Framing the Nature and Scale of Cyber Security Vulnerabilities within the Current Consumer Internet of Things (IoT) Landscape

2020

Authors: Jack Malan, James Eager, Eugénie Lale-Demoz, Giorgio Cacciaguerra Ranghieri, Michaela Brady

Centre for
Strategy & Evaluation
Services

Centre for Strategy & Evaluation Services LLP
Westering House
17 Coombe Road
Otford, Kent TN14 5RJ
United Kingdom
E: enquiries@cses.co.uk
T: +44 (0) 1959 525122

Table of Contents

Tables

Figures

Boxes

Executive Summary

This study sought to examine the nature and scale of cyber security vulnerabilities within the current and future consumer Internet of Things (IoT) landscape by collecting and analysing data on the:

- **Future scale of consumer Internet of Things devices across the UK**, focusing on the adoption and spatial distribution of such IoT devices over the next 5 to 10 years.
- **Types of consumer IoT vulnerabilities,** including the impacts associated with each type of vulnerability on consumers, businesses and the wider economy, and the future growth of each type of vulnerability.
- **Impact of vulnerabilities and future risks**, i.e. the potential impact of consumer IoT vulnerabilities on the UK economy if exploited at scale; and evidence of the current and potential future risks of insecure consumer IoT devices, including an estimate of the number of cyber attacks using consumer IoT vulnerabilities in recent years.
- **Potential impacts of Government regulation** through mandating a minimum IoT security baseline on different demographic, income and age groups; and the potential impact of a lack of IoT device ownership among specific economic groups in the UK.

The study was carried out for the Department for Digital, Culture, Media & Sport (DCMS) by the Centre for Strategy & Evaluation Services (CSES) in early 2020. The CSES team was advised by Dr Konstantinos Mersinas from Royal Holloway, University of London.

For the purposes of this report, consumer IoT is defined as network-connected (and network-connectable) devices and their associated services that are usually available for the consumer to purchase in retail environments. The product's purpose is typically for use within the home or as personal electronic wearables.[1]

Given the increasing connectivity of consumer IoT devices and the constant evolution of the threat landscape, there is a growing cyber security risk. The exploitation of vulnerabilities in such devices can have significant impacts at the personal, local, national and even global levels. At the same time there are information asymmetries in the consumer IoT market. Most consumers have a limited understanding of, or access to, information on cyber security risks and the level of security built into products. Although some manufacturers place a significant emphasis on security, many others currently have no incentive to invest in improving the security of their consumer IoT products.

To address this situation, the Government has been working with key stakeholder groups to develop a regulatory approach to improve the security of consumer IoT devices, and to encourage the market to embed 'secure by design' principles in their design, manufacturing and development processes.[2]

1. Future Scale of Consumer IoT

Overall, the study confirms that there will be strong growth in future years in the overall adoption of consumer IoT devices. In the UK, the number of IoT connections is predicted to grow from 13 million in 2016 to over 150 million by 2024.[3] But there will be differences in this respect between the three product categories identified in this study: "Big Ticket" items (e.g. smart televisions, white goods, kitchen appliances), "Connecting the Home" items (e.g. smart speakers, smart meters, other devices

[1] Definition provided by DCMS for the study 'Framing the nature and scale of cyber security vulnerabilities within the current Consumer Internet of Things ('IoT') landscape'.
[2] Department for Digital, Culture, Media & Sport (DCMS). (2020). Consultation Outcome: Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation.
[3] Ofcom. (2017). Connected Nations 2017: Data analysis

that are used to control and monitor activity within a home), and "Consumer Lifestyle" items (e.g. wearables, toys, smartphones, etc.). Nevertheless, continued growth is anticipated across the wide spectrum of product types. This will be driven by a range of factors, including:

- The integration of connectivity and development of improved functionality into more and more products by manufacturers, technological innovators and other economic operators;
- New connected products appearing on the market;
- Improving affordability as a result of increasing availability and ubiquity;
- Improving consumer awareness and understanding of cyber security issues associated with consumer IoT devices, leading to increased trust in devices and the industry as a whole;
- Emerging business models and remote working environments.

