quocirca

European Perceptions, Preparedness and Strategies for IoT Security

New research conducted in the UK and German-speaking regions exposes the challenges organisations face in managing and securing Internet of Things (IoT) devices

Executive summary:

- The IoT is playing an increasing role in a range of business processes, leading to device proliferation and **extending IT attack surfaces**
- The need to put in place **new technologies to discover, manage and secure devices** is accepted by the majority
- It is recognised that IoT security **cannot rely on agents** installed on devices as some will be unknown and others will run unusual operating systems
- Traditional tools fall short in managing and securing IoT devices, organisations have to **rethink IoT security policies**

Report Authors

Bob Tarzey

Tel: +44 7900 275517

Email: bob.tarzey@quocirca.com

Louella Fernandes

Tel: +44 7786 331924

Email:Louella.fernandes@quocirca.com

Commissioned by

ForeScout

Introduction – IoT opportunity and risk

The Internet of Things (IoT) is changing the way business is done; it is recognised by the majority of organisations as an opportunity to improve and streamline business processes and a new way to interact with customers. The impact and growth of IoT has the potential to be as big as the Internet was in the 1990s with device numbers expected to at least triple by 2020 (see box on page 3). However, the large number and wide range of devices involved expands network attack surfaces and requires existing security measures to be adapted and scaled.

New research is presented in this report from interviews with 201 senior IT decision makers in the UK and German-speaking regions (Germany/D, Austria/A and Switzerland/CH, abbreviated to **DACH**); all the figures included are based on the views expressed by the respondents. The research covered a range of industry sectors and businesses with as few as 10 employees up to large enterprises with more than 10,000 employees (see Appendix 2). The research follows on from an earlier survey carried out in the U.S. (see appendix 1).

The report examines current thinking around the IoT, the number of devices involved and capability and plans to discover, manage and secure devices. It concludes by looking at where organisations stand with regard to an IoT security policy and the issues they must overcome to exploit the full potential of the IoT.

View of the IoT

One third of respondents say the IoT is already having a major impact on their organisation, a further third expect it to soon. The remainder believe the IoT will mainly impact other organisations, only 6% think it is over-hyped (Figure 1).

DACH and UK were both close to the overall values. 10,000 plus employee organisations were around twice as likely to be in the MAJOR category as smaller organisations. IT and telecommunications are the most advanced sectors (Figure 2). Healthcare lags behind, a sector which many think stands to benefit much from the IoT, so it seems the message is yet to get through to many of these organisations.

Full definitions of figure category titles (abbreviated on figures):

- **MAJOR** – It is already having a major impact on our organisation
- **EXPECTANT** – It has not impacted our organisation much yet, but we expect it will soon
- **WILL IMPACT OTHERS** – It will impact other organisations, but not our own
- **OVER-HYPED** – It is an over-hyped phenomenon that will not come to much

Figure 1: View of potential impact of the IoT on the respondents organisation BY SIZE

