25 March 2021

Literature review on connected devices within enterprise networks

Ipsos MORI

Ipsos MORI

Contents

List of figures

List of tables

Executive Summary

Connected devices are used within the daily operation of thousands of organisations around the UK. However, vulnerable devices can provide a route for hostile actors to attack enterprise systems. Evidence of prior exploitation and attacks demonstrates that insecure IoT is not simply a threat to the individual user or corporate network into which it is connected. It can actually represent a large-scale strategic risk to the overall digital environment, and in this sense IoT security is not simply a matter of individual or organisational need – it is a public need and a public good.

This report investigates relevant literature with the initial aim of exploring three issues:

- which sectors' large organisations are using the highest total number of connected devices within their networks;
- which connected device categories are deployed in the highest numbers within the sectors;
- how enterprise device deployment differs from how consumers typically use consumer connected devices.

In practice, the lack of available evidence constrains the ability to look at specific sectoral usage in a detailed manner. A potentially significant issue that the current analysis is not yet able to reflect upon is the impact of the COVID-19 pandemic. It is likely that the pandemic-prompted upsurge in homeworking will have accelerated the trends observed in this report, particularly in terms of homeworking occurring within environments surrounded by potentially insecure consumer IoT devices on the same networks. This issue is likely to require further study in the relatively near future. However, the review is nonetheless able to offer a number of relevant insights into enterprise usage of connected devices and their overall prevalence in a cross-sector context.

Key findings from the current review are summarised as follows:

- Connected device adoption in organisations is significant. The vast majority have deployed them and/or plan to extend their usage, with only around 10% having no IoT adoption plans.
- Cyber security represents the primary area of related concern. While some organisations view it as a barrier to growth, many are extending their deployments in spite of the concern. In parallel, various reported incidents demonstrate that security concerns are valid and result in genuine impact.
- Many sanctioned enterprise deployments of connected devices are based upon potentially vulnerable consumer grade technologies. Such deployments include devices directly purchased by the enterprise as well as via permitting use of employees' personal devices within the enterprise network.
- Organisations face a significant challenge from the volume of *unsanctioned* connected device deployments, with the resulting 'shadow IoT' introducing vulnerabilities that may remain unseen by enterprise IT teams.
- Connected devices have a significant presence across numerous sectors and vertical industries, including an inevitable overlap into the use of consumer-grade technologies. While

further primary data collection would provide more detailed insight into the specifics of usage, it is clear that many existing deployments will include vulnerable technologies.

Enterprise usage of connected devices is driven by different needs to those of consumers, but the use of the same technologies can result in larger scale deployments being based upon vulnerable foundations. The risk is further amplified if these are then integrated within wider enterprise applications and processes.

The review is supported by extensive reference to sources, encompassing both the latest research and findings, and studies relating to consumer connected devices and enterprise IoT adoption.

1 Introduction

Connected devices are used within the daily operation of thousands of organisations around the UK. Vulnerable devices in these environments can end up being used as routes for a hostile actor to attack enterprise systems because they contribute to existing issues within large organisations, such as device management and site maintenance practices. The first step towards improving the resilience of UK enterprises is to identify via a literature review how consumer-grade and enterprise-specific IoT devices are deployed within large organisations' networks.

1.1 Objectives and scope

The three objectives of the review are to:

- conduct a mapping of relevant literature to determine which sectors' large organisations are using the highest total number of connected devices within their networks;
- identify through literature - within each relevant sector identified above - which connected device categories are deployed in the highest numbers;
- identify through literature how enterprise device deployment differs from how consumers typically use consumer connected devices.

For the purposes of this literature review, the IoT devices that are particularly considered within scope are as follows:

- Smart locks
- Smart lighting
- Smart alarms
- Smart thermostats
- Smart TVs
- Smart speakers/assistants
- Smart wearables/trackers
- Network-connected printers
- Smart smoke/CO detectors
- Smart entry sensors
- Smart appliances
- Network-connected cameras
- SOHO-grade routers
- Network-attached storage

1.2 Methodology

A review of publicly available literature online was conducted in March 2021. The scope of the review was open in terms of candidate sources, with academic papers, international government papers, think tank reports, relevant charity/non-profit publications and corporate documents (e.g., research papers from cyber security companies) all eligible for inclusion.

A range of terms were used in order to constrain the search to identify relevant sources, such as:

- *Device-related terms,* e.g. ‘consumer connected device’, ‘consumer IoT’, ‘IoT device’, ‘smart device’;

- *Enterprise-related terms*, e.g. ‘business’, ‘enterprise’ and ‘workplace’.

Examples of resulting search strings were combinations such as ‘“consumer IoT” enterprise’, ‘“consumer IoT” workplace’, ‘”IoT device” enterprise’ and ‘“smart device” workplace’. It was not intended (or necessary) to use all combinations of terms exhaustively, as many permutations tended to lead to the same sources in practice. A specific search was also conducted for ‘shadow IoT’ in recognition of this representing a particular route by which consumer devices could enter the enterprise. In addition, further searches were conducted in order to supplement the overall findings with sector-specific evidence, e.g. ‘healthcare IoT’, ‘manufacturing IoT’, ‘retail IoT’.

Further searches were planned in order to identify sources relating to security issues and guidelines, however this ultimately proved unnecessary as such sources were highlighted as a natural consequence of searching for the more general consumer IoT materials.

In order to ensure relevance and currency, the review had a cut-off point of 2016. Even here the older sources dating near to 2016 tended to relate to materials such as guidelines and standards, whereas the majority of available evidence relating to device usage tended to be drawn from 2018 onwards. This report was reviewed by Ciaran Martin, former CEO of the National Cyber Security Centre and currently Professor of Practice in the Management of Public Organisations at the Blavatnik School of Government, to provide helpful insight.

1.3 Availability of evidence

Although the scope of the review was not constrained in terms of eligible sources, it quickly became apparent that the majority of relevant materials were to be found in industry-focused reports as opposed to academic sources. One contributing reason for this was that industry organisations were in a position to draw data from their customer and user communities, providing them with a direct evidence base in relation to the scale and nature of connected device usage in practice. As such, these sources tend to be the primary reference point for evidence and commentary within this review. They have been informed by sources from governments and standards bodies (in relation to highlighting relevant guidance and national initiatives) and technology news sources (in relation to details of relevant reported incidents and the like).

In terms of addressing the three specific objectives of the review, an examination of the IoT landscape quickly reveals that there is no shortage of studies and surveys that address the topic in some way. However, a more targeted assessment also reveals that these vary significantly in focus and perspective. There is ample evidence to suggest that IoT is being adopted in the workplace, and so it is easy to show that IoT has a strong presence in large organisations. However, few large studies have documented a sector-based analysis – there are various that report having surveyed organisations across different sectors, but the subsequent presentation of results tends not to be offered on a sector basis. Similarly, there is some evidence that comments upon the particular types of devices and uses involved, but the level of detail and the categorisation of devices is variable (e.g. many refer to broad categories of use - such as Industrial IoT or environmental sensors - rather than highlighting specific types of device).

There is also a wealth of information that covers the general use of consumer IoT, and some that comments upon the use of consumer-grade devices in the workplace. However, the workplace coverage is typically addressed at a general level (e.g. the risk of 'shadow IoT' based on consumer devices), rather than calling out specific types of device or the sectors that are using them. As such, the resulting situation is that there are few sources that provide reliable direct evidence that sits in the intersection of the target topics. This unfortunately limits the extent to which it is possible to draw definitive conclusions in relation to the objectives of the review.

It is also worth noting that there was a lack of UK-specific data to draw from, and as such the review draws upon international sources across all elements of the discussion. Having said this, much of the non-UK evidence is drawn from US sources, and US experiences are typically viewed as a good proxy for likely experience in the UK as well. Equally, where findings are drawn from or applicable to particular countries, this is appropriately highlighted in the accompanying text.

2 Background

This section aims to set the scene for the discussion as a whole by presenting some illustrative evidence of the level of adoption of IoT devices within enterprise contexts. At this stage, the focus is not placed exclusively upon consumer level devices, as these are not being specifically highlighted within the reported figures. However, as later discussion will indicate, such devices can be expected to represent a tangible sub-group within the numbers reported.

2.1 Enterprise adoption of IoT connected devices

There is ample published evidence to suggest that IoT adoption and use within enterprises is the norm rather than the exception. Illustrative of this are the following three reports from recent years:

- The extent of IoT adoption plans was clearly reflected in the responses from the 416 (predominantly North American) respondents to a 2017 'state of the industry' survey from James Brehem & Associates[1], with only 12% indicating no IoT plans. Meanwhile, half (51%) had *already* deployed IoT, and the remainder were at varying stages of advancement on the route of piloting or planning its use.

- A survey of commercial adoption from the Eclipse Foundation (based upon 366 global respondents) determined that only 10% of organisations had no plans at all to deploy IoT solutions (by contrast, 39% had already deployed IoT, 22% had plans to do so within 2 years, and 29% were unsure of their plans)[2].

- A 2019 study conducted by PwC that surveyed approximately 1,000 business executives in the US revealed that a significant majority had IoT-related projects in progress[3]. Specifically, 19% reported that they had fully integrated IoT with other technologies across their organisation, and a further 45% indicated that they had begun to do so and had plans to go further. An additional 26% had not performed any IoT integration at the time of the survey, but planned to do so, leaving only 10% with no IoT integration and no related plans. At the same time, their deployments were not without concerns, with almost half indicating that their progress had been slowed as a result of concerns around cyber security (48%) and privacy (46%).

Figure 1 presents the level of growth in worldwide IoT spending that was predicted for 2020, contrasting the expectations across different industry sectors, as well as against growth in consumer IoT device usage[4]. These predictions were made mid-year and show growth in almost all sectors despite the COVID-19 pandemic (the exception being personal and consumer services, which includes hotels and cinemas, which would clearly have been amongst the most impacted). The pandemic itself is likely to have delayed plans for deployment in offices and wider workplace contexts, but at the same time is likely

1 James Brehem & Associates. 2017. *The Connected Conversation: 2017 IoT State of the Industry Survey*. 25 January 2017. https://www.jbrehm.com/blog/2017/1/25/the-connected-conversation-2017-iot-state-of-the-industry

2 Eclipse IoT. 2020. IoT Commercial Adoption Survey 2019 Results. Eclipse Foundation, Inc. March 2020. https://iot.eclipse.org/community/resources/iot-surveys/assets/iot-comm-adoption-survey-2019.pdf

3 PwC. 2019. 2019 IoT Survey: Speed operations, strengthen relationships and drive what's next. https://www.pwc.com/us/en/services/consulting/technology/emerging-technology/iot-pov.htmly

4 IDC. 2020. "Worldwide Spending on the Internet of Things Will Slow in 2020 Then Return to Double-Digit Growth, According to a New IDC Spending Guide", IDC press release, 18 June 2020. https://www.idc.com/getdoc.jsp?containerId=prUS46609320

to have resulted in more deployment within people's homes (as well as an accompanying increase in people homeworking alongside existing, potentially insecure, home IoT devices).