Future growth will depend on reducing the barriers to adoption of consumer IoT devices identified through this research, which include concerns related to cost, security, privacy and ease of use. The affordability of technology is a key consideration for potential consumers, but according to a recent techUK survey on the State of the Connected Home, 52% of respondents stated they are willing to pay more for some of the benefits of a connected device.[4] Similarly, in the survey conducted as part of this study, 47% of consumers stated that price was only "moderately" important (versus "very" or "extremely"), demonstrating some flexibility among consumers when deciding whether or not to purchase a device.

Trust in the security and privacy protection measures of consumer IoT devices is likely to remain a significant driver of adoption and market growth. However, many economic operators in the market currently face challenges in this regard, due at least in part to higher costs associated with increasing and maintaining device security.

Emerging business models will also influence the future of the consumer IoT market. For instance, this study finds that economic operators are more readily moving to as-a-service business models, either by offering services to support the use of IoT devices bought by a consumer or by requiring the consumer to use an IoT device to participate in a service (examples include the car insurance industry providing 'black boxes' to monitor driving performance). It is anticipated that these emerging business models will require a greater focus on cyber security, as reputation and brand will become more important considerations for companies providing services rather than standalone devices.

2. Types and Impacts of Consumer IoT vulnerabilities

Although the cyber threat landscape is constantly evolving and is becoming characterised by more sophisticated and complex threats, this study suggests that the majority of threats facing consumer IoT devices exploit simpler vulnerabilities, such as the use of default or hard coded passwords. That said, there is a wide range of cyber threat types relevant to consumer IoT devices, including Distributed Denial of Service (DDoS) attacks, spoofing and repudiation attacks.

The study also finds that such attacks are often not particularly difficult to implement, as there are a wide range of vulnerabilities commonly found in consumer IoT devices that can be exploited. In addition to the use of default passwords, such devices commonly have vulnerabilities related to insecure network services or ineffective ecosystem interfaces, lack of device management and lack of secure update mechanisms. Furthermore, many manufacturers and developers of consumer IoT devices do not have fast and reliable vulnerability disclosure policies.

Different consumer IoT product types face different cyber risks as new players enter the IoT market, such as large manufacturers that add connectivity to existing appliances (e.g. smart fridges, smart TVs)

[4] techUK. (2019). The State of the Connected Home: Edition Three.

and small and medium tech firms create new devices. Some of these producers may have little experience in security engineering or have limited financial resources to invest in device security features (i.e. encryption or security updates). Furthermore, as the number of devices rises and the number of connections increases, the threat of cyber attacks will also increase.

Cyber attacks exploiting vulnerabilities can have significant impacts both at the individual and business levels. This study's consumer survey revealed that 23% of respondents had received a security warning notification from their IoT device and 11% reported their device having been infected with a virus, malware or ransomware. Attacks can result in privacy breaches, financial loss and service interruption. Consumer IoT products that are affected by security issues can cause emotional distress to their users, as reported by 17% of the survey respondents who had experienced a cyber security issue.

According to this study's business survey, the main impacts that businesses reported as being very damaging were 'reputational damage to the device manufacturer/retailer' (45%), 'loss of consumer confidence' (55%) and 'loss of personal/customer data' (57%). From businesses' perspective, IoT cyber attacks can also lead to financial losses, which for smaller companies can represent a significant proportion of their revenues.

The exploitation of consumer IoT vulnerabilities, particularly through botnets, can have significant impacts at the national and even global levels. An example of a potential future cyber risk relates to the use of high wattage domestic appliances (e.g. air conditioners and heaters) to launch large-scale coordinated attacks on power grids, potentially denying electricity to large numbers of citizens.