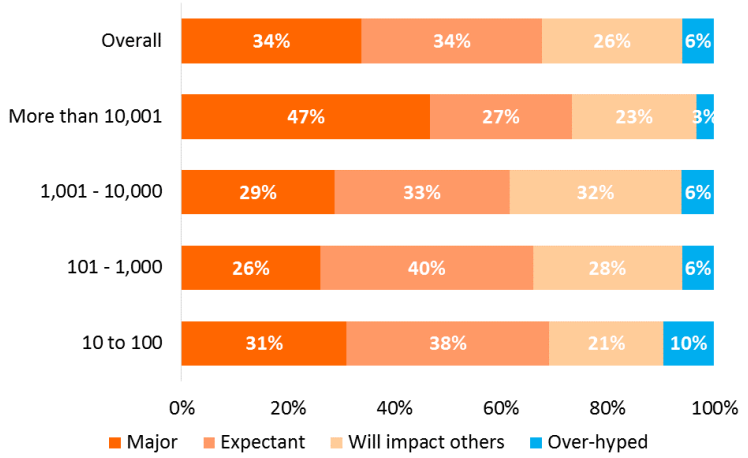
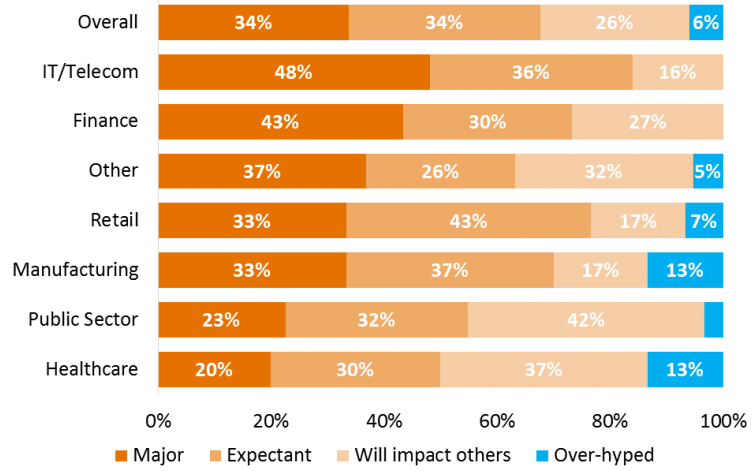


Figure 2: View of potential impact of the IoT on the respondents organisation BY SECTOR



Increased size and heterogeneity of attack surface

The average business expects to be dealing with 7,000 IoT devices over the next 18 months (Figure 3).

This figure is skewed by the number for larger businesses, however, even smaller businesses expect the numbers to be hundreds or thousands, far more than they are used to securing, when it comes to traditional user endpoints. Even organisations that believe the IoT is overhyped expect to have an average of 1,500 IoT devices online in the near future (see appendix 3 for calculation).

Whilst these figures may sound daunting to those charged with device management and security, they are actually conservative compared to other industry estimates (see box below). Over the next 18 months most organisations expect these numbers to increase as the percentage of all devices that are IoT devices increases (Figure 4). Nearly all organisation (98%) expect IoT devices to be connected to their network within 18 months.

Whatever estimates are believed, the deployment of smart devices at every scale from wearables, through building controls, national infrastructure management and even *things* in outer space, there are going to be many more network attached devices to contend with in the future.

Gartner: 6.4 billion connected "things" will be in use in 2016, up 30% from 2015[1]

Juniper: IoT-connected devices to almost triple to over 38 billion by 2020[2]

McKinsey: "20 billion or 30 billion [IoT] units" by 2020[3]

Figure 3: Potential number of devices involved in IoT related applications over the next 12 months

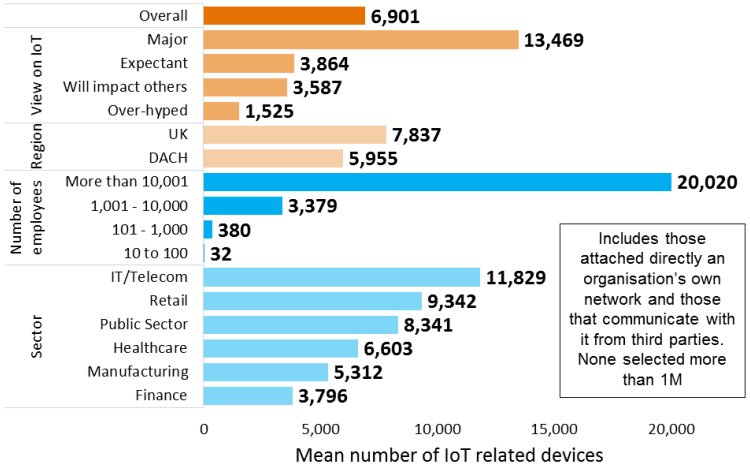
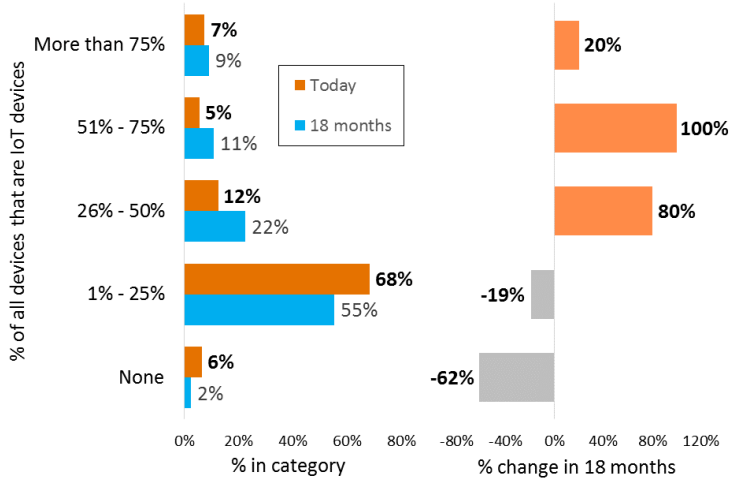


