quocirca

Business and IT Analysis

The many guises of the IoT

Effective IoT application design and security

December 2015

Throughout 2015 there has been much talk about the Internet of Things (IoT). Too often this has been with little context, as if the whole IoT phenomenon is something completely new and discrete from other IT issues. The truth is that the IoT is not new, it is not discrete, but it is at the core of an increasing number of IT applications, often involving the integration of legacy devices.

This report presents new research into the perceptions held with regard to the IoT and shows where promise is turning into practice. It looks at what those with less experience can learn from those in the IoT vanguard, about changes to IT management and security necessary to support effective deployments and reduce concerns.

Bob Tarzey
Quocirca Ltd
Tel : +44 7900 275517
Email: bob.tarzey@quocirca.com

Louella Fernandes
Quocirca Ltd
Tel: +44 7786 331924
Email: Louella.Fernandes@Quocirca.com

Executive Summary

The many guises of the IoT

Effective IoT application design and security

Enthusiastic or sceptical, no business can ignore issues arising from the growing numbers of network attached devices than constitute the IoT. This compels a review of existing management and security capabilities and a determination of necessary changes. Although this will require investment, the returns will make it worthwhile.

Few doubt the relevance of the IoT to their organisation	A small number (3%) think the IoT is over-hyped; some others (11%) believe it is not relevant to them. However, the overwhelming majority say the Internet of Things (IoT) is already impacting their organisation (37%) or that it will do soon (45%). The experience and approach of those in the vanguard demonstrate the opportunities; they also show where the pitfalls lie and how these can be avoided.
IT departments, lines of business and end users will all drive IoT uptake	In some cases lines of business are driving requirements, for example, in manufacturing where the way humans interact with machines is being improved. In other areas the initiative is being taken by IT departments as they increase automation of IT infrastructure management and enhance existing business applications. A third acknowledged driver, is the need to manage the ad hoc arrival of *things* on networks introduced by end users.
The IoT will improve existing and introduce new processes	The IoT is not a new concept. The human-to-machine (H2M), machine-to-human (M2H) and machine-to-machine (M2M) communication that underlie the IoT concept are as likely to be enhancing existing processes as they are to be creating new ones. Whilst new ways of interacting with customers will be created, much of the activity will remain within a given business.
The IoT will scale from the personal to the extra-terrestrial	One area where the IoT is expected to do as much about improving customer interaction as improving internal processes is at the personal level through wearables. Beyond this the IoT will scale up through vehicles, buildings, cities to the national and global level, even extending into outer space. The management and security capabilities put in place to support IoT enabled applications must operate at all these scales.
Design is essential for managing IoT scalability and security	Effective management and security will only be possible through good design. It is misguided to believe every sensor, probe and widget needs to be directly addressable. Those with experience already see the IoT as a series of hubs that interoperate with spokes on closed networks. Such an approach makes network configuration and security more manageable.
Constant verification of the identity of *things* is core to effective IoT security	Some existing security measures are adaptable to manage IoT-related risk, for example denial-of-service protection, DNS management and geolocation. However, new measures will need introducing; this is especially true when it comes to the necessity to constantly identify and verify that *things* are what they purport to be. Experienced IoT operators are turning to 3rd party registries and physical device characteristics to ensure they know what is what on the IoT.

Conclusions

Whilst the IoT is nothing new, the scaling out of it to millions of devices per organisation is. The IoT represents new opportunities at many levels. To make the most of these will require new investment in management and security capabilities, to ensure the same rigor and vigilance applied to *traditional* IT devices is extended to all connected *things*. The IoT vanguard is already ring-fencing budgets for this, others will follow and there will be new risks and rewards for all.

quocirca

Introduction – the IoT at the business core

The Internet of Things (IoT) seems to have been the topic du jour for much of 2015. Often the commentary is couched in such a way that you could be left with the impression that it is a discrete phenomenon within the broader discipline of information technology (IT). The truth is that the IoT is not new, it is not discrete and it is at the core of an increasing number of IT applications.

The new UK-focussed research presented in this report starts by looking at the degree to which the IoT is already relevant to different industries. It goes on to examine the management and security challenges that will be faced as the devices or *things* that constitute the IoT become pervasive. The aim is to show why the IoT is relevant to all businesses and how it is changing the world in which they operate.

To ensure as much consistency as possible from the respondents it was first necessary to try and cut through the rhetoric and provide some sort of definition. To this end Quocirca turned to Wikipedia, which starts its definition of the IoT as follows:

The Internet of Things is the network of physical objects or "things" embedded with electronics, software, sensors, and connectivity to enable the network to achieve greater value and service by exchanging and/or collecting data.

To this Quocirca added:

This may be entirely within a given business or may extend to "things" installed on the premises of partners and customers (including consumers).

Thus informed, respondents were first asked what the potential impact of the IoT would be for their organisation (Figure1). More than a third agreed it was '*already having a major impact*' and even more expected it soon. A much smaller number felt it would not impact their organisation; we have grouped them together with a handful that considered the IoT over-hyped or simply didn't know as sceptics. These three groupings with regard to their "*View on IoT*"; MAJOR, EXPECTANT and SCEPTICS are used throughout this report to expose how those in the vanguard differ from the laggards.

For example, so far, the impact of the IoT has been greatest in the transport (which includes distribution and logistics) and retail sectors, but expectations in all sectors are high (Figure 2).