3. Potential Impacts of Government Regulation

Regarding the potential impact of Government regulation on the consumer IoT market, the study finds that manufacturers and other economic operators will incur a range of administrative and substantive compliance costs. The extent of these costs is difficult to quantify and will depend on the nature of the regulatory approach and the extent to which product redesign costs are required. Furthermore, there are additional complexities, for example in relation to supply chain management and thus the implementation of vulnerability disclosure practices or software updates. These could also have impacts on the costs to the market associated with implementation. However, it is likely that these costs will not be significant and will therefore not be passed on to consumers.

At the same time, there could be positive economic effects, including increasing sales volumes, as a result of greater confidence and trust in the security of consumer IoT devices. Additionally, increased device security should act to mitigate the risks to manufacturers of cyber attacks against their products and the related negative impacts. There could also be a range of significant benefits to consumers such as: a reduction in the number of insecure consumer IoT devices; increased confidence and trust, leading to increased ownership and greater realisation of the benefits associated with the IoT; and wider positive impacts on cyber security at a national and global scale.

However, there could also be negative impacts on consumers and a major challenge is to ensure that the responsibility for being informed about cyber security does not lie with the consumer. Should security labelling be introduced, the onus will remain on the consumer; however, the onus will lie with manufacturers and developers if they are required to implement aspects of the top three Code of Practice guidelines. Furthermore, potential negative impacts on consumer access are possible as a result of potential increases in device prices and the potential for non-UK providers to exit the UK market. However, these effects are considered unlikely.

The potential impact of regulatory intervention on certain demographic groups in terms of age, gender and household income suggests that certain groups will not experience specific negative impacts. However, certain consumer groups will benefit from greater positive impacts as a result of the implementation of minimum security requirements. For instance, higher income households are likely to have higher levels of IoT adoption, leading to greater benefits than lower income households.

Headline Statistics from the Study

- In the UK, the number of IoT connections is predicted to increase to more than 150 million by 2024, with 80% of these connections coming from device categories such as wearables, connected media, smart meters and emergency calling services (Ofcom, 2017).
- According to the consumer survey conducted for this study, security ranks third, after functionality and durability, with regard to the factors that are prioritised when buying a consumer IoT device (60% ranked security as either 'extremely important' or 'very important', compared to 88% for functionality and 63% for durability).
- Gemalto (2019) carried out a study to assess the state of IoT security and found that globally, almost half (48%) of companies still cannot detect if any of their IoT devices have been breached, despite companies increasing their focus on IoT security (spending on protection has grown from 11% of IoT budget in 2017 to 13% in 2018).
- Human error is estimated to be responsible for 95% of security breaches (Ahola, M., 2019).
- This study's consumer survey revealed that 23% of respondents had received a security warning notification from their IoT device and 11% reported that a device they own has been infected by a virus, malware or ransomware.
- In the UK, 46% of businesses report having experienced a cyber security breach in the last 12 months, affecting in particular 68% of medium-sized businesses and 75% of large businesses, although this was not only IoT-related attacks (Ipsos MORI, 2020 Cyber Security Breaches Survey).
- The business survey for this study reported that a majority of respondents (57%) perceived loss of personal / consumer data as the result of an IoT cyber attack as 'very damaging'. This was followed by a loss of consumer confidence (55%) and reputational damage to the device manufacturer / retailer (45%).
- Researchers from University College London found that in relation to five types of consumer IoT devices (smart TVs, smart watches, Wi-Fi routers, security cameras and thermostats) individuals were willing to pay, on average, between 14% and 63% more for greater security in IoT devices (Blythe et. al, 2020). Research conducted by Harris Interactive in 2019 found that, overall, more than half of survey respondents (59%) were willing to pay a premium of 5% for a product with a security label compared to a product without.

4. Methodological Note

The research, which combined a literature review, interview programme and a survey of consumers and businesses, was carried out in the period from February to April 2020.