Figure 4: IoT device penetration

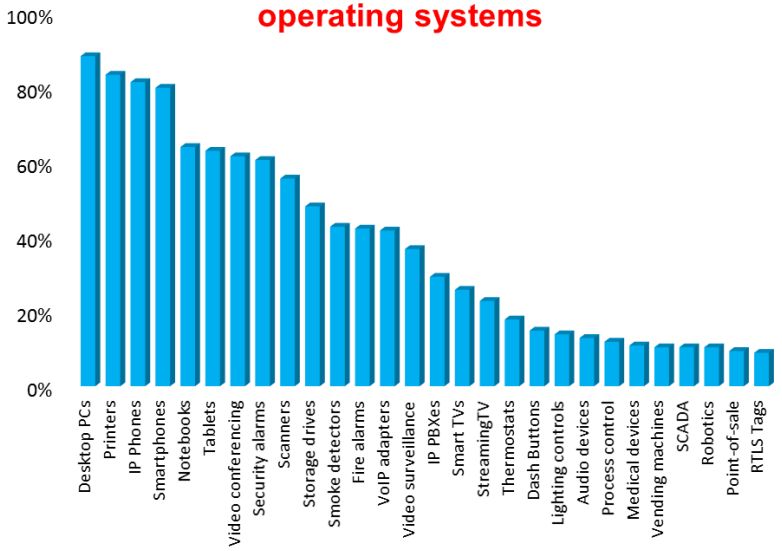


Whilst traditional IT devices (PCs, printers, etc.) are still the most common type of endpoint under management there is a long tail of other devices to contend with (Figure 5). Many will have non-traditional operating systems (see box below) and firmware to support the unusual requirements of *things*, such as low power use and limited memory and/or compute power. Many of these operating systems are open source and can therefore be adapted by device manufacturers leading to many variants.

Example IoT operating systems (OS) and real time OS (RTOS)

TinyOS: for low-power devices such as sensors, wearables and smart meters
Contiki: open source OS for connecting tiny low-cost, low-power microcontrollers
Nano-RK: RTOS for multi-hop wireless sensor networks
FreeRTOS: RTOS kernel for embedded devices and microcontrollers
ARM mbed OS: embedded OS designed specifically for the IoT
RIOT: for memory-constrained systems with a focus on low-power wireless
Mantis: "Multimodal Networks of In-situ Sensors"; OS for wireless sensor networks
Lite-OS: RTOS for use in memory-constrained sensors

