty industry. Neutrogena developed its SkinScanner, a magnifying device that clips on to an iPhone and analyses the likes of pore size and wrinkle deepness. At the premium end of the beauty spectrum, Shiseido revealed its Optune system, an app-connected machine that processes skin, sleep and environmental data, and dispenses a customised serum based on the user's reading each day.

> It is possible, even imperative, for a brand to explore how to bring the benefits of connected technologies to customers

Arrival of connected tech in the beauty industry was belated but inevitable, according to Andy Hood, head of emerging technologies at digital agency AKQA.

"The sector is prime for IoT," he says. "There is almost infinite variety in people's skin conditions and responses, physical appearance and personal taste. This makes for an industry where learning about someone and applying what is learnt to what is communicated to them is clearly hugely important and beneficial.

"Now, in an era when technologies are cheap, data is easy to gather and there are a great many ways in which to turn these things into customer value, it is possible, even imperative, for a brand to explore how to bring the benefits of connected technologies to customers."

And yet, when was the last time you saw a connected beauty device in Superdrug? Why hasn't Boots cleared space for an IoT aisle? For all that the beauty world hails the arrival of tech-driven products as a revolution, the consumer demand for them has been muted at best.

This is most clearly displayed in the market failure of a raft of beauty technology. Samsung, for instance, unveiled its S-Skin device to great fanfare during the Consumer Electronics Show (CES) in 2017; three years later, it isn't available for purchase. And that Kérastase smart brush? No longer on the market.

"Every year at CES you see all this amazing technology from the big brands and you rarely end up seeing them in stores," says Benjamin Lord, chief marketing officer of beauty search engine Mira. "These products are usually extremely expensive, $300 or more. There's definitely a lot of mistrust from consumers. And the branding itself is just not very good. The superfuturistic positioning beauty brands take, it's probably not right."

For Lord, beauty's investment play in IoT is currently just that, an investment play. Periodically showing up at tech conferences with impressive IoT devices proves to shareholders a brand is anticipating future consumer trends and worthy of headlines across a broad array of media.

"The increase in connected technologies is not driven by customer demand," Hood agrees. "Beauty-based businesses are using new technologies to differentiate their brand and provide new services that elevate their products and evangelise their expertise, delivering more value and being more attractive to customers."

But if delivering tech in the beauty industry is an investor or public-relations game, it's certainly an expensive one for most to be playing.

L'Oréal's Balooch has built a team that spans offices in San Francisco, New York, Paris and Shanghai, and developed IoT products for hair colour, lipstick colour and everything in between. Its latest development is Perso, a three-in-one system that manages to combine IoT with AR and artificial intelligence-gathered Instagram trends.

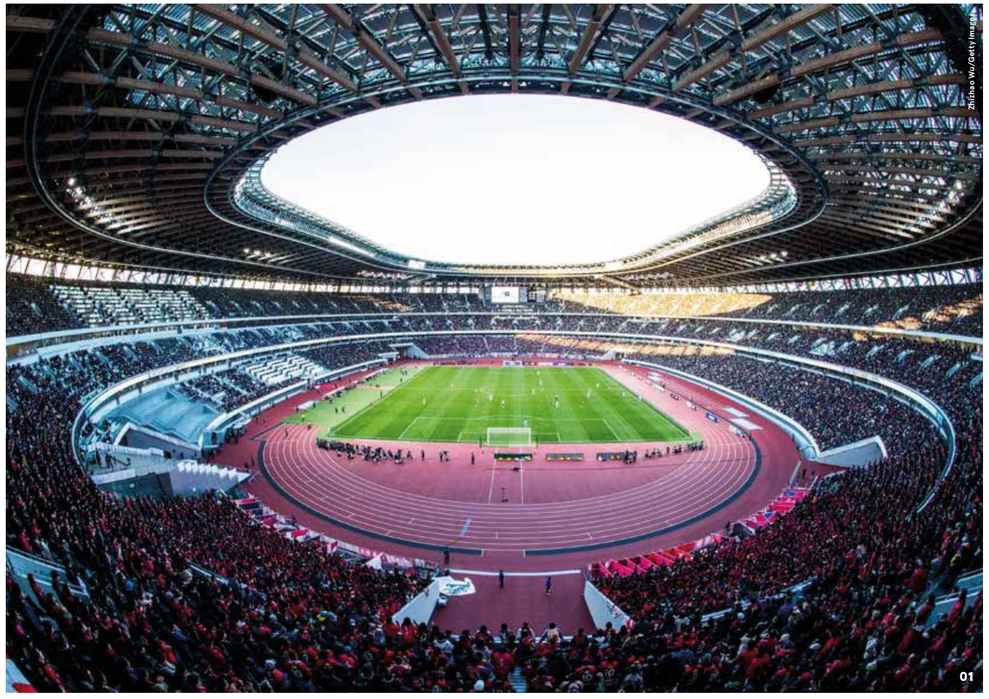
Pioneering such products to a company tied to a fast-moving consumer goods business model, a legacy manufacturing process and a relatively price-elastic product catalogue hasn't been easy, he concedes.