The literature review examined existing research, industry publications and 'grey' literature in relation to each of the study objectives. In total, some 80 different sources were examined. In order to support all aspects of the analysis, 23 interviews were conducted with stakeholders including manufacturers of IoT devices, industry and consumer associations.

In addition, two online surveys were undertaken, one targeting users of consumer IoT devices and one targeting businesses and other organisations (from different sectors and varying in size) who either manufacture, import or sell consumer IoT devices. A total of 108 responses were obtained. There were 51 business responses and 57 consumer responses.

It should be noted that the fieldwork for this research took place during the COVID-19 pandemic, which may have affected the response rate. The relatively small number of survey responses means that these results are indicative and caution should be exercised in interpreting the findings. The data captured via these means supported a number of case studies illustrating real-life examples of cyber attacks against consumer IoT devices and their impacts.

1. Introduction

1.1 Study objectives and scope

The purpose of this study was to examine the nature and scale of cyber security vulnerabilities within the current and future consumer Internet of Things (IoT) landscape. More specifically, the research aimed to deliver several key outcomes in relation to four objectives:

- **Evidence the future scale of consumer IoT across the UK**, covering the manufacture, adoption and spatial distribution of such IoT devices.
- **Evidence types of consumer IoT vulnerabilities**, in particular: (i) detailing the impacts associated with each type of vulnerability on consumers, businesses and the wider economy; and (ii) estimating the future growth of each type of vulnerability.
- **Evidence the impact of vulnerabilities and future risks**, i.e. the potential impact of consumer IoT vulnerabilities on the UK economy if exploited at scale, and the current and potential future risks of insecure consumer IoT devices, including the scale of cyber attacks using consumer IoT vulnerabilities in recent years.
- **Evidence the potential impacts of Government regulation** through prescribing a minimum IoT security baseline on different demographic, income and age groups, and the potential impact of a lack of IoT device ownership among specific economic groups in the UK.

1.2 Background – Consumer Internet of Things vulnerabilities

The Internet of Things (IoT) has been growing rapidly over the past few years. There were 8.4 billion devices or 'things' connected to the Internet in 2017 and it is estimated that there will be 20.4 billion IoT devices worldwide by 2020, growing to 75 billion by 2025.[5,6] In the UK, the number of IoT connections is predicted to grow from 13 million in 2016 to over 150 million by 2024.[7] Internet connected devices and associated services available for consumers to purchase in retail, to use at home or as personal wearables are known as consumer IoT devices. These are currently the largest category of connected 'things' and are expected to represent 63% of connected devices worldwide by 2020.[8]

Consumer IoT devices offer consumers greater convenience and an improved quality of life.[9] A study by McKinsey found that by 2025, consumer IoT could contribute some £155-£270 billion per year to the global economy as a result of more efficient energy management, labour savings through automation and the avoidance of injuries and fatalities as a result of improved home security.[10] However, despite the IoT's contributions to increased societal and economic productivity, consumer IoT devices also create significant challenges in terms of security and privacy.

Moreover, IoT security has not been given the importance it needs as many devices have poor security features, compromising consumers' privacy and security. [11] 'Smart' devices can be easy points of access for hackers to enter consumers' networks, thereby compromising the data that is transferred

[5] Gartner. (2017). Press Release.
[6] Statista. (2016). IoT Devices.
[7] Ofcom. (2017). Connected Nations 2017: Data analysis.
[8] Petrov, C. (2019). Internet of Things Statistics 2020 [The Rise of IoT]. Techjury.
[9] Parliamentary Office of Science & Technology. (2019). POSTNOTE 593: Cyber Security of Consumer Devices. Houses of Parliament.
[10] Manyika et al. (2015). Unlocking the Potential of the Internet of Things, McKinsey Global Institute.
[11] Capgemini. (2017). Consumer Security and the IoT.

across it. Attacks can also lead to infringements of data protection and privacy, financial losses, and physical safety being put at risk.[12]

Over the last few years, cyber attacks have become more common and are becoming increasingly sophisticated, complex and monetised. Practices that help hackers and cyber attackers to avoid detection have also become more common, making it difficult to detect when a consumer IoT device has been infiltrated. Consequently, consumers may not even be aware that their personal data has been compromised or that they are at risk of fraud until it is too late.