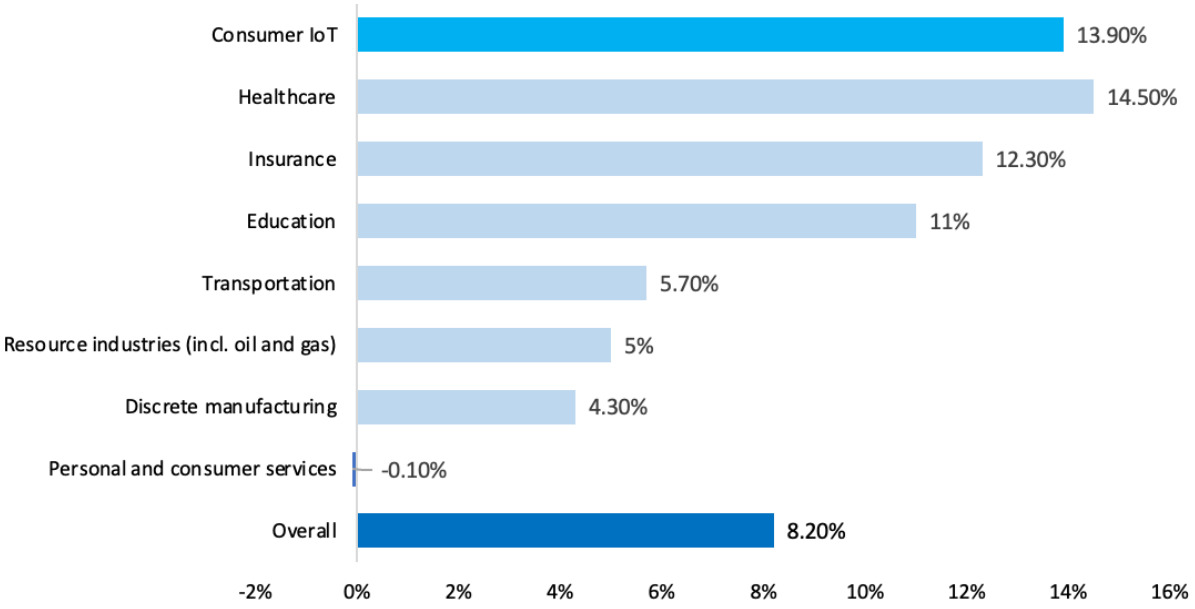


Figure 1: Predicted growth in worldwide IoT spending during 2020

The adoption trend is the underlying focus of a 2018 report from Abrua, which comments on how employee behaviours and expectations are accelerating the consumerisation of the workplace[5]. The findings are based on a global study of 7,000 employees across 15 countries, and draw on data from organisations across industrial, government, retail, healthcare, education, finance, and IT/technology/telecommunications sectors. While it does not further disaggregate the results by organisation size, location or sector, the report highlights that IoT technologies are blurring the distinction between technologies that are traditionally managed by an organisation's IT function and its Facilities team. In particular, respondents indicated that IoT-driven technologies were being used for automated temperature controls and lighting (24%), voice-activated and wireless conference room AV technology (23%), and bespoke corporate mobile apps offering location-based information (23%). By way of comparison to more established technologies, 82% of organisations were using Wi-Fi. The report also makes an interesting observation that the consumerisation of technology is creating an increased appetite and expectation for digitally-enabled workplaces.

5 Aruba. 2018. *The Right Technologies Unlock the Potential of the Digital Workplace*. https://www.arubanetworks.com/assets/eo/Aruba_DigitalWorkplace_Report.pdf

2.2 Security implications of IoT adoption

While the surveys above demonstrate the significant extent of IoT adoption within enterprises, it is notable that this was not happening in the absence of related concerns. More connected devices means more potential points of entry into enterprise networks, leading to the:

- compromise of enterprise data and wider systems through lateral movement
- failure of those connected devices, causing disruption to businesses

In parallel with highlighting the scale of adoption, studies typically tend to highlight security as the most prominent concern.

The earlier text already mentioned the concerns raised in the PwC survey, and it is relevant to highlight how it was reflected in several other sources as well.

- Respondents in the 2019 study from Eclipse Foundation cited 'Data Security' as the topmost area of concern or priority in deploying an IoT solution, cited by 26% of respondents[6]. This placed it ahead of 'Performance' and 'Data Collection & Analytics' as the primary concern for other respondents, cited by 19% and 17% of them respectively.

- Taking a different perspective, a 2019 survey from technology distributor Farnell gathered 2,015 global responses primarily from what it characterised as "engineers of IoT solutions"[7]. Security was notably in the responses to two questions. When asked about their key concerns, security topped the list, with 35% of respondents citing it (ahead of connectivity, interoperability and ecosystem, with 27%, 25% and 13% respectively). Equally, however, security was also recognised as the most important consideration when developing IoT solutions, cited by 47% and ahead of communication reliability (23%), ecosystem (13%), edge device reliability (10%), and ease of data review/analysis (7%).

- The 2017 State of the Industry findings from James Brehem & Associates drew upon respondents with a wide range of roles within companies from across the IoT ecosystem (including executives, strategy, marketing, sales, IT and engineering roles), but the findings were again consistent with others in showing security as the primary area of concern[8]. In this case respondents were asked to cite 'Barriers to growth in IoT', with two-thirds (65%) flagging security. This placed it ahead of 14 other named issues (including cost, interoperability, lack of expertise, and management buy-in) and it was notably the *only* topic that more than half of the respondents believed to be a barrier.

- A 2020 study from Vodafone (based on a global survey of 1,639 businesses) interestingly framed things in a slightly different way[9]. While the vast majority recognised security as an issue, 84% viewed it as an issue to be overcome and only 18% cited it as actually being a barrier to IoT deployment (and indeed, 74% indicated that their IoT security concerns were no

6 Eclipse IoT. 2020. IoT Commercial Adoption Survey 2019 Results. Eclipse Foundation, Inc. March 2020. https://iot.eclipse.org/community/resources/iot-surveys/assets/iot-comm-adoption-survey-2019.pdf

7 Farnell. 2020. *Farnell IoT Survey 2019*. February 2020. https://uk.farnell.com/global-iot-survey-2019

8 James Brehem & Associates. 2017. *The Connected Conversation: 2017 IoT State of the Industry Survey*. 25 January 2017. https://www.jbrehm.com/blog/2017/1/25/the-connected-conversation-2017-iot-state-of-the-industry

9 Vodafone. 2020. *IoT Spotlight Report 2020*. Vodafone Business. https://www.vodafone.com/business/news-and-insights/white-paper/iot-spotlight-2020

greater than their concerns around other new technologies). This gives a sense of overall perspective that is arguably missing from other accounts that look at IoT security in isolation and do not view it in context alongside other aspects of security. Essentially, it highlights that IoT security *is* important, but that is because *security* is important in general, and so IoT is not going to be an exception.

These findings clearly suggest that (in principle at least) security concerns are not going unrecognised and are often uppermost in the minds of those deploying the technologies. At the same time, other evidence would seem to suggest that security concerns are well-founded. For example, 2017 findings from Hewlett Packard Enterprise indicated that 84% of IoT adopters had *experienced* a security breach and 93% of executives *expected* IoT security breaches in future[10]. In both contexts, malware was the most prominent threat type (cited as having been experienced by 49% of adopters, and anticipated by 56% of executives), followed by spyware (experienced by 38% and anticipated by 50%). Meanwhile, a 2019 study from Gemalto, based on a global survey of 950 IT and business decision makers, indicated that only 48% of businesses considered themselves able to detect if any of their IoT devices experienced a breach[11]. Interestingly, the respondents appeared to lay responsibility for this at the door of IoT manufacturers, with 62% indicating that security efforts from the IoT industry need to improve and 79% were looking for more robust guidelines on IoT security.

[10] Ashton, K. 2017. *Making sense of IoT: How the Internet of Things became humanity's nervous system*. Hewlett Packard Enterprise. http://engage.arubanetworks.com/LP_REG_510245507_510245507_ARUBA_WW_EN-US

[11] Moore, B. 2019. "Half of companies unable to detect IoT device breaches", SecurityBrief, 19 January 2019. https://securitybrief.eu/story/half-of-companies-unable-to-detect-iot-device-breaches

3 Consumer connected devices in enterprises

This section draws the focus specifically towards the types of consumer level devices that underpin the main objectives of the review, and attempts to uncover evidence of their adoption in enterprise settings. It should be noted that the level of detail that it is possible to present is limited by the literature sources, insofar as there is relatively little comparative evidence that considers the different categories of devices in use. Moreover, some sources tend to blur their discussion of consumer IoT devices with the use of personal devices and BYOD (Bring Your Own Device) scenarios.

One dimension that the review has *not* sought to address here is the impact of the COVID-19 pandemic. The prolonged period of enforced homeworking will have meant that domestic environments indirectly became part of the enterprise, with work occurring via consumer-grade routers and networking equipment and staff, and their families, potentially using their own smart technologies on the same networks[12]. However, attempting to encompass this within the current report would essentially confuse the interpretation of enterprise usage, and it would be preferable to reflect upon any resulting impacts from the standpoint of a post-pandemic period (i.e. when any longer-term and lasting impacts can be identified).

3.1 Modes of use of connected devices within enterprise contexts

An important distinction to consider in terms of the use of connected devices within an enterprise is the mode in which they are being used – has the enterprise itself invested in them, or is the use occurring from the perspective of sanctioned or unsanctioned use by individual staff members.

A 2019 study from NCC Group identified three specific categories of consumer IoT that are being adopted in enterprise environments: IP-connected cameras, Smart Assistants, and Smart TVs[13]. While it did not put specific figures to the respective levels of adoption, nor consider relative usage across different sectors, the report did highlight a range of potential security and privacy questions that adopters ought to be considering. For example, questions that organisations ought to be asking include:

- If the devices are capturing recordings (e.g. video from cameras, audio of user requests to smart assistants) are these stored and if so where?
- Do the devices have security features and are they configurable?
- To what extent have the devices been tested from a security perspective and is there any baseline security information available?
- What networks are the devices going to connect to, and to what extent will they connect to and integrate with employees' BYOD devices (e.g. smartphones)?

These questions would, of course, be relevant in the context of adopting enterprise-grade devices as well, but with more of an underlying expectation that they would have been considered from an

[12] NCSC. 2020. "Home working: preparing your organisation and staff", National Cyber Security Centre, 17 March 2020. https://www.ncsc.gov.uk/guidance/home-working

[13] Garcia, L. 2019. *Security Impact of IoT on the Enterprise*. NCC Group, November 2019. https://www.nccgroup.trust/globalassets/our-research/uk/whitepapers/2019/11/iot-whitepaper-matt.pdf

enterprise deployment perspective within the design of the devices. This is likely because they are inherently more likely to interact with existing enterprise device management systems or include enterprise-specific protocols and technologies.