Figure 5: The plethora of device types and operating systems



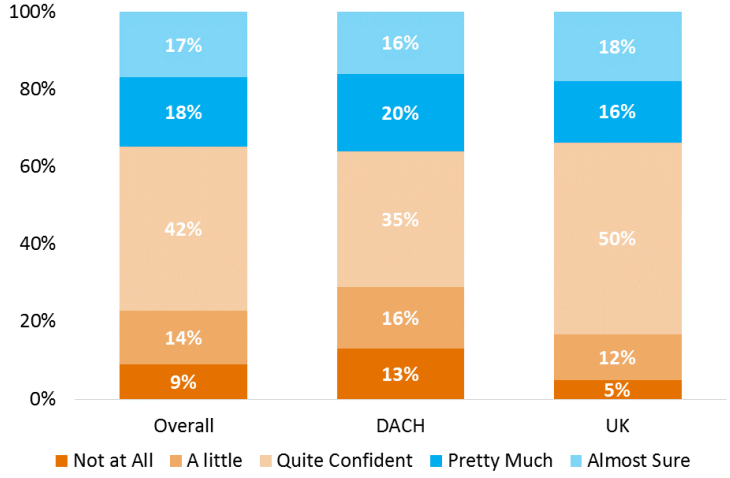
Knowledge of the IoT attack surface

To address IoT security an organisation needs to know what it actually has on its network. Around 35% of respondents say they are already confident they can identify and control all the devices on their network (Figure 6). The remainder – 65% are less sure, 23% have little confidence they are able to do so.

Quocirca expects there is a level of over-confidence as their current view may be coloured by the predominance of traditional IT devices on their networks which they have experience of managing. Unlike user endpoints, many IoT devices are permanently on and connected, making them prime targets for attackers to exploit as network ingress points. As more and more new types of device are attached, confidence may decrease.

Whatever the true confidence levels about knowing and controlling the device access to networks, this can only be achieved with the right tools in place. The

Figure 6: Confidence that all IoT devices connected to networks are identified and controlled



majority of respondents recognise the importance of being able to discover and classify devices (Figure 7) and to be able to do so without the use of agents (Figure 8).

An agent is a small piece of software installed on a device allowing it to be managed. Traditional network management and control tools use agents as they were only dealing with known corporate devices such as employees' PCs and printers. This started to change with the advent of bring-your-own-device (BYOD) and guest networks, whereby employees and visitors respectively request network access for previously unknown devices, which by definition do not have an agent installed. Although much smaller than IoT, BYOD led to the creation of a complete new market for enterprise mobility management products.

Many IoT devices can only become known once they attach to a given network. The proliferation of specialist operating systems can lead to hundreds or even thousands of device/operating system combinations. Most agents will only support a few popular operating systems such as Windows, Android, iOS and OS X, it would be hard to keep up with the portability required beyond this; a problem not faced with agentless management of devices. This need for agentless management is particularly recognised in certain sectors with some of the most unusual devices, such as healthcare.

Figure 7: How important is it to:

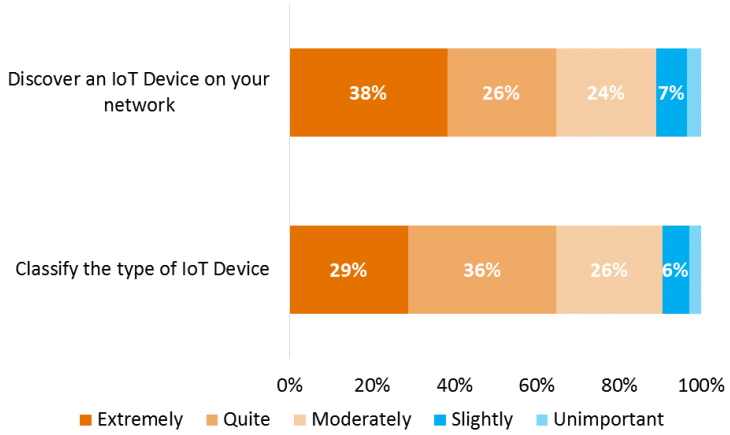
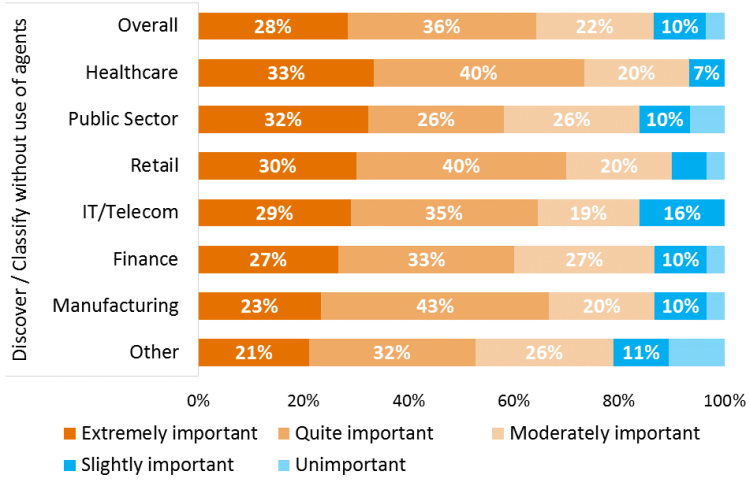