Against this background, in 2018, the UK Government published a Code of Practice (CoP) for Consumer IoT Security (CoP).[13] The aim was to improve baseline security and advance an industry-wide 'security by design' approach, which encourages manufacturers to "develop IoT devices with security as a central component of its use, rather than working backwards to try and create security measures via software updates or other tactics".[14] The aim was also to reduce the burden on consumers to configure their own devices.[15] The top three CoP guidelines include: all IoT devices should have unique passwords, which are non-resettable to any universal factory setting; a public point of contact for reporting vulnerabilities to the product manufacturer, and details of the minimum length of time that products will receive security updates.

In May-June 2019, DCMS carried out a consultation on regulatory proposals to improve the security of consumer IoT products.[16] This included the possibility of incorporating specific aspects of the voluntary CoP for IoT Security within a regulatory framework. The consultation stressed the need to ensure "manufacturers are clear and transparent with consumers by sharing important information about the cyber security of a device, meaning users can make more informed purchasing decisions".[17] The consultation put forward three different options, namely: a mandatory security label on consumer IoT products; mandatory use of the top three guidelines from the Code of Practice for IoT Security and the ETSI TS 103 645; and mandatory use of all thirteen CoP guidelines.

The purpose of this study was to gather additional evidence on the nature and magnitude of cyber security vulnerabilities across different IoT product groups, and the socio-economic impacts if such vulnerabilities are exploited.

1.3 Methodological Approach

The research combined a literature review, interview programme and a survey of consumers and businesses.

The literature review examined existing research, industry publications and 'grey' literature in relation to each of the study objectives. In total, some 80 different sources were examined, listed in Appendix A. In order to support the analysis, we conducted a total of 23 interviews with stakeholders. This included representatives of businesses manufacturing or using IoT devices, and industry and consumer associations. These interviews were mostly undertaken by telephone using an interview checklist that was approved by DCMS.

[12] Heartfield et al. (2018). A Taxonomy of Cyber-Physical Threats and Impact in the Smart Home. Computers & Security, Vol 78, pgs 398–428.

[13] Department for Digital, Culture, Media & Sport (DCMS). (2018). Code of Practice for consumer IoT security.

[14] Daube, N. (2019). Regulating the IoT: Impact and new considerations for cyber security and new government regulations, Help Net Security.

[15] Department for Digital, Culture, Media & Sport (DCMS). (2018). Code of Practice for consumer IoT security.

[16] Department for Digital, Culture, Media & Sport (DCMS). (2020). Consultation Outcome: Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation.

[17] Ashar, J. (2019). Regulatory proposal on mandatory IoT security label. GovTech Leaders.

In addition, two online surveys were undertaken, one targeting consumers of consumer IoT devices and one targeting businesses and other organisations (from different sectors and vary in size) who either manufacture, import or sell consumer IoT devices. The following table provides a breakdown of the responses.

Table 1.1: Summary – Survey Responses

Target Groups	No. Responses	Completion Rate
Consumers	57	56%
Business	51	43%
Total	**108**	**50%**

The consumer survey elicited a response from a total of 57 respondents, 45 of whom accessed the questionnaire via a link provided by GetSafeOnline. There is no evidence that the use of this link skewed the responses in favour of those who are likely to be more aware, or potentially have been a victim of online crime, but it is important to note that this could have been possible. The surveys were administered online, and therefore households in the UK without access to the Internet and who do not own IoT devices would not have been captured by the survey.

An analysis of the sample characteristics and responses for the two surveys is contained in the appendices to this report. It should be noted that the fieldwork for this research took place during the COVID-19 pandemic, which may have affected the response rate. The relatively small number of survey responses means that results should be treated as indicative and caution should be exercised in interpreting the findings.