In addition to intentional deployments (i.e. the organisation making a conscious decision to deploy a consumer-grade technology as part of their infrastructure), there are also two further – and potentially overlapping - guises in which consumer IoT can enter the workplace:

- **Personal devices**: employee-owned devices that may connect to organisational networks or systems within them.
- **Shadow devices**: technology devices being used in a business context that the IT department is unaware of.

The first category implies that the use of such devices is recognised (and at least implicitly sanctioned) by the organisation.

One of the most direct reports of 'non-business' device usage comes from Palo Alto Network's 2020 report on the connected enterprise. The findings are based upon responses from 1,350 IT business decision-makers (from 14 countries across Asia, Europe, the Middle East and North America)[14]. Of these, 89% had seen an increase in IoT devices on their networks, and Figure 2 illustrates and compares the particular results that were reported in relation to non-business devices.

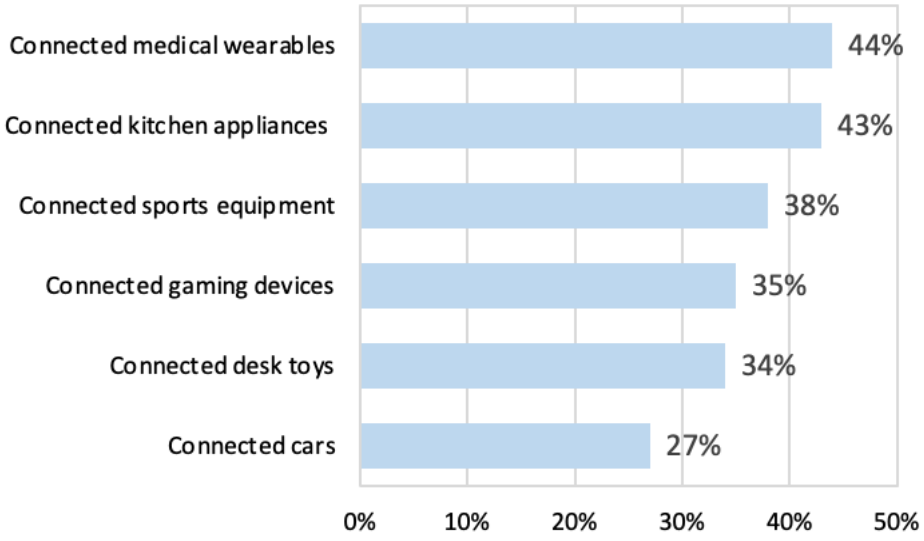


Figure 2: Reported use of non-business devices on enterprise networks

However, the extent of usage is not accompanied by a similar degree of confidence in the level of security. Only 4% of respondents felt they had no need to improve current IoT security practices, while 58% considered there was a need for significant improvement or a complete overhaul.

[14] Palo Alto Networks. 2020. The Connected Enterprise: IoT Security Report. September 2020. https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/research/connected-enterprise-iot-security-report-2020

According to 2018 findings from Infoblox, 35% of companies in the US, UK and Germany reported more than 5,000 non-business devices connecting to the network each day[15]. Moreover, US and UK employees report using personal devices while connected to the enterprise network for a range of non-work activities (with 39% accessing social media and downloads of apps, games and films from 24%, 13% and 7% respectively).

Taken directly from the Infoblox report, Figure 3 depicts the overall findings relating to the number of devices in each category.

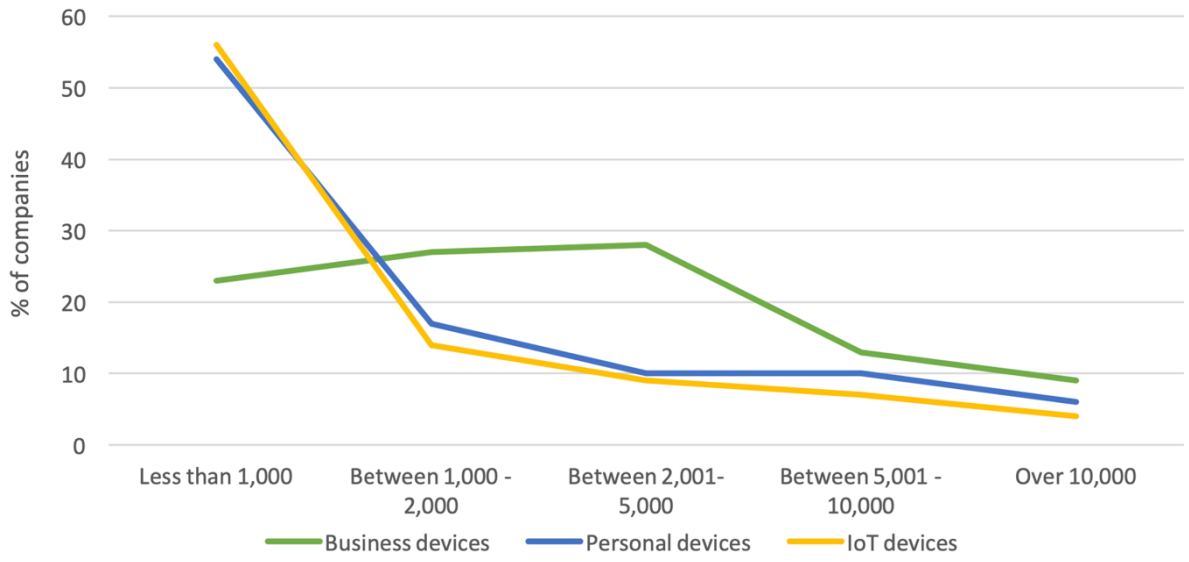


Figure 3: Number of devices connected to enterprise networks (Source: Infoblox, 2018)

[15] Infoblox. 2018. *What is Lurking on Your Network: Exposing the threat of shadow devices*. https://www.infoblox.com/wp-content/uploads/infoblox-report-what-is-lurking-on-your-network.pdf

The study also identified the most common devices found in enterprise networks, the results of which are summarised in Figure 4.

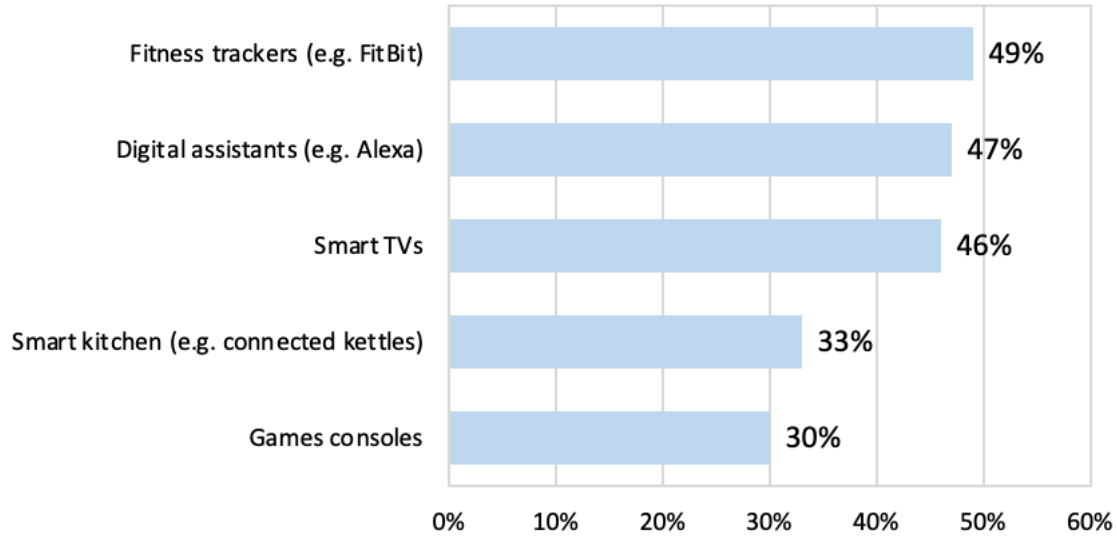


Figure 4: Non-business IoT devices found in enterprise networks

Shadow IT (also known by other names, such as feral, rogue and stealth IT) has been a long-recognised area of risk, and essentially refers to the use of devices, software, and services without the approval of the IT department. The growth of IoT technology has led to an accompanying rise in shadow deployments of these devices as well. In terms of how to interpret the issue for the context of this review, it should be noted that while *shadow* IoT does not automatically equate to *consumer* IoT, it is highly likely that most shadow deployments are going to be based on consumer grade technologies.

Following on from their 2018 study, Infoblox published a report in 2020, with findings indicating that only 20% of IT leaders had *not* found any shadow IoT devices on their networks[16]. Meanwhile, as illustrated in Figure 5, the majority were finding between 6 and 50 devices having been connected without authorisation.

[16] Infoblox. 2020. *What's Lurking in the Shadows 2020? Exposing how IoT devices open a portal for chaos across the network.* https://www.infoblox.com/wp-content/uploads/infoblox-whitepaper-whats-lurking-in-the-shadows.pdf

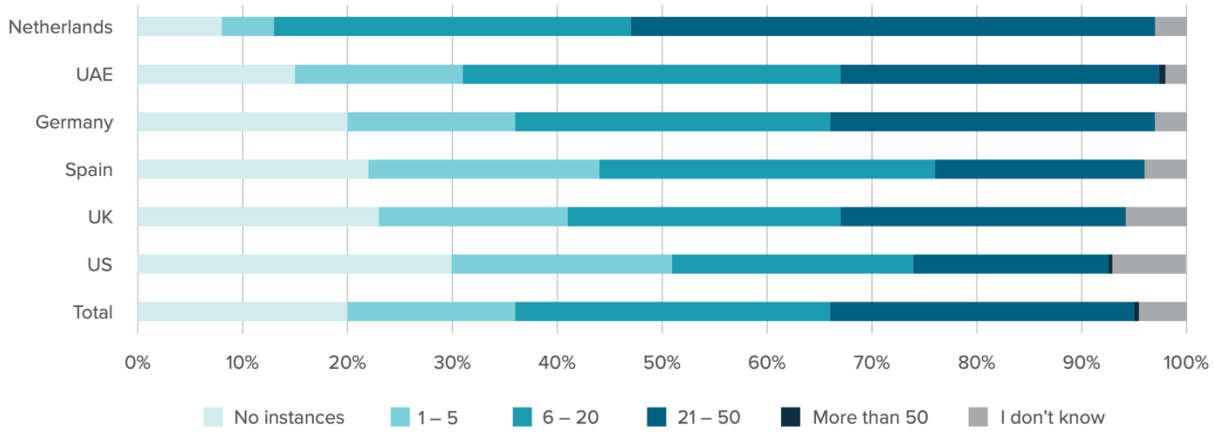


Figure 5: Number of instances of shadow IoT devices discovered within enterprise networks (Source: Infoblox, 2020)

Some further and final evidence comes from Zscaler, who measured the traffic volumes originating from different IoT device types within the enterprise and found that consumer-grade devices were the most prominent[17]. The findings are presented in Figure 6, based on a sample of almost 500 million transactions taken from over 2,000 organisations in a two-week period. The total sample encompassed 553 IoT devices falling into in 21 categories, but the representation in the chart focuses on the most prevalent ones that Zscaler themselves have highlighted as consumer IoT[18]. However, within the 'other' category are further devices that would potentially (or explicitly) be expected to include consumer grade examples, including "Printer" (4%), "IP Camera" (1.8%), "Digital Home Assistant" (0.7%), and "Smart Home" (0.7%).