Figure 8: How important is it to *discover/classify without use of agents* BY SECTOR



Taking control of the IoT

The majority (84%) of organisations responding to this survey try to identify some way of controlling and securing IoT devices (Figure 9). However, for 72% the primary control is rudimentary, a network password or a standard control such as WPA2, which requires a key to access a Wi-Fi access point, such approaches provide poor protection compared to the more advanced controls now available. Only 12% rely on a specialised agent, which is subject to the limitations discussed earlier regarding unknown devices and specialist operating systems.

As Figure 10 indicates, 45% of organisations responding to this survey say they have plans to put in place new technology to provide greater control over the endpoints attached to their networks. These plans are highest among those EXPECTANT about the IoT. Even some of the organisations (17%) who see IoT as over-hyped have plans to invest in new technology to see and control what is connected to their network.

There are two primary considerations when selecting the appropriate technology to take control of the IoT:

1. The provision of continuous visibility of what is connecting to networks, both for traditional and IoT devices. Given that many such devices will be unknown, the only practical approach is real-time agentless assessment.
2. The ability to apply automated actions that can be tuned based on a device's classification. This includes controlling how devices are allowed to attach to networks (for example limited to a given subnet and/or via certain hubs), limiting the resources they can interact with, installing or updating software and ensuring a given level of on-device security, as well as logging device activity.

Figure 9: Primary approach to controlling and securing IoT devices

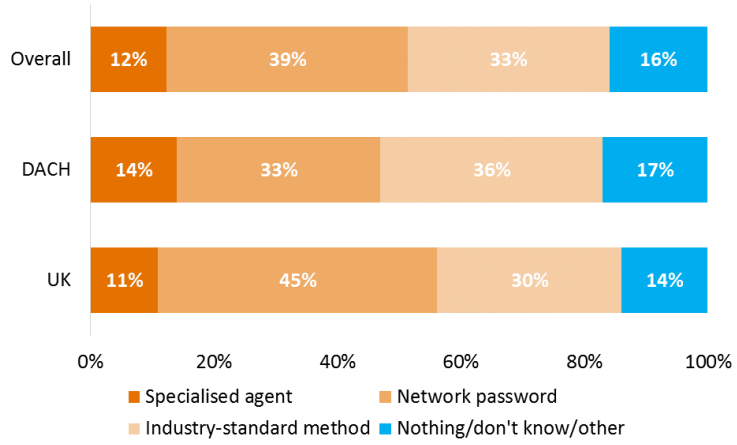
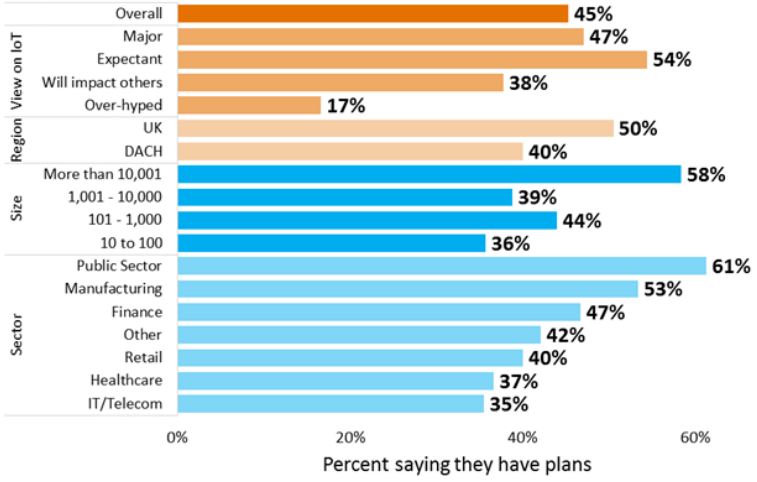