The data captured via these means supported the development of a number of case studies illustrating real-life examples of cyber attacks on consumer IoT devices and the resulting impacts.

2. The Future Scale of Consumer IoT

Box 2.1: Key Findings: Evidence the future scale of consumer IoT

- In the UK, the number of IoT connections is predicted to increase to more than 150 million by 2024, with 80% of these connections coming from device categories such as wearables, connected media, smart meters and emergency calling services.[18]
- The future of the IoT is positive in terms of overall adoption and integration into users' lives – consumers are recognising the benefits of connected utilities and personal lifestyle items, from on-demand music and video streaming to hands-free device interaction and cloud storage of data.
- The convergence of new technologies (5G networks and Artificial Intelligence) can deliver significant benefits to users. For example, 5G networks boast increased processing speeds and widespread connectivity, while AI-based technologies continuously learn from massive datasets how to optimally perform tasks and automate often mundane activities. However, an increase in overall adoption of consumer IoT may also bring an increase in cyber security risks.
- Consumer IoT devices are currently most popular among the affluent and tech enthusiasts – these are the early adopters. Young people (under 16s and 16-24) are the most likely users of consumer lifestyle items, and smart home appliances are more popular among adults. These devices are less popular in the over-70s age demographic, but this could change in the next 5-10 years as devices become easier to use, more consumers realise how IoT devices can improve their lives, and remote communication, work and connectivity becomes part of everyday life.
- The main barriers to adoption include cost (both the product itself and of learning how to use it), scepticism of device security and a lack of consumer awareness of what the IoT entails. The main driver of consumer adoption is trust in the device and the brand.
- Low consumer awareness of security means that there is a lack of incentives for manufacturers to improve the cyber security of their products. In addition, competition and pressure to bring products to market results in shortcuts taken during the manufacture and design processes.
- Precise market forecasts are nuanced, as studies differ on the inclusion or exclusion of different "connected" consumer IoT devices. Furthermore, it is important when estimating the market size of each product category to account for retention rate, as consumers may purchase a device and then abandon it.

This section is divided into three broad product categories: (i) "big ticket" items (e.g. connected white goods/household items such as ovens, refrigerators, televisions); (ii) "connecting the home" items (e.g. smart speakers and home assistants, smart lighting, smart thermostats); and (iii) consumer lifestyle items (e.g. watches, toys, baby monitors). For each category, we examine existing research on the projected market size, both in terms of the number of devices and the number of connections, the routes for consumer adoption of these specific technologies, and the factors that deter consumers from purchasing them.

The backdrop to the study is that technological innovation is proliferating across all aspects of consumers' daily lives. Tracking personal health data or allowing users to adjust heating temperatures from their smartphones, are but a few examples of what consumer IoT devices can do.[19] IoT devices