Figure 1: Potential impact of the IoT with regard to respondents organisation

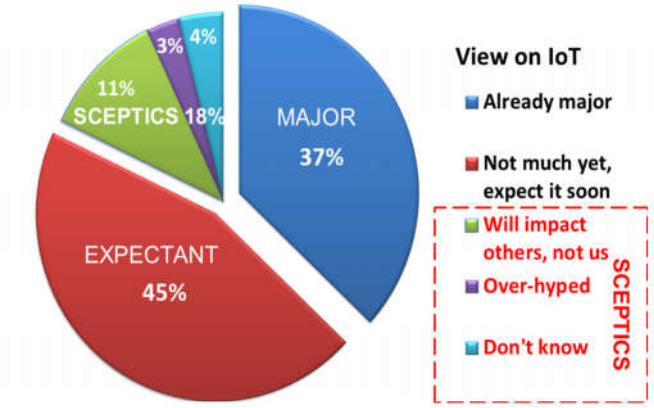


Figure 2: Industry views on impact of IoT

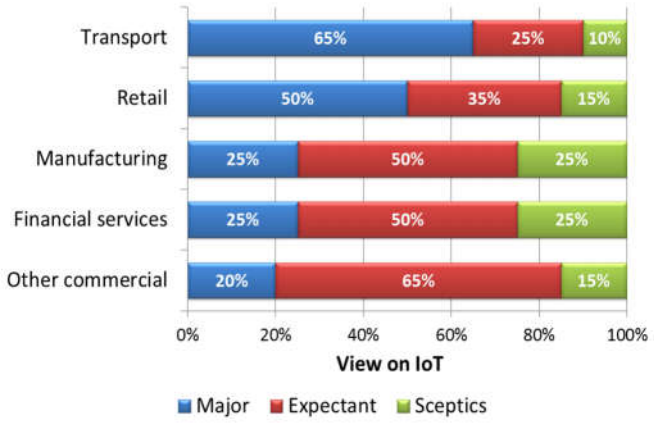
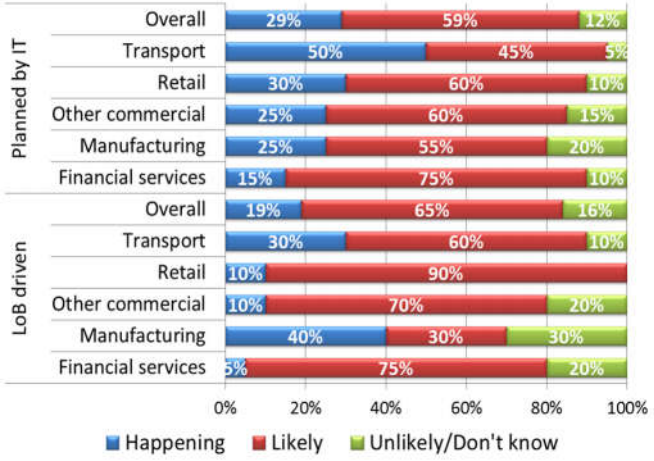


Figure 3: IT or line-of-business (LoB) driven?



The way the IoT already is or will become relevant varies. The actual roll out of applications may be due to initiatives taken within the IT function, driven by line-of-business or even due to actions taken by end users (Figures 3 and 4).

For IT departments the IoT enables improved services provision, through supporting more access points and remote devices, more effective infrastructure monitoring and the roll out of better physical security and surveillance applications, which are often part of the function's broader remit. In manufacturing lines-of-business are already taking the lead as they see opportunities to improve the way equipment is managed and monitor how processes are performing.

In some areas growth of the IoT will be ad hoc rather than planned as end users bring *things* into the workplace. For most this already includes smartphones, however, as other devices from TVs to kettles are shipped with network enabled chips embedded there may be many more. Effective IoT management will be required to control and limit this. Those with experience of the IoT are the most likely to recognise the reality of this (Figure 4).

The potential benefits should not be overlooked; 40% of retailers said ad hoc IoT was '*already happening*', perhaps as they encourage customers to actively or passively make use of mobile devices to enhance their in-store retail experience; for example, leading them to relevant products and enabling on-the-spot checkout. Revolutionary as this is, this result is to enhance an existing process – shopping – rather than create a totally new process.

IoT evolution

For most organisations, the IoT is not a new, but an evolutionary concept. It has as much power to improve existing or brown-field business processes as it does to create new green-field ones (as Intel puts it "*connecting the unconnected*"). Consequently there will be many different approaches to deployment and security.

Whether the IoT is more relevant to brown-field or green-field processes depends on the type of communication. Many equate the IoT purely to machine-to-machine (M2M) communications; however, it is also about how humans interact with machines. This can either be improved management via human-to-machine (H2M), for example of industrial equipment or consumer devices (cars, utility meters etc.) or machine-to-human (M2H) for better monitoring devices through data collection or digital signing for consumers. Put both of these together in an industrial setting