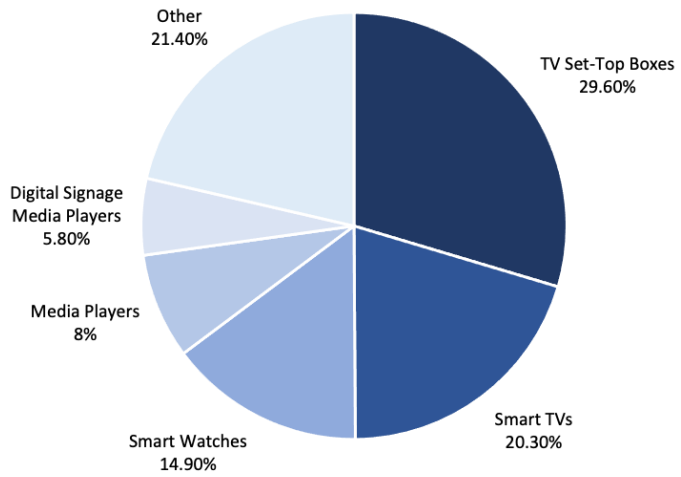


Figure 6: Prevalence of IoT devices in the enterprise by traffic volume

17 Zscaler. 2020. *IoT in the enterprise 2020: Shadow IoT emerges as security threat*. Zscaler ThreatLabZ, February 2020. https://info.zscaler.com/resources-industry-iot-in-the-enterprise

18 Zscaler. 2020. *What Things Are in Your Network? IoT in the Enterprise 2020*. Zscaler Infographic. https://www.zscaler.com/resources/infographics/IoT-report-2020.pdf

Having established clear evidence that consumer connected devices are in use, this links to a follow-on issue of how they have been deployed. Indeed, the earlier-cited NCC report raises the question of how the devices have been secured and whether they are connected to the main network or segregated on their own network with or without Internet access. This is supported by specific evidence from the Palo Alto networks study, which reports a lack of segmentation[19]. A quarter of respondents (24%) indicated that their IoT devices were not segmented into separate networks from their primary business devices and applications, and only a fifth (21%) indicated that they had applied micro-segmentation in order to isolate and control the devices more tightly.

3.2 Security challenges of consumer IoT devices

A clear concern is that consumer-grade IoT devices have not been specifically designed and implemented with enterprise usage in mind and may consequently fall short in terms of the provisions that may be expected – including security. As an illustration of this, NIST has established the potential weaknesses of consumer-level IoT devices, with a 2019 study having documented a technical review of the security features to be found across a range of device categories (including TVs, plugs, bulbs, and security devices)[20]. The review examined the provision and sufficiency of the security features, identifying a number of common themes across multiple categories of device, including:

- Weak passwords permitted on companion mobile apps and websites;
- Open network ports, offering opportunity to attackers;
- Potential for man-in-the-middle attacks between the devices and companion apps running on mobile devices; and
- Lack of updates for known vulnerabilities.

Without attention, the same vulnerabilities would persist with the deployment of such devices in organisational contexts (noting that the NIST study was ultimately expressing concern even in the context of domestic deployments). One of the key concerns for organisations adopting consumer connected devices should therefore be the extent to which they could add to external visibility and exposure. Search engines such as Shodan[21] or Censys[22] provide an easy means of both discovering connected devices and identifying the services they are running and potential vulnerabilities. While this does not equate to gaining access, it is a first step and can assist potential attackers in homing-in on devices within organisational networks that may be targeted for vulnerabilities. There is ample evidence of Shodan being used to uncover vulnerable (often wide open) devices, falling into both consumer and non-consumer categories, with access often enabled via default passwords (or a complete lack of

19 Palo Alto Networks. 2020. The Connected Enterprise: IoT Security Report. September 2020. https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/research/connected-enterprise-iot-security-report-2020

20 Fagan, M., Yang, M., Tan, A., Randolph, L. and Scarfone, K. 2019. *Security Review of Consumer Home Internet of Things (IoT) Products*. Draft NISTIR 8267, National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8267-draft

21 Shodan bills itself as “the world's first search engine for Internet-connected devices” and can be accessed via https://www.shodan.io.

22 Censys can be accessed via: https://censys.io/

authentication). It has even prompted a practice called 'Shodan Safari', where hackers share images of their finds on Twitter[23].

There are various instances of specific vulnerabilities being discovered. For example, there have been several instances of unintentional data leakage via smart TVs[24] and smart assistant devices[25], which could in turn provide a basis for an espionage risk. Meanwhile, there are also instances of vulnerable connected devices being harnessed and used to attack others:

- One of the most widely-known examples of an IoT breach was the Mirai botnet in 2016. This was first discovered in August and then used to launch a series of Distributed Denial of Service attacks in subsequent months. The Mirai malware compromised vulnerable IoT devices and enlists them as bots used to attack other targets. Amongst the most notable resulting events was the attack against the service provider Dyn, which was targeted and put out of action on 21 October 2016[26]. This in turn led to outages for various online services (including leading providers such as Reddit, Spotify and Twitter)[27], demonstrating that the ultimate impact of the Mirai attack was significantly more widespread (and felt by a far wider community of users) than just Dyn as the direct target.

- In 2019, security firm Imperva released details of a Distributed Denial of Service attack that lasted 13 days and involved a botnet coordinating 402,000 IP addresses. Most of the sources involved were judged to be infected IoT devices. Reflecting upon the attack and its similarity to the vulnerabilities exploited by Mirai, Imperva observed that "since 2016, many new IoT vendors have entered the market (and) few have learned from the security mistakes of the past. As a result, today IoT devices are used in most of the large botnets we have seen"[28].

These incidents are indicative of a notable wider issue - insecure IoT is not just a threat to the individual user or corporate network into which it is plugged. It can actually represent a large-scale strategic risk to the overall digital environment.

While Mirai is arguably still the most well-known example of IoT-related malware, there has been significantly more evidence of activity targeting this space. As another specific example, VPNFilter[29] was notable in that it targeted SOHO-grade equipment and yet simultaneously contained code to control Industrial Control Systems. This implied that the attacker knew that they could pivot from consumer-grade kit into more valuable devices within networks. There has also been a general increase in IoT

[23] Whittaker, Z. 2019. "Shodan Safari, where hackers heckle the worst devices put on the internet", TechCrunch, 21 January 2019. https://techcrunch.com/2019/01/21/shodan-safari/

[24] Roberts, J. 2017. "Is your smart TV spying on you? All you need to know about smart TVs and your privacy", Trusted Reviews, 8 February 2017. https://www.trustedreviews.com/news/smart-tv-privacy-problems-vizio-samsung-lg-sony-panasonic-2952175

[25] Gartenberg, C. 2019. "Apple's hired contractors are listening to your recorded Siri conversations, too", The Verge, 26 July 2019. https://www.theverge.com/2019/7/26/8932064/apple-siri-private-conversation-recording-explanation-alexa-google-assistant

[26] Williams, C. 2016. "Today the web was broken by countless hacked devices – your 60-second summary", The Register, 21 October 2016. https://www.theregister.com/2016/10/21/dyn_dns_ddos_explained/

[27] Etherington, D. and Conger, K. 2016. "Large DDoS attacks cause outages at Twitter, Spotify, and other sites", TechCrunch, 21 October 2016. https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/

[28] Simonovich, V. 2019. "Imperva Blocks Our Largest DDoS L7/Brute Force Attack Ever (Peaking at 292,000 RPS)",Imperva, 24 July 2019. https://www.imperva.com/blog/imperva-blocks-our-largest-ddos-l7-brute-force-attack-ever-peaking-at-292000-rps/

[29] Hilt, S. and Merces, F. 2021. "VPNFilter Two Years Later: Routers Still Compromised", Trend Micro, 19 January 2021. https://www.trendmicro.com/en_us/research/21/a/vpnfilter-two-years-later-routers-still-compromised-.html

malware more broadly. For example, Kaspersky Lab[30] reported a significant growth in malware samples for IoT devices from 2016 to 2018, increasing from 3,219 in 2016 to 121,588 during the first half of 2018[31]. Further findings from Kaspersky the following year indicated a significant increase in resulting attacks on smart devices. While the first half of 2018 had seen 12 million attacks from 69,000 distinct IP addresses, the first half of 2019 saw this increase to 105 million attacks from 276,000 distinct addresses (the report also noted that Mirai malware was still the underlying cause in 39% of cases)[32].

Meanwhile, moving away from malware-based exploitation, in 2019 Microsoft reported the discovery of attempts "*to compromise popular IoT devices (a VOIP phone, an office printer, and a video decoder) across multiple customer locations*"[33]. Microsoft attributed these attacks to an 'activity group' called STRONTIUM, which it had more widely observed in attacks targeting a range of sectors, including defence, education, engineering, government, IT, medicine, and military. The relevance of the example in the context of this report is that it further illustrates how organisations utilising vulnerable IoT devices could leave themselves open to threats from multiple directions.

Given that many of the security incidents are underpinned by vulnerability exploitation, it is interesting to consider the extent to which the manufacturers of consumer IoT devices are positioned in terms of disclosing vulnerabilities within their products. Related findings from Copper Horse Limited's research have been published by the IoT Security Foundation in 2018, 2019 and 2020, revealing that only a small minority of the 330 surveyed companies producing consumer IoT technologies have a disclosure policy in place. Specifically, the overall findings were 9.7% in 2018, 13.3% in 2019, and 16.3% in 2020[34]. The companies concerned encompassed 22 consumer IoT product categories, but the main concentrations were of devices in smart home, security, lighting and health and fitness – with none of these areas standing out as being significantly better in terms of the overall likelihood of having a vulnerability disclosure policy in place.