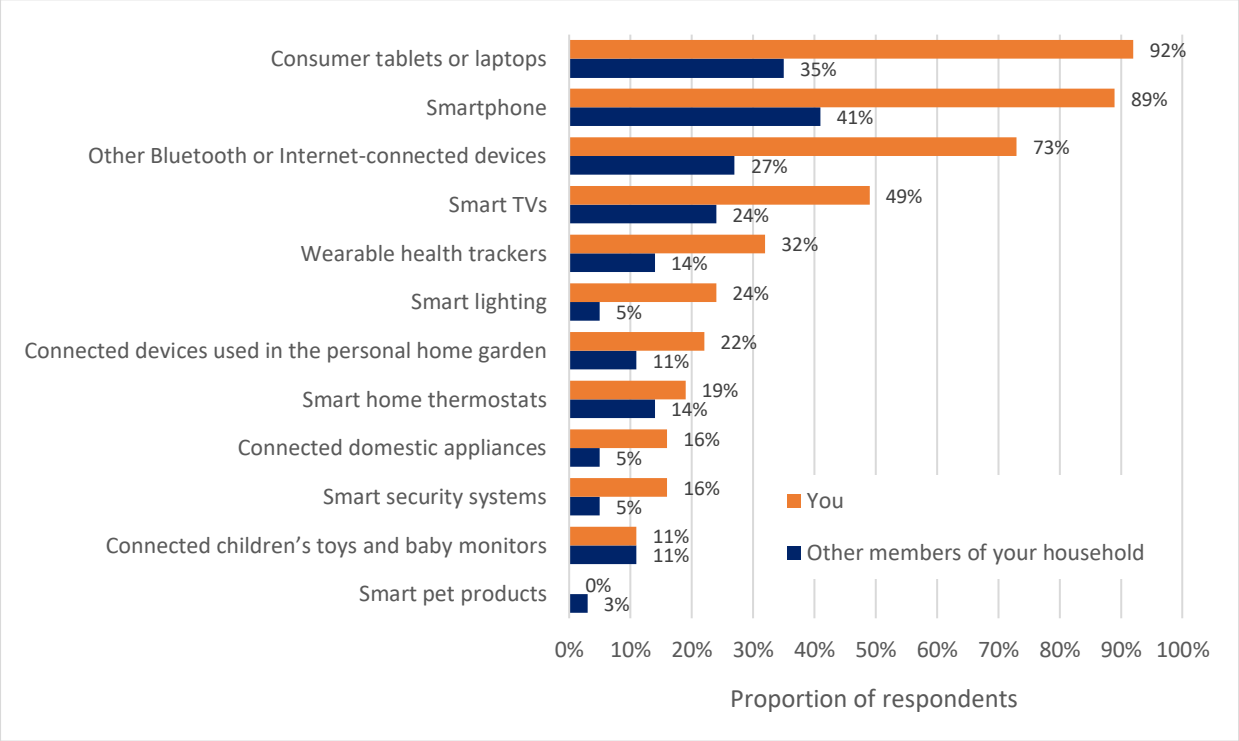
[18] Ofcom. (2019). Connected Nations 2019 UK Report.
[19] Mishra, R. (2020). 15 Examples of Internet of Things Technologies in Use Today.

represent an impressive convergence between basic hardware for everyday use and an Internet-based service.

The literature provides several estimates of an upward trend in IoT development and adoption, with the number of active, connected IoT devices in use worldwide estimated to currently be 21 billion—"active" here meaning devices that were purchased and are still in use. This number is likely to double to 42 billion connected IoT devices, generating 79 zettabytes (ZB) of data by 2025.[20]

In the UK, the number of connections is predicted to increase to more than 150 million by 2024, with 80% of these connections coming from device categories such as wearables, connected media, smart meters and emergency calling services.[21] Indeed, the wearables and white goods market are thought to account for over 40% of all consumer IoT devices currently.[22] The top smart products of 2019, in terms of ownership, were TVs, speakers, thermostats, wearables, smoke and gas leak detectors, and washing machines.[23] In addition, it is projected that by 2024, the total number of connected utilities, mainly smart meters, will be around 36.5 million worldwide, and up to 3 million in the UK.[24] However, one caveat is that the number of connections does not directly correspond to the quality of these connections. In other words, a large number of connections does not factor in the number of devices that may sit in the home unused after a few months of ownership, or that the actual connection to the network, and therefore functionality, meets the consumer's expectations.[25]

Figure 2.1: Respondent's Device Ownership and Other Members of Their Household's Ownership



Source: CSES Survey findings (consumers), Q8 & Q14 (N=37)

[20] International Data Corporation (IDC). (2019). The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast.
[21] Ofcom. (2017). Connected Nations 2017: Data analysis.
[22] Ofcom. (2017). Connected Nations 2017: Data analysis.
[23] techUK. (2019). The State of the Connected Home: Edition Three.
[24] Winchcomb, T., Massey, S., & Beastall, P. (2017). Review of the Latest Developments in the Internet of Things. Cambridge Consultants.
[25] Winchcomb, T., Massey, S., & Beastall, P. (2017). Review of the Latest Developments in the Internet of Things. Cambridge Consultants.