Figure 4: Ad hoc arrival of IoT devices introduced by users

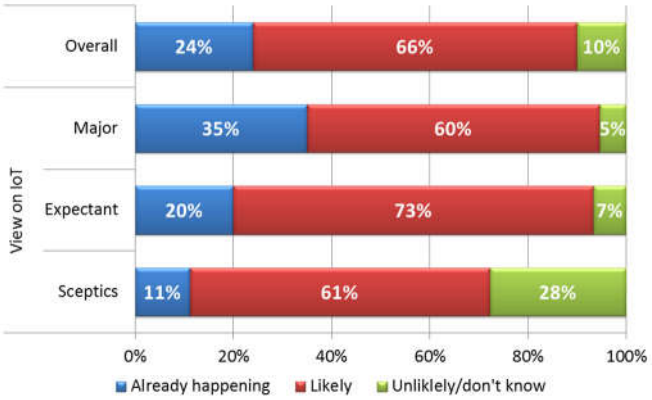
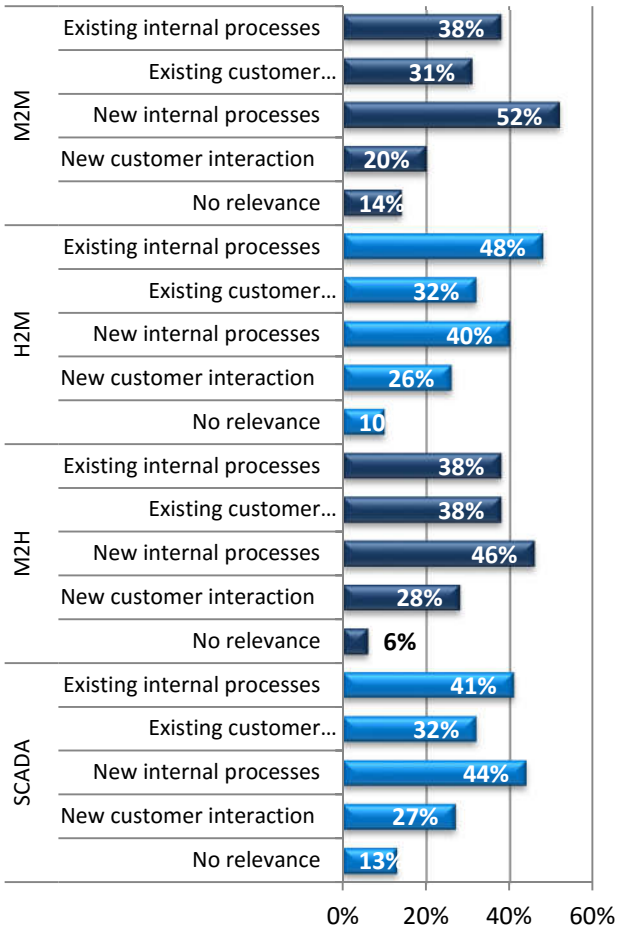


Figure 5: How IoT interactions relate to business processes



% believing IoT interaction type will shape a given process

and you get SCADA, the often heard but rarely spelt out abbreviation for *supervisory control and data acquisition*.

M2M, H2M, M2H and SCADA are all expected to drive internal processes more than customer interaction (Figure 5). H2M interaction is more likely to improve existing internal processes as management of existing equipment is streamlined. Gathering new data via M2H will enable new processes to be developed. All that said, M2M is going to be the driving force behind many of the IoT's challenges as it removes the latency of human interaction and drives automation.

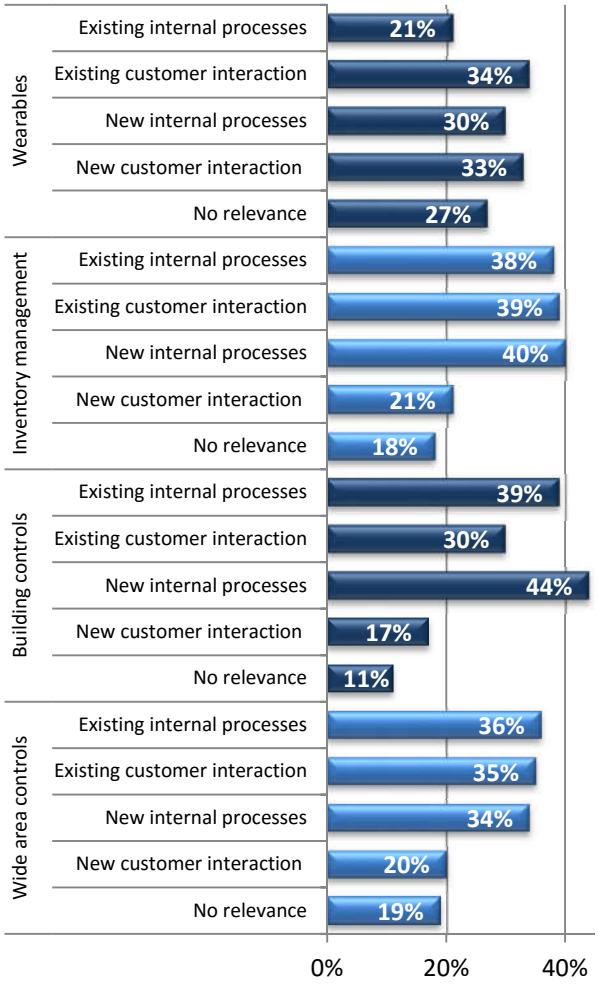
However, even with the speed of M2M communications, different applications will need to be managed in different ways to cope with varying feedback loops systems. For example, a racing car's fuel injection system needs to respond quickly to feedback from its breaking system to maximise fuel efficiency. Whilst a home heating system may need to plan many hours ahead to keep temperature levels close to constant, as heat is slowly leaked to the atmosphere as weather conditions change. Cars and homes are just two of the scales at which the IoT will operate.

IoT scale: from the personal to the extra-terrestrial

The IoT is relevant at different scales depending on the type of application. The smallest scale is personal and driven by wearables; smartwatches, bio-sensors, smart glasses etc. Here, both improvements to existing and new interactions with consumers are expected to take the lead (Figure 6). Wearables are also likely to become more important in the workplace, perhaps freeing up the hands of logistics workers and field service engineers whilst keeping them online. Scaling up, vehicle area networks will serve both consumers and workers making their vehicles more efficient, safe and convenient to operate.