"We're going to see many more new business models, more subscription-based offers, more personalisation, maybe more products that are made with exactly the right amounts for what you're trying to achieve, rather than it being just one specific amount," he concludes. "We're at a critical stage where we're trying to understand that value creation. But in a company like ours, we're constantly looking to push the boundaries. And it hasn't been as difficult as I thought."

SMART CITIES

Tokyo on track for smartest Olympics ever

Robotic guides, crowd control directed by artificial intelligence and immersive virtual reality are among the technologies, enabled by the internet of things, set to excite fans at Tokyo's 2020 Olympic Games


Zhihao Wu/Getty Images

01

Rebecca Hallett

At the 1964 Tokyo Olympics, the world was wowed by demonstrations of innovative technology, such as the bullet train. Fast forward and by the 21st century Japan had cemented its status as a technological world leader, in areas as diverse as aeronautics, robotics and consumer electronics. It's no surprise, then, that the Tokyo 2020 Olympic and Paralympic Games' slogan is "Discover Tomorrow". But how might Japan use the leading tech of 2020, notably the internet of things (IoT), to make the Olympics run smoothly?

Tokyo 2020 is a huge undertaking. Around 11,000 athletes from 206 nations will be competing in 33 different sports and 7.8 million tickets are being distributed. Though 4.5 million of these have been set aside for the Japanese market, the remaining tickets will go to visitors from overseas. These visitors will strain the city's infrastructure, particularly accommodation, transport and waste management.

Security will be a key concern, and high-tech approaches may help with crowd control and risk assessment. Venues will also need to meet access requirements for visitors with mobility restrictions, and find ways to make the user experience smooth and enjoyable.

Tokyo has already implemented many smart city ideas using IoT technology. With one of the most-used public transit systems in the world, integrated innovative technological solutions are vital to make sure trains, buses and trams run safely and on schedule.

Trains on the Yamanote subway line depart every two to four minutes, carrying a dizzying 34 million passengers a week. With such high demand, periodic maintenance closures are a real problem, so an IoT-based smart maintenance system was introduced to minimise disruption. Sensors attached to train cars collect data, identify weak points, predict equipment failures, and pinpoint precisely when and where maintenance is needed.

> **IoT will play a key role in responding to the real-world problems presented by an event on this scale with digital technology**

Tokyo is well on its way to developing a smart energy system. The 2011 earthquake and tsunami caused severe power shortages, highlighting the need for a more adaptable and resilient grid. This is where smart meters and other energy management technology come into play. The data collected through these IoT devices have already underpinned new energy-saving measures. According to the Tokyo Bureau of Environment, the scheme achieved a 27 per cent drop in CO^2 emissions at the 12,000 registered facilities between 2010 and 2017.

This is all part of Tokyo's plans to use smart technology to become a zero-emissions city. Development around the Olympics will also play a part, with the athletes' village due to be turned into a fully hydrogen-powered smart district after the Games.