Figure 10: Plans to deploy new technology in the next 18 months to control what attaches to networks



IoT security policy enforcement

Only a third of respondents say they have well-established IoT security policies (Figure 11). The figure is highest in regulated sectors such as financial services, larger organisations and those saying the IoT is already MAJOR for their organisation. The more IoT devices an organisation has, the more likely it is to have IoT security policies, or to be planning them.

Successful IoT applications will often be driven by line-of-business requirements[4] and IT departments need to work closely with the business to ensure success. This will be a challenge for many as the wide-reaching requirements of successful IoT projects already mean getting the various IT functions (networking, security, DevOps etc.) to work together is one of the top IoT security challenges. Only a minority considered too few personnel to be problem, but well over half worry about budgets and the availability of appropriate products (Figure 12).

Cyber-threats are becoming ever more sophisticated and targeted. Cyber-criminals are now the most prolific hackers stealing and selling personal data and intellectual property. All too often, it is only after data has been stolen that the theft is detected. This has led to increased focus on preventative measures to prevent cyber-attacks happening in the first place rather than just the wherewithal to respond to them after damage may already have occurred[5].

To achieve this there is a need for orchestration between different security tools, in order to pre-empt sophisticated threats. Such orchestration enables the enforcement of unified network security policy addressing both traditional and IoT devices. The sharing of security insights between multiple tools is necessary both at the time of initial network access and on-going via continuous real-time monitoring to enable immediate response as the security situation changes.

The knowledge gathered and held about devices and their network activity is an important feed for broader security systems and monitoring tools such as security information and event management (SIEM) and vulnerability assessment (VA) tools, helping to ensure IoT policy is enforceable.

Figure 11: Status of IoT security policy

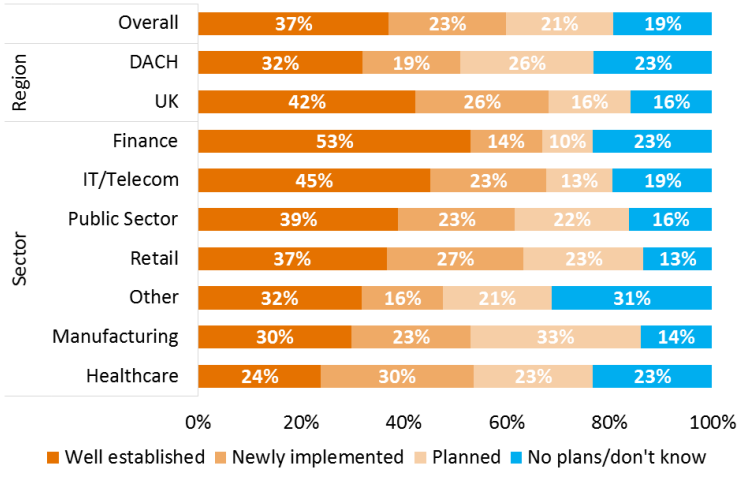
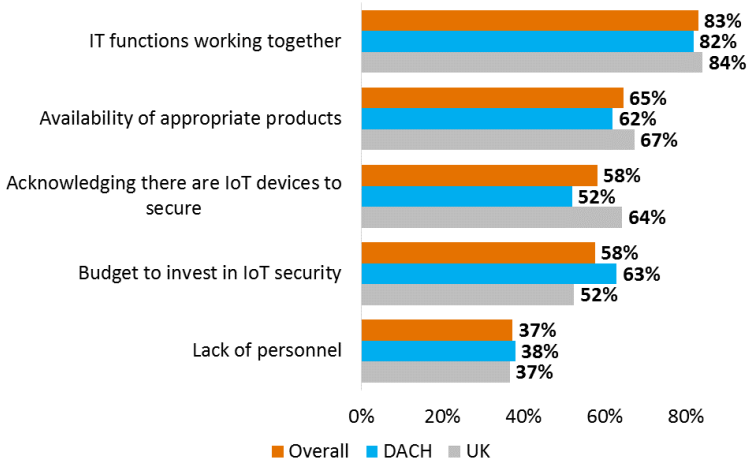