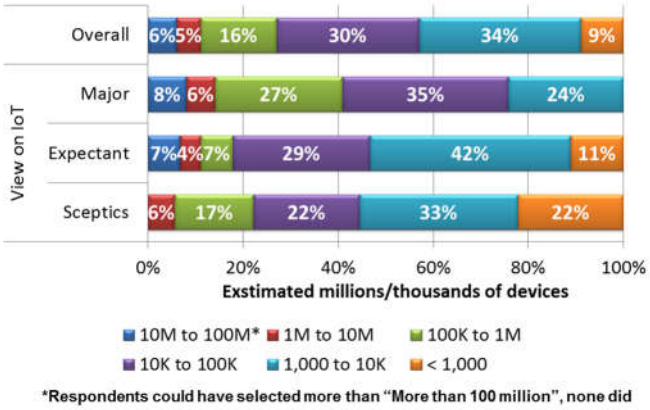
Better inventory management is relevant at many scales; from the devices workers carry to the equipment installed across vast utility networks. The use of radio frequency identity (RFID) to automate inventory management will improve both internal processes and customer interactions and reduce operating costs. Predictive maintenance is also easier through devices proactively reporting their status, for example, printers and/or copiers running out of ink, or ATMs and vending machines seeing an unexpected run on supplies. Much of this is not new, but can be improved with the growing number of supporting tools and services available.

Figure 6: How the IoT is expected to scale



% believing IoT applications at different scales are relevant

Figure 7: Potential number of devices involved over the next 12 months by view on IoT



*Respondents could have selected more than "More than 100 million", none did

The buildings in which we work and play are all expected to become more intelligent and efficient, as are our homes, for example, more integrated physical security and smarter energy use. Local governments will connect buildings and infrastructure across cities enabling the faster and cheaper distribution of goods and services and improved public safety, for example, smarter surveillance and improve traffic flow via dynamic signalling. Traffic management systems already extend beyond cities to national networks and will be improved over time, the same will happen with energy supply.

Some networks will be global, for example, surveillance information shared between airports and inventory managed globally by aircraft and shipping manufacturers. Outer space has a role, at a practical level for earthlings, as geolocation systems feed into IoT applications, and for research purposes, as space agencies monitor the many sensors aboard the robot explorers in orbit around, and moving on the surface of our planetary neighbours and further afield. The Voyager probes launched back in 1977, which are now moving into inter-stellar space, are icons both for the potential scale of the IoT and the need for legacy integration.

All this activity adds up to huge number of devices. The overall average per individual UK organisation over the next 12 months runs into millions (Figure 7). Scale this up across multiple organisations worldwide and you can see why some estimates for future run into tens of billions of *things*. Actual experience of the IoT drives up the numbers considerably, the sceptics putting in much lower estimates. All these devices will be attached to a variety of networks; there will be increased stress on the existing ones and new networks will need to be deployed.

Network variety and the IoT

As with the IoT itself, the supporting networks will scale from the personal to the wide area. Hard-wired links may make sense in some cases, for example, between sensors and a central in-car controller. However, due to the nature of many IoT deployments the use of wireless will be commonplace speeding up installations and keeping costs down. Wires are a nuisance about the person, and Bluetooth LE (low energy) for personal area networks (including certain healthcare applications) is already well established.

Figure 8: Network variety for supporting IoT deployments

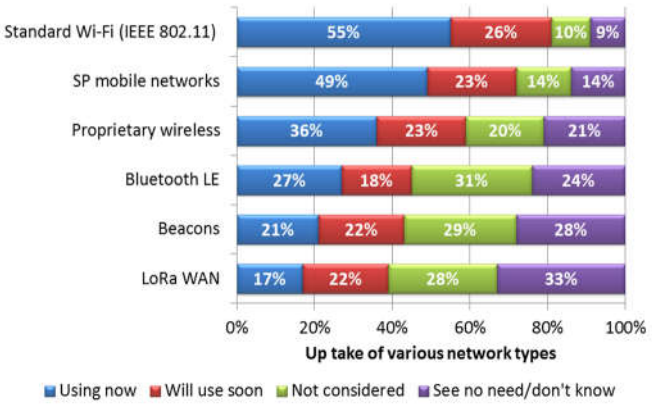


Figure 9: Use of beacons, by view on IoT and relevance of IoT to wide area controls

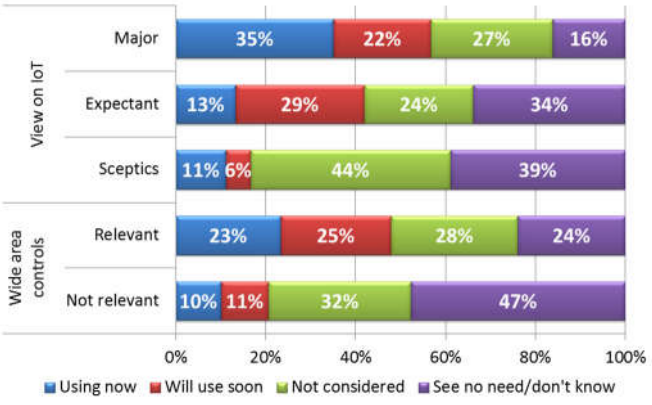
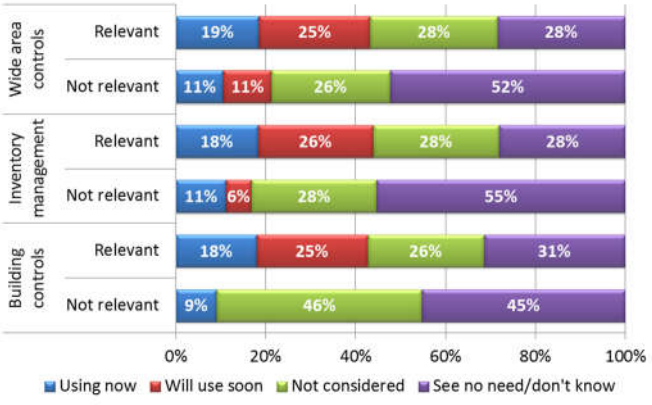