To meet the challenges presented by the Olympics, Tokyo's existing smart city tech may be developed further, but we'll probably also see a few new things using cutting-edge IoT and 5G technology.

rafapress/Shutterstock

Tokyo 2020 and the race for 5G

Underlying much of the technological innovations proposed for Tokyo 2020 is 5G. Though it's been a buzzword for the past couple of years, this high-speed mobile internet is technology only now becoming available to consumers. Simply put, 5G is very fast mobile internet, potentially ten to twenty times faster than 4G, which enables streaming of HD and 4K video.

On a larger scale, it makes data-intensive communications possible in ways we haven't seen before, for instance enabling ultra-HD footage to be transmitted and viewed with almost no delay. This is the kind of application NTT Docomo and Rakuten would be using for their proposed virtual reality streaming of Olympic events, potentially enabling an immersive experience of the Games for those who can't attend in person.

And, of course, the applications don't end with live-streaming sports. The dramatically reduced lag is incredibly useful in areas as varied as video-gaming, piloting drones and even remote surgery.

China's Huawei is one of the most prominent companies on the global stage when it comes to the development of 5G infrastructure. However, after effectively blacklisting the company due to cybersecurity concerns in 2018, the United States will be looking to find other providers of the technology.

If Japanese companies such as NTT, Rakuten and NEC, which was involved in the smaller-scale use of 5G at the 2018 Pyeongchang Winter Olympics, manage to roll out 5G in any significant way for Tokyo 2020, it could have a real political impact, establishing Japan as a major player in the race for 5G.

01 Inside the new National Stadium in Tokyo

02 Inflatable statue at Be the Change Tokyo 2020 event

Robots are emblematic of Japan's status as a world leader in futuristic technology, so it's likely they'll be front and centre at the opening and closing ceremonies. Visitors may be greeted by one of the Haneda Robotics Lab robots, which will serve both as multilingual airport guides and as security, scanning bins for suspicious objects and alerting human guards to unattended luggage.

The International Olympic Committee has been working with Toyota to develop vehicles powered by artificial intelligence (AI) for use in the main stadiums. Some will use sensors and cameras to deliver equipment to athletes, while others will help fans with accessibility requirements.

With its smart stadium concept, telecommunications company NTT is playing a key role in applying IoT technology to the Games. High-speed internet at each venue will enable everything from in-seat food orders to live stats and replays, while English–Japanese translation AI chatbots will be installed on robots at the major venues.

Though it remains to be seen whether the technology will be ready by summer 2020, virtual reality (VR) is also a major area of innovation, using a distributed camera network and the smart stadium's super-fast 5G to enable a live feed of events. NTT's Kirari project would use IoT tech to create an immersive VR experience of what's happening. Rakuten has been working on similar smart stadium VR tech, to enable fans to preview seats before booking them.

It's likely that we'll also see the largest-scale application of AI-based security measures ever at Tokyo 2020, relying on real-time updates from cameras and other internet-enabled devices dotted throughout the venues. Behind the scenes, NEC and Intel facial recognition terminals will verify the identities of the 300,000 accredited people at the Olympics.

The general public are more likely to spot drones owned by Rakuten or interact with robots which look like the Games' mascots, both of which will also be equipped with facial recognition technology. Whether everyone will know they're being observed in this way when waving at the cute robot remains a thorny issue.

Panasonic's crowd-forecasting software might also provide a glimpse of the future of security at Tokyo 2020. Using camera data from police vehicles, the software would analyse crowd movements to identify suspicious behaviour and help with real-time management of crowd flow. This could be used in combination with security firm ALSOK's emotional visualisation robots, which flag people showing high levels of anxiety or aggression.

Tokyo 2020 is sure to be a showcase not only of world-class sporting talent, but of cutting-edge technology in areas as varied as commerce, security and accessibility. IoT will play a key role in responding to the real-world problems presented by an event on this scale with digital technology, and will contribute to the most technologically exciting Olympic and Paralympic Games we've yet seen.

11,000
athletes

206
nations

7.8m
tickets distributed

Tommo/Shutterstock

02

You Already Know Telit Modules — Now Get to Know Our IoT Connectivity Services

One-Touch Solutions for Streamlined Cellular IoT Deployments

Ask us about our SIMs, global data plans, multicarrier services and Telit simWISE ™

To learn more, visit Contact.Telit.com/SIM

Telit