A final point of note in this part of the discussion is that the different devices do not pose equivalent risk in, as evidence suggests that some forms of device have experienced more security issues than others. Specifically, findings from Palo Alto Networks' threat intelligence team, Unit 42, have compared the prevalence of different types of IoT devices in the enterprise versus the security issues linked to devices of each type[35]. The findings are illustrated in Figure 7, and it is apparent that some devices are more prone to security issues than others. The report explicitly links the level of security issues to the likelihood of the devices being enterprise or consumer grade, observing that while IP phones are often designed for enterprise-grade security and reliability, cameras are more typically consumer-grade, with a focus upon simplicity and ease of deployment.

30 It should be noted that despite widespread reports of Western Governments' concerns about Kaspersky's alleged ties to the Russian state, the company's research on consumer IT is generally treated respectfully across the western expert community.

31 Kuzin, M., Shmelev, Y. and Kuskov, V. 2018. "New trends in the world of IoT threats", SecureList, 18 September 2018. https://securelist.com/new-trends-in-the-world-of-iot-threats/87991/

32 Kaspersky. 2019. "IoT under fire: Kaspersky detects more than 100 million attacks on smart devices in H1 2019", Kaspersky Press Release, 15 October 2019. https://www.kaspersky.com/about/press-releases/2019_iot-under-fire-kaspersky-detects-more-than-100-million-attacks-on-smart-devices-in-h1-2019

33 MSTIC. 2019. "Corporate IoT – a path to intrusion", Microsoft Threat Intelligence Center. 5 August 2019. https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/

34 IoTSF. 2020. *Consumer IoT: Vulnerability Disclosure – Expanding The View Into 2021*. IoT Security Foundation, November 2020. https://www.iotsecurityfoundation.org/wp-content/uploads/2020/11/Vulnerability-Disclosure-2021.pdf

35 Unit 42. 2020. *2020 Unit 42 IoT Threat Report*. Palo Alto Networks / Unit 42. March 2020. https://start.paloaltonetworks.com/unit-42-iot-threat-report

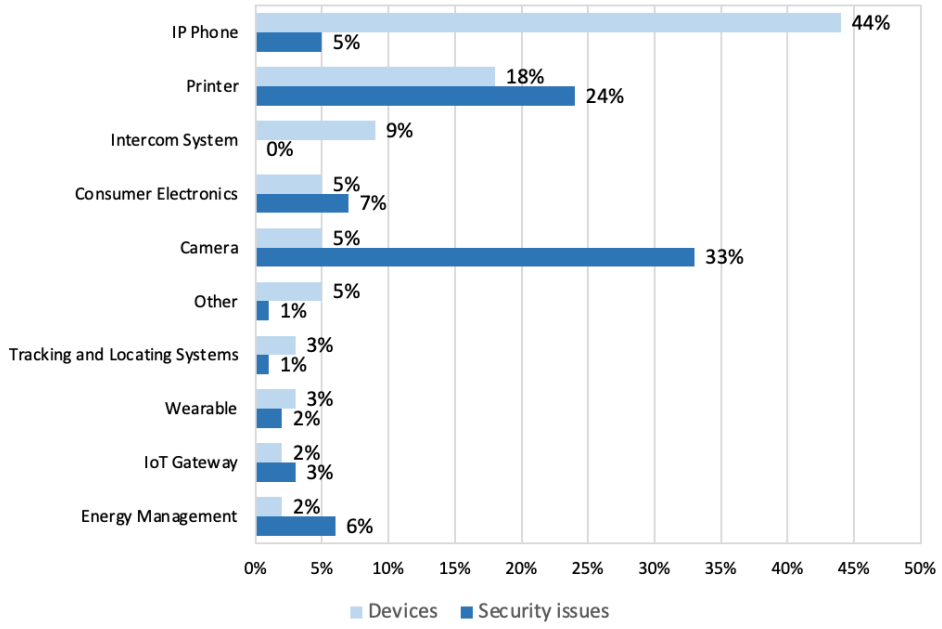


Figure 7: Comparing prevalence of enterprise IoT devices and related security issues

3.3 Relevant IoT security standards

The fact that vulnerable devices have been deployed and exploited is not to suggest that guidance and standards for consumer-grade IoT or enterprise-grade IoT devices cannot be found, but clearly there are questions around the extent to which they have been followed during the design and deployment of devices.

In the US, for example, Senate Bill 327 on the information privacy of connected devices introduced a requirement that, from the start of 2020, manufacturers of internet-connected devices must:

"equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure"[36]

The Bill encompasses all connected devices rather than specifically IoT devices, but clearly has particular relevance in this context.

Taking a more specific focus on consumer connected products, 2016 best practice guidelines from the IoT Security Foundation identify ten areas in which companies bringing IoT products to market would be expected to give attention (with the guidance indicating that if there are valid technical or business reasons that any areas cannot be *implemented*, this should still be *documented* in the design)[37]. Following a similar theme, and drawing on the UK context, 13 related guidelines are presented in the

[36] California Legislature. 2018. SB-327 Information privacy: connected devices. Senate Bill No. 327. Chapter 886. 28 September 2018. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327

[37] IoTSF. 2016. *Connected Consumer Products. Release 1.0. Best Practice Guidelines*. IoT Security Foundation, December 2016. https://www.iotsecurityfoundation.org/wp-content/uploads/2016/12/Connected-Consumer-Products.pdf

2018 Code of Practice for Consumer IoT Security published by DCMS[38], and based upon the same principles, ETSI's EN 303 645 standard presents baseline requirements for security of consumer IoT and identifies 13 almost identically named provisions[39]:

The UK will be one of the first countries to legislate security requirements for connected consumer devices. It is likely that other countries will monitor the extent and impact of the UK Government's regulations both in relation to consumer products, and their future proposals on other verticals such as enterprise IoT[40].

It is notable that all of these developments are relatively recent, and so many of the devices already in use will have been deployed without the standards having been available to reference and to set expectations.

At the same time, all of the above represent standards and recommendations for consumer grade devices and consumer level deployment. The baseline security expectations for deployment in enterprise contexts will likely need to be more rigorous, as is illustrated by recent work from the US National Institute of Standards and Technology's NISTIR 8259 document series. The main standard here addresses Foundational Cybersecurity Activities for IoT Device Manufacturers, reflecting a set of pre- and post-market cybersecurity considerations for device manufacturers. Four further documents in the series then cover device capability core baseline (8259A) and non-technical and supporting capabilities for IoT devices (8259B), how IoT devices can be profiled against the capabilities (8259C), and an illustrative example of such a profile in practice (8259D). Using NIST8259A as an example[41], it describes its core baseline as "*a set of device capabilities generally needed to support common cybersecurity controls that protect an organization's devices as well as device data, systems, and ecosystems*" and states that the aim is "*to provide organizations a starting point to use in identifying the device cybersecurity capabilities for new IoT devices they will manufacture, integrate, or acquire*".

The specific capabilities that are identified within the baseline are listed as follows:

- **Device Identification:** The IoT device can be uniquely identified logically and physically.
- **Device Configuration**: The configuration of the IoT device's software can be changed, and such changes can be performed by authorized entities only.
- **Data Protection**: The IoT device can protect the data it stores and transmits from unauthorised access and modification.
- **Logical Access to Interfaces**: The IoT device can restrict logical access to its local and network interfaces, and the protocols and services used by those interfaces, to authorized entities only.
- **Software Update**: The IoT device's software can be updated by authorised entities only using a secure and configurable mechanism.

38 DCMS. 2018. *Code of Practice for Consumer IoT Security*. Department for Digital, Culture, Media & Sport. October 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

39 ETSI. 2020. *CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements*. European Standard ETSI EN 303 645 V2.1.1 (2020-06). https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

40 UK Gov. 2020. 'Collection: Secure by Design'. https://www.gov.uk/government/collections/secure-by-design, n.p.

41 Fagan, M., Megas, K.N., Scarfone, K. and Smith, M. 2020. *IoT Device Cybersecurity Capability Core Baseline*. NISTIR 8259A. National Institute of Standards and Technology, May 2020. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259a.pdf

- **Cybersecurity State Awareness**: The IoT device can report on its cybersecurity state and make that information accessible to authorized entities only.

These capabilities are in turn expected to contribute to supporting the following risk mitigation areas (as identified in an earlier NIST report on managing IoT cybersecurity and privacy risks[42]):

- Asset management
- Vulnerability management
- Access management
- Device security incident detection
- Data security incident detection
- Data protection

The consequence of all this is that the security of consumer grade IoT technology is likely to see improvement over time, as newer devices are designed and released with these considerations in mind. However, it still requires the enterprise to be making informed choices if it is electing to deploy such technology, and it does not address the issues of either shadow usage or legacy kit that is already in use.

Looking at IoT more broadly, other national and international standardisation efforts are also ongoing. A number of relevant examples are highlighted in as follows:

- IEC/ISO have several cyber security standards under development, and in particular ISO 27402 is currently under development and aims to define baseline requirements across the IoT horizontal industry[43].

- GSMA[44] released a set of IoT security guidelines with five components: an overview, separate guidelines for IoT service ecosystems and for IoT endpoint ecosystems, guidelines for network operators, and an IoT security assessment checklist. Graded recommendations are provided in each. For example, enterprises may consider advice for endpoint ecosystems including the use of anomaly detection, trust anchors for data privacy, and pen-testing[45].

- The IoT Security Foundation published a document proposing a hub-based architecture designed for enterprise-managed IoT devices and solutions[46]. The document gives guidance on threat assessment, network management and security, how to connect devices securely, and device lifecycle management.

42 Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K., Nadeau, E., Piccarreta, B., Gabel O'Rourke, D. and Scarfone, K. 2019. *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*. NISTIR 8228. National Institute of Standards and Technology, June 2019. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf

43 ISO/IEC CD 27402 - Cybersecurity - IoT security and privacy - device baseline requirements". https://www.iso.org/standard/80136.html

44 GSMA. 2020. "IoT Security Guidelines – Overview Document, Version 2.2". https://www.gsma.com/iot/iot-security/iot-security-guidelines/, n.p.

45 GSMA. 2020. *IoT Security Guidelines for Endpoint Ecosystem*. Version 2.2. https://www.gsma.com/iot/wp-content/uploads/2020/05/CLP.13-v2.2-GSMA-IoT-Security-Guidelines-for-Endpoint-Ecosystems.pdf, 45-57

46 IoT Security Foundation. 2018. *IoT Security Architecture and Policy for the Enterprise - A Hub-Based Approach*. https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/IoT-Security-Architecture-and-Policy-for-the-Enterprise-a-Hub-Based-Approach.pdf, 9.

- The European Union Agency for Cybersecurity (ENISA)[47] has published a set of guidelines for IoT security to help manufacturers, developers, integrators, and other stakeholders involved in the IoT supply chain. The document is designed to help make better security decisions when assessing, building, or deploying IoT technologies.

- In January 2021, the Chinese Ministry of Industry and Information Technology (MIIT) launched a consultation on a publication titled "Guidelines for Building Basic Security Standard System for the Internet of Things". This publication identifies 5 core areas for standardisation, ranging from Security Management through to Gateway and Terminal security. This approach aims to have 10 industry standards drafted by 2022[48].