Figure 10: Use of Lo Ra WAN, relevance of IoT to wide area/building controls and inventory management



The use of standard Wi-Fi and service provider mobile networks will be the starting point for many (Figure 8). However, those in the vanguard are already supplementing these, for example, boosting networks with local beacons (Figure 9), especially where wide area controls are needed. LoRa WAN (Long Range WAN) an open specification for wide area Wi-Fi, is also relevant for inventory management and building control (Figure 10).

IoT management challenges

The greatest management concern with the IoT is that data volumes will overwhelm networks (Figure 11). Experienced users worry about this even more than average, along with the worry that they will not be able to effectively analyse all the data generated. However, they are taking actions to address these concerns, including deploying network edge processing to reduce data at the core, new business and operational intelligence tools and integration with enterprise applications, such as ERP systems (Figure 12). Such tools enable the required intelligence to be derived from IoT deployments; simply connecting *things* does little without the addition of such capabilities.

There is no shortage of standards, initiatives and consortia to enable the IoT (Figure 13 and Table 1). The list may look overwhelming and this may put some would-be IoT users off. However, those with experience worry less than average, they just seem to be getting on with it, making use of established standards or those that seem likely to become so.

Basics such as SSL/TLS and PKI top the list – underlining the need for security. Windows 10 is already high on the list; recognition of the benefit of consistency of deployment of operating environments across IoT devices and supporting platforms. Some standards are specific to use cases, for example, ZigBee (see Table 1) is of greater interest where inventory management is involved.

One often-touted IoT problem, the issue of IPv4 internet address availability actually bottoms the list of concerns by some measure. In fact IPv4 is more likely to be in use than IPv6 (Figure 14). The use of IPv6 is similar regardless of *view on IoT*, supporting the idea that this is a neutral low concern issue. The reason is that not all "devices" on the IoT are equal and design reduces the need for unique IP addresses.

Figure 11: General concerns about IoT

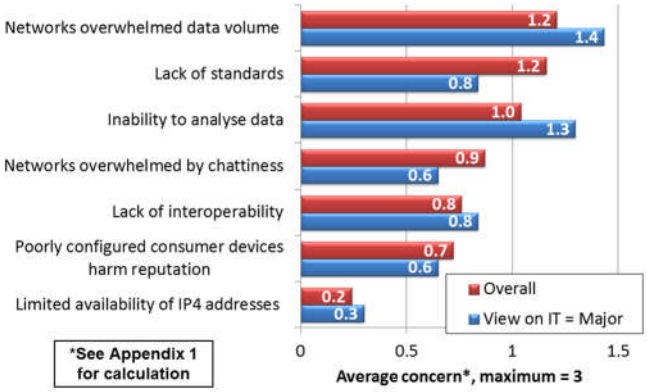
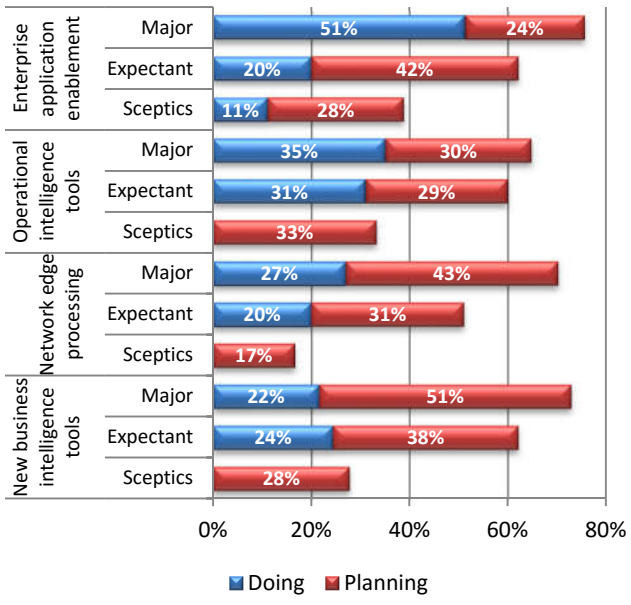


Figure 12:Actions taken to enable IoT deployments by "view on IoT"



Hubs or gateways which control communications with the outside world, for example, network routers, set top boxes, smartphones and satellites, **do** need unique IP addresses; hubs communicate onwards with spokes, which **do not**. This is as in traditional network management, where network address translation (NAT) avoids the need for each device to have a unique IP address.

This hub and spoke approach can work at any scale: personal, car, home, national and so on. A hub may communicate with its spokes using one network type and the outside world with another. Hub and spoke also makes the selective, effective and cost efficient deployment of IoT security more straightforward.