Figure 12: IoT Security challenges



Conclusions

Most organisations recognise the opportunity the IoT represents. However, they also fret about the risk it introduces through an expanded network attack surface. In some cases, the deployment of new IoT applications is being held back. These concerns can be overcome through the deployment of new advanced security technologies.

Better visibility, enabling the discovery and classification of the broad range of *things* involved with IoT deployments without the need for any pre-installed software on the device, is key. This means previously unknown devices and those running unusual operating systems can all be supported. Permanently connected devices that are an integral part of many IoT applications are monitored, managed and secured at all times.

IT security teams need to prepare for a future where they will be charged with securing a greater number and variety of devices than they have been used to in the past. They need to be provided with the means to do this effectively.

Appendix 1 – the U.S. survey

The questionnaire used for the current survey was developed by ForeScout Technologies, Inc. in the U.S. and first completed by 350 attendees in the spring of 2016. The European targets were selected to produce similar coverage of sectors and business sizes as the U.S. survey, except in Europe where organisations with less than 10 employees were not included, whilst these composed 10% of the U.S. sample.

Two questions were added for the Europe version of the survey; the one asking about an organisation's view of the IoT (see Figure 1) and the one asking about the potential number of devices (see Figure 3).

The U.S. survey can be accessed at: https://www.forescout.com/iot-security-survey-results/

Because of the different survey methods used in the U.S. and Europe, comparisons between the two data sets should be guarded, but are of interest. In many areas, the results were broadly similar. The main differences were as follows:

- In the U.S. there were more organisations stating there was currently zero IoT device penetration, this may just reflect some of the very small organisations included. At other end of the scale, penetration was a little higher.
- U.S. organisations were less confident about their ability to identify and control devices on their networks. This difference was too large to be explained by the 10% of very small business in the U.S. and, because European organisations were no more likely to have tools in place (see next bullet), this cannot be explained by technology deployment. U.S. organisations may be more advanced in their understanding of the IoT and, therefore, have become more aware of the challenges.
- Only 15% of U.S. organisations said their primary means for controlling access for devices was a network password compared to 39% in Europe. They were almost twice as likely to have specialised agents installed on devices, suggesting more advanced thinking about IoT, despite the drawback of this approach discussed in this report.
- When it comes to device types, U.S. organisations were about twice as likely to have IP PBXs and VoIP adapters on their networks, they were also ahead when it came to smart TV and streaming TV. European organisations were well ahead when it came to linking up fire alarms and smoke detectors, suggesting a stronger influence on health and safety regulations on IoT plans.

Appendix 2 – Demographics

The European survey involved targeted telephone interviews with senior IT decision makers in 201 organisations based in the UK and German speaking regions (Germany/D, Austria/A and Switzerland/CH, abbreviated to DACH). The break down by company size and business sector is shown in figures 13 and 14