- The Cloud Standards Customer Council provides some guidance on how to enforce security measures in the IoT cloud[49]. The Institute of Electrical and Electronics Engineers (IEEE)[50] IEEE P2413 is focused on developing an IoT reference architecture, covering basic building blocks, and their integration into multi-tiered systems.

- The IPSO Alliance[51] is developing a platform that includes definitions and support of smart objects, with an emphasis on object interoperability with regards to protocols and data layers, as well as related identity and privacy technologies.

- The Object Management Group[52] is a technical standards consortium that is developing several IoT standards, including ones that focus on the Data Distribution Service (DDS) and Interaction Flow Modelling Language (IFML), dependability frameworks, threat modelling, and a unified component model for real-time and embedded systems.

- In Europe, the EU Cybersecurity Act, which came into force in June 2019, set the ball rolling for the development of more comprehensive, mutually recognised cyber security certification schemes across the continent. In Asia, the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) published IoT Security Best Practice Guidelines in 2020[53]. In Australia, a Code of Practice for Securing the Internet of Things for Consumers was published by the Department of Home Affairs[54].

47 ENISA. 2020. *Guidelines for Securing the Internet of Things: Secure Supply Chain for IoT*. https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things, 6-7.

48 China Briefing, Dezan Shira & Associates. 2021. "China's Draft Guidelines for Industrial Standards for the Internet of Things". https://www.china-briefing.com/news/china-internet-of-things-industrial-standards-draft-guidelines-released-5-major-standards/, n.p.

49 Cloud Standards Customer Council. 2016. "Cloud Security Standards: What to Expect & What to Negotiate Version 2.0". https://www.omg.org/cloud/deliverables/CSCC-Cloud-Security-Standards-What-to-Expect-and-What-to-Negotiate.pdf, 5-28; Cloud Standards Customer Council, 2017, "Security for Cloud Computing Ten Steps to Ensure Success Version 3.0", https://www.omg.org/cloud/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf, 5-34.

50 IEEE. n.d. "Internet of Things: IEEE Standards Enabling Products with Real-World Applications". http://standards.ieee.org/innovate/iot/index.html, n.p.

51 OMASpecWorks. n.d. "OMASpecsWorks: For a Connected World". https://omaspecworks.org/ipso-alliance/, n.p.

52 OMG. n.d. "IIoT Standards". https://www.omg.org/hot-topics/iot-standards.htm, n.p.

53 HKCERT. 2020. *IoT Security Best Practice Guidelines*. https://www.hkcert.org/f/guideline/262205/cc040767-fa07-4c87-aaa9-cdf46d4b92c6-DLFE-14203.pdf, n.p.

54 Australian Government. 2020. *Code of Practice - Securing the Internet of Things for Consumers*. https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf, n.p.

Other notable international contributions include various publications by the Japanese Government, such as the IoT Security Safety Framework (IoT-SSF)[55] which covers various types of IoT devices and systems including enterprise and the IoT Security Checklist[56] from JPCERTCC (Japan Computer Emergency Response Team Coordination Centre). Additionally, the Information-Technology Promotion Agency, a METI-affiliated institution, published IoT Safety/Security Development Guidelines (Second Edition) focusing on IT and cybersecurity, in 2017[57]. This document provides technical guidelines for manufacturers of IoT devices. Moreover, the Singapore Infocomm Media Development Authority published the Internet of Things (IoT) Cyber Security Guide[58] and in March 2020, Singapore announced that it would introduce a Cybersecurity Labelling Scheme for IoT devices.

Some countries are also now mandating the standards as legal requirements. For example, some states in the USA have recently brought IoT security laws and frameworks into effect. Additionally, the USA's IoT Cybersecurity Improvement Act (ratified in December 2020) directs NIST to develop standards and guidelines on how federal government agencies should appropriately use and manage IoT devices connected to information systems. In doing so, it directs NIST to develop minimum information security requirements for managing cyber security risks associated with IoT devices[59]. Another relevant example is the US Cyber Shield Act, which proposes a voluntary certification standard for IoT devices and would enable compliant products to display a related label that indicates a security assurance to consumers. This was originally proposed in 2019 but has recently been reintroduced in 2021[60].

As a final point in the context of standards and related activities, there are several potentially relevant projects funded by the *PETRAS National Centre of Excellence for IoT Systems Cybersecurity*. Projects of particular interest here could be GISt[61], which provides "an analysis of the political dynamics of the complex ecosystem of IoT security standards" focusing on the Industrial IoT context, and IoTMSP[62], which includes an objective on "shaping the country's IoT agenda and informing policy options for the government to promote the safe deployment of IoT across a plausible set of sectors". A further project of potential relevance could be IoT Observatory[63], which relates to the sharing IoT datasets (and may therefore host datasets that give an insight into organisational device deployment and usage).

55 METI. 2020. *IoT Security Safety Framework*. https://www.meti.go.jp/english/press/2020/pdf/1105_002a.pdf, n.p.
56 JPCERTCC. 2020. "IoT Security Checklist". https://www.jpcert.or.jp/english/pub/sr/IoT-SecurityCheckList.html, n.p.
57 IPA. 2017. "IT Knowledge Center on Emerging Tech Trends". https://www.ipa.go.jp/english/sec/reports/20160729-02.html, n.p.
58 Singapore IMDA. 2020. "Guidelines: Internet of Things (IoT) Cyber Security Guide". https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/ICT-Standards/Telecommunication-Standards/Reference-Spec/IMDA-IoT-Cyber-Security-Guide.pdf?la=en, n.p.
59 Congress.Gov. 2020. H.R.1668 - IoT Cybersecurity Improvement Act of 2020. 12/04/2020. https://www.congress.gov/bill/116th-congress/house-bill/1668
60 Miller, M. 2021. "Lawmakers reintroduce legislation to secure internet-connected devices", The Hill, 24 March 2021. https://thehill.com/policy/cybersecurity/544711-lawmakers-reintroduce-legislation-to-secure-internet-connected-devices
61 See *Geopolitics of IIoT Standards (GISt)* at https://petras-iot.org/project/geopolitics-of-iiot-standards-gist/
62 See *IoT Multi-disciplinary Standards Platform (IoTMSP)* at https://petras-iot.org/project/iot-multi-disciplinary-standards-platform-iotmsp/
63 See *IoT Observatory* at https://petras-iot.org/project/iot-observatory/

4 Sectoral analysis

This section examines the adoption of IoT devices in different sectors, and thereby attempts to give some insight in relation to the questions around which ones are using the highest volume of connected devices and which types of device categories are deployed in the highest numbers. However, there is again a significant limitation here due to the current level of literature evidence, as the published reports tend to look at IoT adoption by sector in general/overall terms, rather than examining the categories of devices being used and whether or not they are consumer or enterprise-grade.

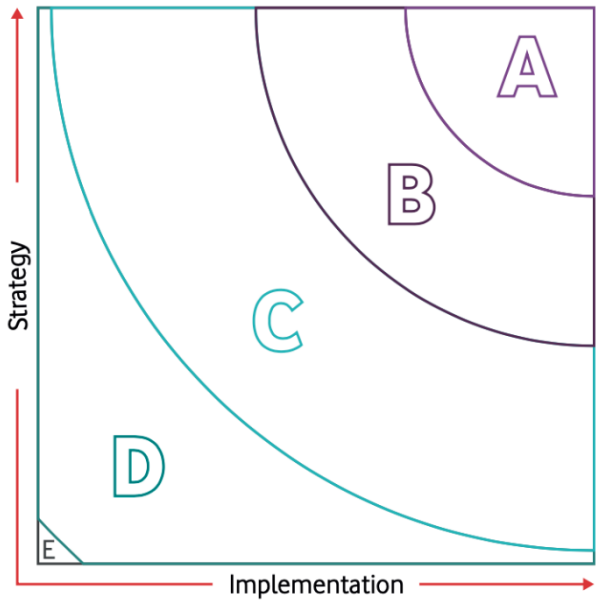
Vodafone Business's IoT Barometer 2019 report[64] provides a good example of the evidence constraints, examining the extent of IoT adoption across several industries but lacking a specific disaggregation of the types of device involved. The survey is based on responses from 1,430 respondents across three geographic regions (the Americas, APAC and EMEA) and encompassing eight vertical sectors (automotive; energy and utilities; financial services; healthcare and wellness; insurance; manufacturing and industrials; retail, leisure and hospitality; and transport and logistics). In overall terms, it was determined that a third (34%) of organisations were using IoT in 2018, up from just 12% five years earlier.

In examining the level of IoT adoption, the study considers the notion of 'sophistication' in two dimensions:

- **Strategy:** The maturity of IoT consideration within the business, the extent of linkage to business outcomes, the level of reliance upon it, and the extent of integration into core systems.
- **Implementation:** The level of actual IoT experience in practice, in terms of deployments across live activities and pilot projects.

The resulting levels of sophistication are then split across five bands, as illustrated and outlined in Figure 8. To give a sense of the maturity at the time of the study, it was reported that globally just over a quarter (27%) of organisations were falling into the range of the top three bands. At the same time, the survey reported that organisations in higher bands observed increasing benefits and return on investment, suggesting that the path is one that organisations will continue to pursue.

64 Vodafone. 2019. Your IoT-driven future. Vodafone Business – IoT Barometer 2019. Vodafone Business. https://www.vodafone.com/business/news-and-insights/white-paper/vodafone-iot-barometer-2019



A. Most sophisticated
Full-scale projects; IoT deeply embedded in the business

B. Very sophisticated
IoT embedded and seen as mission critical; likely to support decision making

C. Intermediate
At least one full-scale project in place

D. Beginners
Planning to adopt IoT within 2 years, or may have small pilot/trial deployments

E. Still considering
No firm plans to adopt within 2 years

Figure 8: Vodafone Business IoT sophistication model (Source: Vodafone, 2019)

The report does not consistently present the same metrics for all of the sectors, and so the list below presents the most relevant key indicators for the sectors concerned (noting that although Insurance is listed as a distinct vertical sector elsewhere in the report, it appears to have been grouped within Financial Services for this aspect of the analysis).

- **Automotive:** 36% adoption rate, with the highest concentration of adoption around the boundary of bands B and C.
- **Energy and utilities:** 36% adoption rate, with adopters concentrated in Bands B (40%) and C (53%).
- **Financial services:** 34% adoption rate, with concentrations of adoption in Bands B and C.
- **Healthcare and wellness:** Overall adoption rate not stated, and levels of sophistication are dispersed across the bands. This was the sector with the highest representation in Band A, but a specific figure was not given.
- **Manufacturing and industrials:** 39% adoption rate, with 92% of adopters falling into Bands B (49%) and C (43%).
- **Retail:** Overall adoption rate not stated, but notable concentrations of adoption in Bands B (18%) and C (36%).
- **Transportation and logistics:** 42% adoption rate (the highest sector), with two thirds (65%) of adopters in the top two bands.