Figure 13: Importance of standards, initiatives and consortiums (see table 1 for more detail)

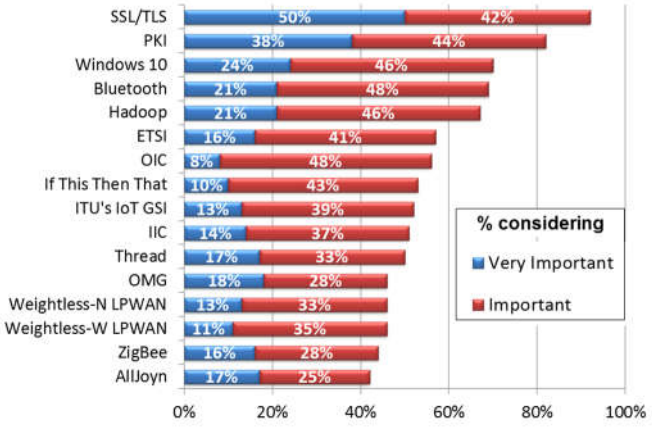


Figure 14: IP versions in use for supporting IoT deployments

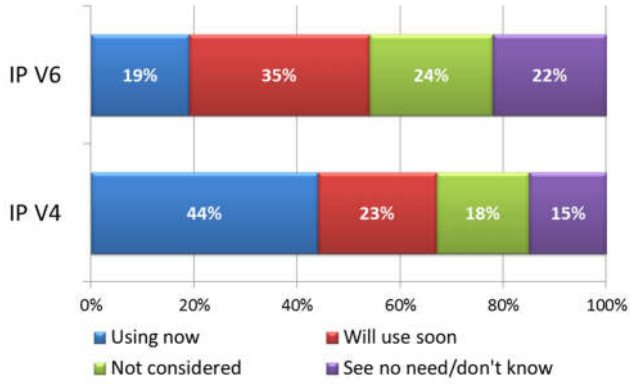


Table 1 – standards, initiatives and consortia (see also Figure 13)	
Standards	
SSL/TLS	Longstanding protocols that can be used for the encryption of IoT data and the authentication of *things*
PKI	Public Key Infrastructure (PKI) for managing SSL/TLS certificates
Hadoop	Big data framework for backend analytics
Bluetooth	Also Bluetooth Smart, for near field communications (NFC)
Consortia	
ETSI	European Telecommunications Standards Institute
OMG	Object Management Group
IIC	Industrial Internet Consortium
Weightless-N LPWAN	Weightless-N low power wide area star network architecture – operates in sub-GHz spectrum using ultra narrow band (UNB) technology
Weightless-W (LPWAN	Weightless-W open standard is based on a low power wide area (LPWAN) star network architecture operating in TV white space spectrum
ITU IoT GSI	International Telecommunication Union IoT Global Standards Initiative
OIC	Open Interconnect Consortium (backed by Intel)
AllJoyn	An open source initiative (backed by Qualcomm)
Company initiatives	
IFTTT	If This Then That, cloud service for scripts to integrate processes across devices
ZigBee	Specification for a suite of communication protocols for creating personal area networks
Thread	Backed by Google and aimed at household devices
Windows 10	Microsoft latest operating system, designed to run on both user and non-user devices

Security – dark side of the IoT

As with general concerns, data related issues top the list of security concerns, in the form of customer privacy (Figure 15). For example insurers may recognise the value of data that can be collected about driving habits through in car sensors but realise the regulatory challenges. Major IoT users worry even more than the average shown about privacy. A close second is the expanded attack surface that that will be exposed as more IoT applications are deployed. In general security issues relating to the IoT can be considered in four broad groups:

1. **Data protection**: many devices gather sensitive data, so its transmission, storage and processing needs to be secure, for both business and regulatory reasons.
2. **Expanded attack surface**: more IoT deployments mean more devices on networks for attackers to probe as possible entry points to an organisation's broader IT infrastructure. Older devices with pre-IoT firmware are likely to be some of the most vulnerable.
3. **Attacks on IoT enabled processes**: hacktivists wanting to disrupt a given business's activities for some reason will have more infrastructure, devices and applications to target, for example, via denial-of-service (DoS) attacks on networks or by compromising and/or disabling individual devices.
4. **Botnet recruitment**: Poorly protected devices may be recruited to botnets. Incidents of this have been reported, for example, a botnet of CCTV cameras in October 2015[2].

Many IoT security issues are addressable through adapting and scaling measures that are already in place for existing IT infrastructure (Figure 16); 39% already have DDoS protection in place, another 31% are planning. However, there is not much difference between major IoT users and sceptics (Figure 17) as DoS attacks have been an issue for many years; more could be addressing the problem (these figures align with previous Quocirca research[1] published in 2014).

IoT hubs can be scanned using the same processes in place for existing IT end-points. Software scanning can be extended to covering IoT firmware, depending on support from both firmware and scanning supplier. Consumer goods manufacturers will need to consider how to update software associated with the *things* they supply; in other words: "*how do we patch the toaster?*"