Figure 13: Demographics – countries by size, showing sample numbers

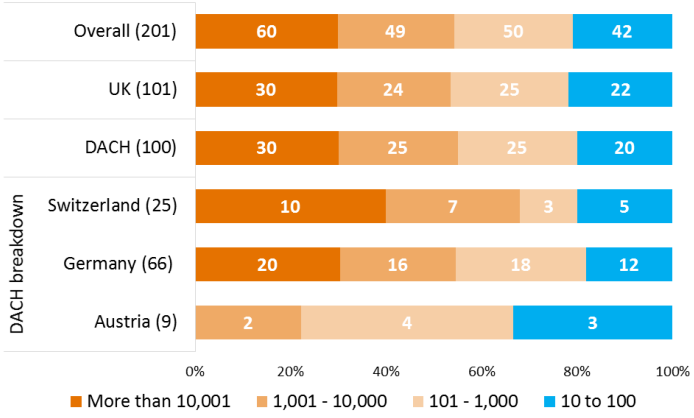
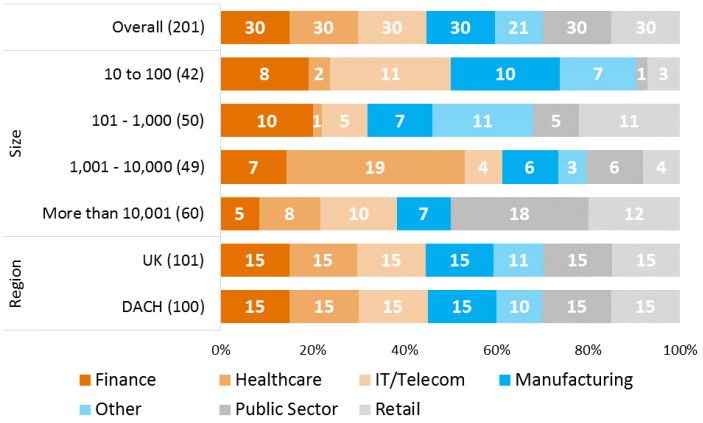


Figure 14: Sectors – by region and size, showing sample numbers



Appendix 3 – Calculations

The actual question asked with regard to number of devices was as follows:

Thinking about your organisation's potential for deploying IoT-related applications and processes over the next 12 months, what is the potential number of devices that could be involved? Include both those attached directly to your network or those that communicate with your organisation from third-party locations:

a) *Fewer than 100 (please specify)*
b) *100 to 999*
c) *1,000 to 9,999*
d) *10,000 to 99,999*
e) *100,000 to 999,999*
f) *More than 1,000,000 (please specify where 2 would equal 200 million)*

To turn the answers in to a mean number of devices for a given set of respondents, the median of each range was taken, e.g. for "100 to 999", the figure was 550 and this was then used to calculate means values.

Appendix 4 – references

1 – Gartner press release, November 10th 2015 http://www.gartner.com/newsroom/id/3165317
2 – Juniper press release, July 28th 2015 http://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020
3 – McKinsey article, December 2014 http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things-sizing-up-the-opportunity
4 – Quocirca, 2015, The many guises of the IoT http://quocirca.com/content/many-guises-iot
5 – Quocirca, 2015, The Trouble At Your Door http://quocirca.com/content/trouble-your-door-targeted-cyber-attacks-uk-and-europe

About Quocirca

Quocirca is a research and analysis company with a primary focus on the European market. Quocirca produces free to market content aimed at IT decision makers and those that influence them in business of all sizes and public sector organisations. Much of the content Quocirca produces is based on its own primary research. For this primary research, Quocirca has native language telephone interviewing capabilities across Europe and is also able to cover North America and the Asia Pacific region. Research is conducted one-to-one with individuals in target job roles to ensure the right questions are being asked of the right people. Comparative results are reported by geography, industry, size of business, job role and other parameters as required. The research is sponsored by a broad spectrum of IT vendors, service providers and channel organisations. However, all Quocirca content is written from an independent standpoint and addresses the issues with regard to the use of IT within the context of an organisation, rather than specific products. Therefore, Quocirca's advice is free from vendor bias and is based purely on the insight gained through research, combined with the broad knowledge and analytical capabilities of Quocirca's analysts who focus on the "big picture". Quocirca is widely regarded as one of the most influential analyst companies in Europe. Through its close relationships with the media, Quocirca articles and reports reach millions of influencers and decision makers. Quocirca reports are made available through many media partners.

To see more about Quocirca's analysts, click here

To see a list of some of Quocirca's customers, click here

To contact Quocirca, please click here.