It should be noted that the full report presents a 'heat map' representation for each sector, to show key concentrations within the sophistication bands.

While the Vodafone report does not give a clear breakdown of IoT device categories, it *does* offer overall responses in terms of what the adopters are using (or planning to use) IoT to detect, measure or track. These findings, represented in Figure 9, suggest that many of the associated devices are likely to fall into non-consumer categories.

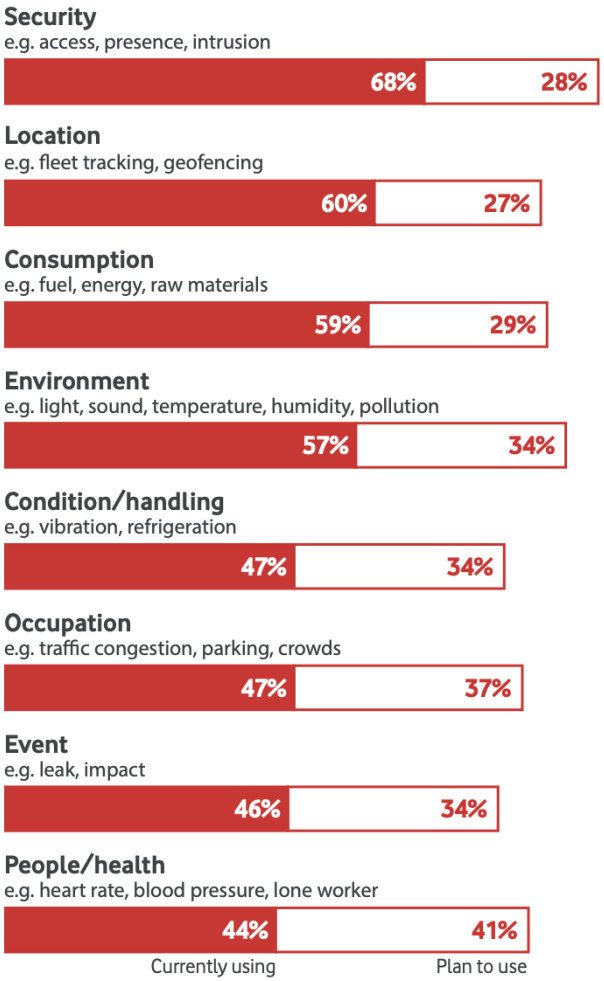


Figure 9: Uses of IoT devices from Vodafone Barometer respondents (Source: Vodafone, 2019)

While the discussion has highlighted the Vodafone study in most detail, there are a number of further sources that also offer insights into IoT adoption by sector. Looking back to 2017, there the earlier-cited *IoT State of the Industry* report from James Brehem & Associates[65]. The related findings from here are reproduced in Figure 10, and it should be noted that the source report acknowledges (but does not explain) the anomaly of healthcare being highlighted as both a leader and a laggard.

[65] James Brehem & Associates. 2017. *The Connected Conversation: 2017 IoT State of the Industry Survey*. 25 January 2017. https://www.jbrehm.com/blog/2017/1/25/the-connected-conversation-2017-iot-state-of-the-industry

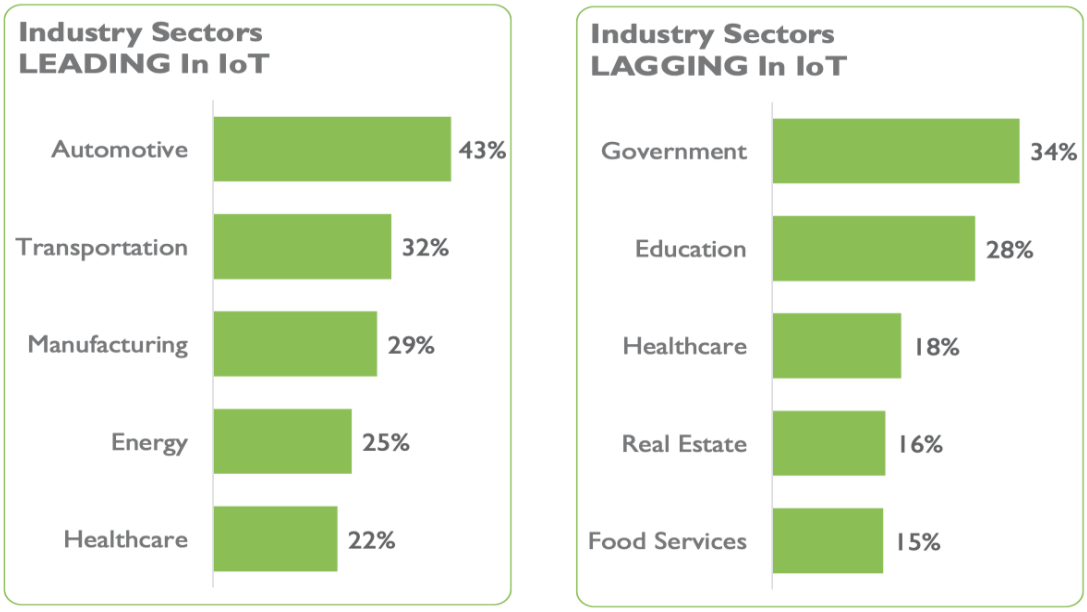


Figure 10: Sectors leading and lagging in IoT deployment (Source: James Brehem & Associates, 2017)

Stepping forward to 2019, an enterprise IoT study from Avasant offers an indication of the relative share of IoT Implementation across different sectors, based upon an examination of 400 use cases and 43 providers[66]. Their results are depicted in Figure 11, based upon the nine categories that Avasant reported. It should be noted that this is reflecting IoT devices in general, rather than specifically consumer-grade devices, and also that the classification of industries is again categorised differently to the other examples so far.

[66] Avasant. 2019. *Enterprise Internet of Things Trends shaping the Market*. April 2019. https://avasant.com/report/enterprise-iot-trends-shaping-market/

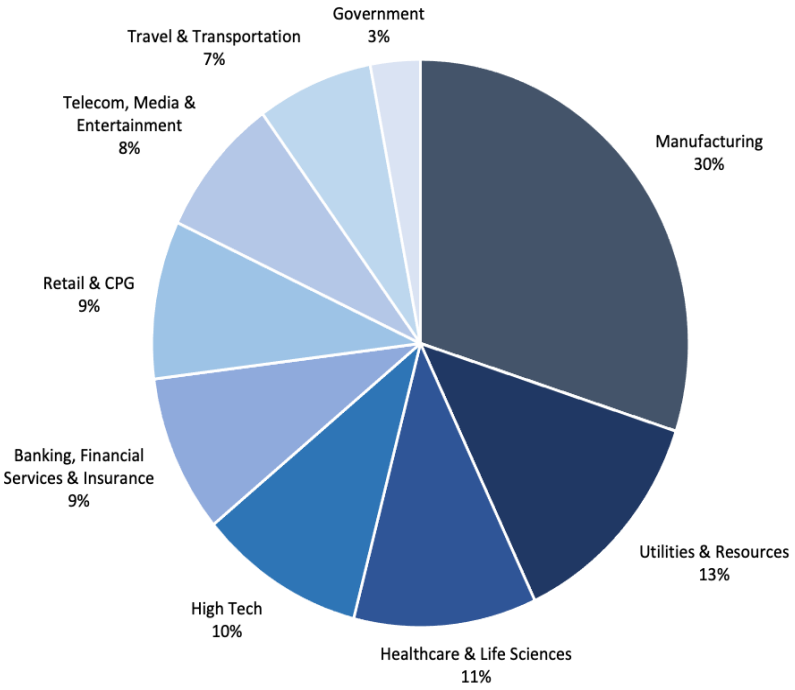


Figure 11: Share of IoT Implementation by sector

Meanwhile, 2020 findings from Syniverse help to provide an insight into how the IoT technologies are being used within different sectors[67]. Based upon a sample of 200 enterprises in North America and Europe, Table 1 reflects the top-ranked business goals behind the deployment of IoT across five target industry sectors, while Table 2 shows what they are using IoT to achieve in terms of actual applications (in both cases the shading is used to help highlight differing levels of deployment priority).

Rankings by industry	Improve efficiency and productivity	Improve product or service quality	Improve customer/citizen experience	Grow revenues from existing customers/ products	Reduce costs
Healthcare	1	2	3	6	7
Retail & hospitality	1	2	6	3	9
Financial services	2	3	1	9	6
Manufacturing	1	2	3	9	7
Transport	1	2	5	10	3

Table 1: Top-ranked IoT deployment goals by sector (Source: Syniverse-Omdia, 2020)

67 Rehak, A. and Tomasi, P. 2020. *Connected Everything: Taking the I out of IoT - Highlights from Syniverse and Omdia's 2020 IoT enterprise survey*. Syniverse / Omdia, April 2020. https://www.syniverse.com/insights/iot-is-transforming-the-enterprise-find-out-how-your-peers-are-doing-it

	Healthcare	Retail and Hospitality	Financial Services	Transport	Manufacturing and Industrial
Connected security	63%	78%	71%	68%	66%
Worker/workplace safety	58%	68%	76%	50%	66%
Remote payment terminals	55%	51%	81%	34%	39%
Smart building systems/Energy management	34%	59%	62%	39%	61%
Asset tracking	45%	49%	29%	61%	66%
Predictive maintenance	42%	46%	45%	47%	61%
Remote asset monitoring	58%	44%	33%	53%	44%
Fleet management	26%	56%	40%	47%	54%

Table 2: IoT applications deployment by sector (Source: Syniverse-Omdia, 2020)

Some further sector-specific commentary can be offered from other sources, but again they support the fact that IoT adoption in general is significant without an insight into the extent to which consumer devices are playing a role:

- **Healthcare:** 2017 findings from Hewlett Packard Enterprise indicated that six in ten healthcare organisations were already using IoT. However, the associated report did not fully decompose the findings, and the named devices would not be classed within the consumer category, or within the scope of IoT used for business productivity (with 64% reporting patient monitors (64 percent) and 41% indicating x-ray/imaging)[68].

- **Manufacturing**: 2020 findings from Transforma Insights surveyed an unspecified number of organisations in the manufacturing sector and suggested that over 80% were already active in IoT but did not offer further clarity on what was being used or for what purposes[69].

- **Retail**: There is significant evidence of IoT use in a retail stores context, but with emphasis given to sector-specific uses (e.g. vending machines, smart shelving, smart signage, self-checkouts and connected cameras) that would largely suggest non-consumer-based technology[70]. The 2017 Hewlett Packard Enterprise report also commented on retail IoT usage, indicating that just under half (49%) had deployed it.