Figure 15: IoT security concerns

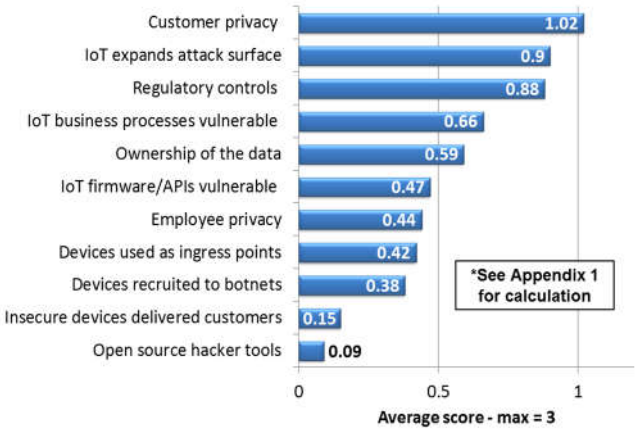


Figure 16: Use of Security measures to enable IoT

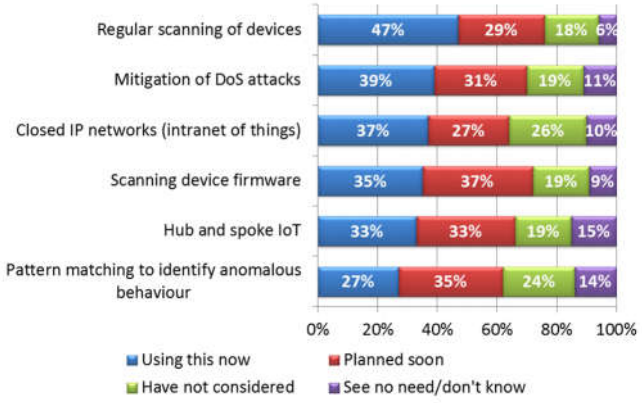
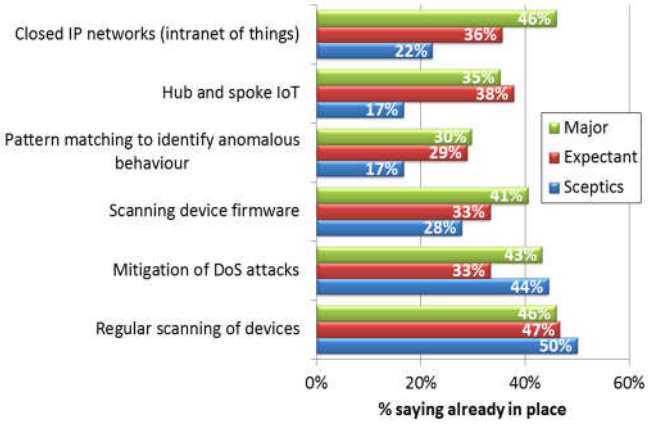


Figure 17: Deployment of security measures by view on IoT



Other security measures are more IoT specific, but aligned with existing IT practices, such as closed IP networks, which are more than twice as likely to be in place with major users of IoT. 35% of major users recognise the value of a hub and spoke approach, compared to just 17% of sceptics. Overall, many more could be using these technologies, whether IoT advocates or not! If the IoT is to be secure into the future there is much work to be done. A key component of this is being able to confidently recognise millions of *things*, which for many requires upgraded device identity management capabilities.

The identity of *things*

There are established ways for authenticating devices in IT and these have their place when it comes to the IoT (Figure 18). Major users and sceptics alike recognise the value of TLS/SSL as a means of authentication and DNS capabilities enabling certain *things*, for example hubs, to be addressed by easily understood names rather than numeric IP addresses. Using SSL means more certificates as devices proliferate and this has led to speculation of a renewed interest in Public Key Infrastructure (PKI) management; the views of major IoT users seem to suggest this may be case.

However, there are also ways of establishing and authenticating identity that stand out as having a strong association with IoT use. Examples include the use of purpose built databases (for example Xively) and neutral 3rd party master registries that can be referred to for identifying *things* and their expected location and function.

There are also elements of a *things'* identity that are more likely to be seen as useful by major IoT users (Figure 19). Certificates and geolocation are powerful, established capabilities in use by many. Others such as registry entries for devices and physical device characteristic or signatures are more likely to be in use by major IoT users. They are also more likely to have in place a capability for co-ordinating policy for network attached devices, with over 80% saying they have some capability to do this compares to less than 70% overall.

Once the elements are in place to be able to ensure the identity of a large numbers of *things* over and over again in near real time, the scene is set for an organisation to move forward with the safe roll out of increasing numbers of large IoT deployments at any relevant scale.

Figure 18: Use of capabilities for establishing and authenticating the identity of devices by view on IoT

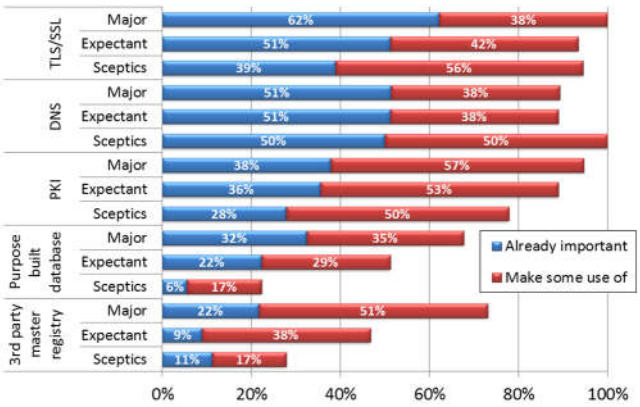
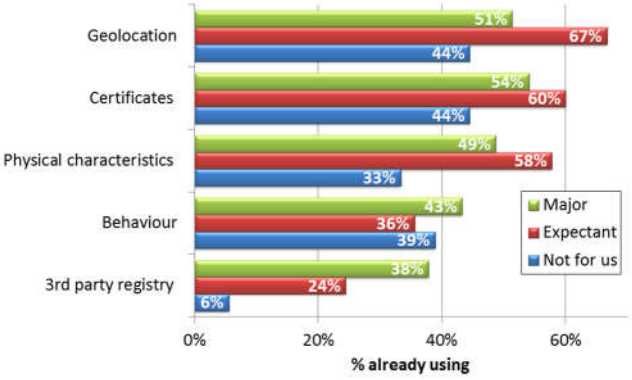