Little further information could be identified regarding the use of specific IoT device types within different sectors. However, a source that presents at least some comparative indication is Forescout Research Labs' 2021 report on the state of IoT security71. This study examined the situation across five sectors

68 Hewlett Packard Enterprise. 2017. The Internet of Things: Today and Tomorrow. http://chiefit.me/wp-content/uploads/2017/03/HPE-Aruba_IoT_Research_Report.pdf

69 Transforma Insights. 2020. *Enterprise IoT Market Research Survey*. May 2020. https://internetofbusiness.com/2020-enterprise-iot-market-research-survey/

70 I-Scoop. "The Internet of Things (IoT) in the retail industry – evolutions and use cases". https://www.i-scoop.eu/internet-of-things-guide/internet-things-retail-industry/

71 Forescout. 2021. *The Enterprise of Things Security Report: The State of IoT Security*. Forescout Research Labs. https://www.forescout.com/company/resources/the-annual-connected-enterprise-reporte

and ranked the 'riskiest' devices being used in each one (with the devices themselves grouped into five type categories). Forescout assessed the 'risk' by aggregating a number of factors (e.g. vulnerabilities, exploitability, potential communication, and business criticality) to determine if devices were inherently risky or risky as a result of their connectivity. The resulting findings are presented in Table 3, which lists all of the devices that Forescout had categorised under 'Smart Building', 'Networking and VoIP', and 'Other'. The empty cells reflect positioning of entries from the 'Healthcare' and 'Operational Technology' device categories, which are omitted because none of the constituent device types would have been consumer-grade. However, it is clear that some of the device types still listed in the table (particularly among the networking devices) are unlikely to be consumer level. Nonetheless, it is still apparent that some of the devices listed within these categories have the potential to be drawn from consumer-level products.

	Financial Services	Government	Healthcare	Manufacturing	Retail
1		Physical Access Control	Pneumatic Tube System		Physical Access Control
2	HVAC	HVAC		Physical Access Control	HVAC
3	IP Camera	Emergency Comms System			IP Camera
4		IP Camera		IP Camera	
5	Network Management			HVAC	Firewall
6	Firewall	Serial-to-IP Converter		Point of Sale	Out of Band Controller
7	Out of Band Controller	Lighting	Physical Access Control	Network Management	Wireless Access Point
8	Router or Switch	Out of Band Controller		Out of Band Controller	Video Conferencing
9	VoIP Server	Video Conferencing	HVAC	Video Conferencing	Router or Switch
10	Printer	Network Management			Net. Attached Storage

Networking and VoIP devices Smart Building devices Other IoT devices

Table 3: Riskiest devices in use per sector

Based on the earlier more general evidence of consumer devices within the enterprise and combining this with the clear evidence of IoT adoption within each sector, there can be little doubt that consumer devices are being used within each of these contexts. However, the different studies are not sufficiently consistent in their categorisation of either the sectors or the connected device types/uses to enable a more detailed analysis. As such, it is not possible to highlight key findings more specifically or to make any direct recommendations for priority sectors. The question of determining whether there are 'typical' use cases would therefore be a relevant area for further primary research and data collection.

5 Distinction between consumer and enterprise deployments

The final question posed in the scope of the review was to identify how enterprise device deployment differs from how consumers typically use consumer connected devices. Illustrative conceptual examples here could include:

- an organisation may deploy meeting room booking displays across its facilities, linking them to both the enterprise network and to the organisation's corporate data to access calendar information; and
- video conferencing systems may be deployed across a multinational organisation's facilities, and in the homes of senior executives, with the devices being connected to each other and to the enterprise network.

It is important to recognise that the enterprise deployment of IoT – whether sanctioned or shadow – is occurring for a reason. While in some cases it is simply creeping in organically, it is more typically linked to a recognition of particular benefits that the technology is seen to provide. The nature of the organisation appetite is neatly summarised by the following quote from Aruba:

"Increasingly, people are looking for a digitally-powered working environment that makes everything – from controlling office climate to booking a meeting room – more efficient. As ever more advanced consumer technologies, such as home automation products, become a feature of most employees' personal lives, they will expect the same benefits in their place of work."[72]

This desire for technology-based convenience and integration, and the potential to leverage it in the workplace is likely to drive a number of practical deployments. In a similar style to the conceptual examples above, the 2019 study from NCC Group suggested a series of further cases in which smart technologies could be used in a manner that differs from their domestic use[73]:

- smart coffee machines could be turned on before staff arrive;
- smart plugs could be used to remotely turn off printers and other non-critical office devices when not in use; and
- use of smart locks, enabling access to physical premises and space to be granted remotely.

The final example was drawn from an actual product example, namely the Kisi app, that allows office managers and access administrators to unlock offices via the Slack collaboration and communication service[74].

[72] Aruba. 2018. *The Right Technologies Unlock the Potential of the Digital Workplace*. https://www.arubanetworks.com/assets/eo/Aruba_DigitalWorkplace_Report.pdf

[73] Garcia, L. 2019. *Security Impact of IoT on the Enterprise*. NCC Group, November 2019. https://www.nccgroup.trust/globalassets/our-research/uk/whitepapers/2019/11/iot-whitepaper-matt.pdf

[74] Mehl, B. 2018. "Introducing Kisi for Slack: Unlock Your Office Door With Slack", Kisi blog, 11 September 2018. https://www.getkisi.com/blog/kisi-for-slack

Such examples are likely sufficient to show that the flexibility of IoT integration will open up numerous further examples, with the building blocks of cloud communications, app services and the connected devices themselves offering the opportunity for new applications via increasingly ambitious and creative combinations. This goes back to the requirement to ensure that the underlying devices themselves are fit for purpose and have been designed with the characteristics that the enterprise would need in order to rely upon them. If the building blocks are based around consumer level devices, then this falls into doubt.

It can be generally observed that much of the use of the devices is occurring in contexts they were not designed to support. The distinction between consumer and enterprise device deployment is not so much in the uses themselves but the characteristics of their usage. For example, network Wi-Fi access points will still be used to provide connectivity but will be carrying enterprise traffic rather than the user's personal data. Similarly, IP security cameras will still be carrying video data and be used for a security purpose but will be getting used to safeguard more significant environments.

More generally, there are characteristics that distinguish consumer and enterprise IoT devices in terms of the scenarios and the applications they are designed to support, with scalability, communications and power requirements all being potentially different, along with the already-recognised issue of cyber security[75]. Additionally, consumer devices may have been designed to support a shorter lifespan, recognising both the potential upgrade/replacement cycle for consumers as well as the relative intensity of use (e.g. any devices with potential for component-related wear and tear would be expected to be designed and built to withstand more intensive use in an enterprise context compared to use in the home).

Overall, this aspect of the discussion does not affect the wider conclusion. Consumer grade devices may lack the capabilities and safeguards that are relevant to even baseline enterprise deployment. If the nature of the deployment becomes more ambitious, integrating them as components within wider enterprise solutions and services, then it only serves to amplify risk that results from doing so.

[75] CDW. 2019. "Consumer vs. Business Usage of IoT Devices", 5 April 2019. https://www.cdw.com/content/cdw/en/articles/networking/2019/04/05/consumer-vs-business-iot.html

6 Conclusions

There is clear evidence that IoT adoption within enterprise contexts has already reached significant levels, and consumer grade devices are playing a significant role within this (albeit sometimes in the guise of shadow technologies rather than intentional and sanctioned adoption). Having said this, it is clear that the review has ultimately been limited in its ability to provide definitive answers to the original questions. While there has been some ability to indicate which sectors are using the highest total number of connected devices within their networks, it remains less clear which categories of connected device are deployed most significantly within them. Similarly, the review has been able to offer only a limited insight into how enterprise device deployment differs from consumer use of the same devices. However, there is sufficient broader evidence to confidently infer that *such use is happening* and warrants further investigation to more fully determine the details.

Looking beyond the constraints, what the review *has* revealed is significant evidence of the *overall* adoption of connected devices within enterprise environments, and the fact that security represents a real issue in this context (in terms of both adopters' concerns and evidence of practical experiences). In parallel, there is a growing attention toward addressing security issues, with relevant activity in terms of standards (most notably the work from NIST) and various national / government initiatives that seek to guide and improve security practice in the design and deployment of connected devices.

Moving forward, further research would be needed in order to enable more direct insights and address the lack of direct primary evidence. In addition to revisiting the sector-specific questions, it could also be relevant to consider the longer-term impacts of the COVID-19 pandemic, as this is likely to have an impact upon device usage. For example, maintaining an increased level of homeworking activities would likely mean that employees' own connected devices could increasingly find themselves essentially becoming part of the enterprise footprint (being used for workplace purposes, connecting to the enterprise network, and/or interacting with enterprise-owned devices). It is therefore suggested that future research would have the opportunity to explore a variety of angles and help to build upon the foundation established by this review. Certainly, while the longer-term impacts of the pandemic effectively render some of the current findings provisional, the expert consensus and actions of Governments worldwide suggest that they are likely to accelerate the trends in this report rather than slow or reverse them. As such, the issue of IoT security assumes even greater significance as we move forward.

Ipsos MORI's standards and accreditations

Ipsos MORI's standards and accreditations provide our clients with the peace of mind that they can always depend on us to deliver reliable, sustainable findings. Our focus on quality and continuous improvement means we have embedded a 'right first time' approach throughout our organisation.

ISO 20252

This is the international market research specific standard that supersedes BS 7911/MRQSA and incorporates IQCS (Interviewer Quality Control Scheme). It covers the five stages of a Market Research project. Ipsos MORI was the first company in the world to gain this accreditation.

ISO 27001

This is the international standard for information security designed to ensure the selection of adequate and proportionate security controls. Ipsos MORI was the first research company in the UK to be awarded this in August 2008.

ISO 9001

This is the international general company standard with a focus on continual improvement through quality management systems. In 1994, we became one of the early adopters of the ISO 9001 business standard.

Market Research Society (MRS) Company Partnership

By being an MRS Company Partner, Ipsos MORI endorses and supports the core MRS brand values of professionalism, research excellence and business effectiveness, and commits to comply with the MRS Code of Conduct throughout the organisation.

Data Protection Act 2018

Ipsos MORI is required to comply with the Data Protection Act 2018. It covers the processing of personal data and the protection of privacy.

For more information

3 Thomas More Square
London
E1W 1YW

t: +44 (0)20 3059 5000

www.ipsos-mori.com
http://twitter.com/IpsosMORI

About Ipsos MORI Public Affairs

Ipsos MORI Public Affairs works closely with national governments, local public services and the not-for-profit sector. Its c.200 research staff focus on public service and policy issues. Each has expertise in a particular part of the public sector, ensuring we have a detailed understanding of specific sectors and policy challenges. Combined with our methods and communications expertise, this helps ensure that our research makes a difference for decision makers and communities.

Ipsos MORI