Figure 19: Use of elements of identity for devices by view of IoT

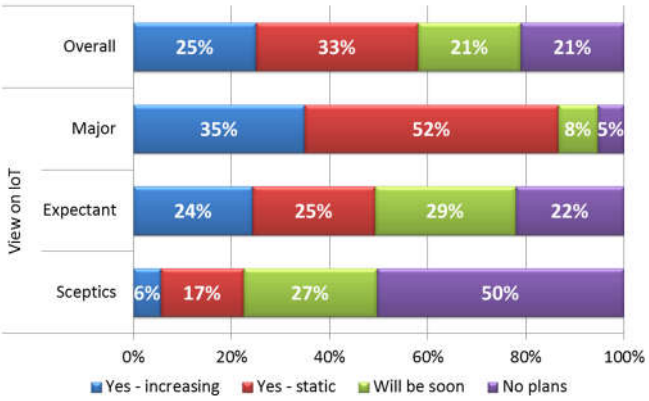


Conclusions

Sceptic or otherwise, the IoT is relevant to your organisation. Whether IoT applications are deployed to help IT function, driven by lines of business or through devices introduced by end users, various practices will need adapting to accommodate the millions of *things* involved which will overtime dwarf the number of traditional IT end-points.

The challenges can be minimised through thoughtful design and the use of hubs, however, certain measures, including new networks, management tools and security capabilities will be necessary to get the most out of the IoT. This is leading to dedicated budgets being set aside for supporting the IoT (Figure 20). The evidence suggests that the cost of supporting investments can be justified by the business value that will be derived from newly IoT-enabled applications.

Figure 20: Does your organisation have a dedicated budget for IoT?



References

1 – Online domain maturity, Quocirca, October 2014
http://quocirca.com/content/online-domain-maturity

2 – CCTV Botnet In Our Own Back Yard; Imperva blog Oct 2015 http://blog.imperva.com/2015/10/cctv-botnet-in-our-own-back-yard.html

Appendix 1 – calculations

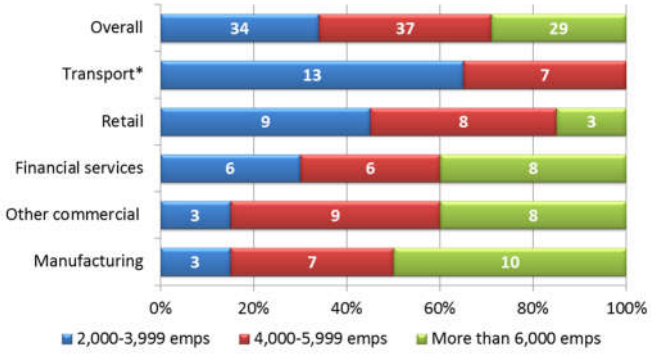
Calculations used in figures 11 and 15.

Users were asked to select and rank their top 3 of 7 general and 11 security specific concerns. In both cases an "other" option was also included that no one selected. To derive a weighted average for each concern, each instance of a top rating was scored 3, a second rating 2, a third rating 1 and unrated 0. Thus, if all respondents had rated the same concern first it would have scored 3, if none had rated any concern it would have scored 0. Figures 11 and 15 both show the average rating for each concern across all 100 responses.

Demographics

100 IT decision makers in UK enterprises were target for this survey. Figure 21 shows the breakdown by sector and size.

Figure 21: 100 senior IT decisions makers from UK enterprises (showing actual sample numbers)



*Transport, includes distribution and logistics

About Neustar

About Neustar

Neustar, Inc. is a trusted, neutral provider of real-time information and analysis to the Internet, telecommunications, entertainment, advertising, and marketing industries. Neustar applies its advanced, secure technologies in routing, addressing, and authentication to its customers' data to help them identify new revenue opportunities, network efficiencies, cyber security, and fraud preventions measures. More information is available at http://www.neustar.biz.

Neustar SiteProtect: Keeping Businesses Safe from DDoS

To combat the dangers of DDoS, Neustar offers SiteProtect, a cloud-based, on-demand DDoS mitigation service. Activated through DNS or BGP redirection, SiteProtect scrubs away malicious traffic in the cloud, letting valid traffic flow to your infrastructure. To do this, SiteProtect relies on a large global mitigation network, featuring 15 IP anycasted scrubbing centres. Using diverse equipment from leading mitigation vendors, SiteProtect is designed to stop numerous types of attacks, including those involving the application layer, IPv6, and encrypted traffic. Technology diversity sets it apart from other mitigation solutions. By drawing on each vendor's strengths, SiteProtect can stop the multi-faceted assaults that are evolving rapidly and redefining the DDoS landscape. Backed by Neustar's 24/7 Security Operations Centre – fully manned on-site by highly experienced experts – SiteProtect supplies the assurance businesses need. While it's best to prepare in advance, Neustar can emergency-provision SiteProtect should your business suddenly come under a DDoS attack. Learn more at http://www.neustar.biz/services/ddos-protection

REPORT NOTE:
This report has been written independently by Quocirca Ltd to provide an overview of the issues facing organisations seeking to maximise the effectiveness of today's dynamic workforce.

The report draws on Quocirca's extensive knowledge of the technology and business arenas, and provides advice on the approach that organisations should take to create a more effective and efficient environment for future growth.

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first-hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to provide advice on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, IBM, CA, O2, T-Mobile, HP, Xerox, Ricoh and Symantec, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at http://www.quocirca.com

quocirca