Existing research points to a substantial growth in the household utilities sector as developers find ways in which to connect these devices to the Internet, and to provide consumers with the myriad benefits these connections can bring.[26] More developers are identifying gaps — aspects of daily life that can be simplified or consolidated through the use of technology — and bringing their products to market. Indeed, this is an opportune time for entrepreneurship, and interviewees have pointed out a very promising phenomenon of cooperation and convergence between previously disparate sectors.

One interviewee highlighted an example of cooperation between connected cars and the home delivery industry: if a parcel recipient is away from home, the delivery person could use their car's GPS data to locate the recipient's vehicle. The recipient would provide the delivery person with a unique, single-use key to open their car boot, and when they return to their vehicle, the parcel would be there.[27] This is a potential solution to missed deliveries, and demonstrates the type of potential innovation in the consumer IoT space. However, even this example exhibits clear security concerns that would have to be addressed in order for such a service to be trustworthy. Another interviewee gave an example involving the convergence of smart metering data with the insurance industry which means being able to keep track of specific home metrics and know when to present users with products for water leak detection or coverage.

Alongside this creative boom is the emergence of 5G technology. 5G networks boast remarkably high download speeds, enabling faster streaming of entertainment services as well as communication, allowing for higher quality connections between edge devices and cloud services.[28] It is a key recommendation that 5G and other new technologies must be able to support up to 1 million IoT devices per square kilometre, as well as the instant response communications these technologies facilitate.[29] An example of the benefits of 5G is the improvement in remote control of consumer IoT devices, which allows the user to remotely interact with an object as if it were in front of them.[30] If connected to a 5G network, such action could be made more efficient and applied to a wider range of devices. However, as the number of connected devices on 5G networks increases, so too do the security risks. Respondents to the survey for this study mentioned that the increase in the number of devices on the market is likely to continue, and even accelerate, faster than the improvements in security.

Cyber security risks and threats, including those linked to emerging technologies, are further explored in Section 3. It should be noted that these risks are not necessarily new, as devices on 3G and 4G networks use remote Wi-Fi but 5G does present the additional challenge of more connected devices, and therefore a more widespread risk.

Both those interviewed for the study and the literature point out that the "hype" surrounding consumer IoT devices does not always align with the actual rate of adoption, or how advanced the technology is. As explained below, adoption routes and barriers vary between product categories, but the recent swell in enthusiasm for IoT products and innovation quite accurately follows the Gartner Hype Cycle: following an innovation trigger, there is a peak of inflated expectations in which "early publicity produces a number of success stories, often accompanied by failures. Some companies take action; many do not."[31] From there, consumers and the market enter a "trough of disillusionment", after which the capabilities and shortcomings of the products, and the actual needs of users are better understood.

For example, interviewees referred to a problematic practice that even well-known brands have implemented – companies will purchase products and parts from external manufacturers and simply

[26] Ofcom. (2017). Connected Nations 2017: Data analysis.
[27] Claburn, T. (2015). Your Audi As Amazon Package Drop.
[28] Huber, N. (2019). A Hacker's Paradise? 5G and cyber security. Financial Times.
[29] International Telecommunication Union (ITU). (2015). ITU defines vision and roadmap for 5G mobile development.
[30] Ofcom. (2017). Connected Nations 2017: Data analysis.
[31] Gartner. (n.d.). Gartner Hype Cycle: Interpreting technology Hype.

put their name on the final device without vetting for security gaps. Although a brand may have a substantial reputation and familiarity among its consumer base, this is not enough to guarantee its IoT products will be secure throughout their lifetimes. Therefore, these major brands should lead by example as the market continues to grow, and ensure their products are safe and transparent, before they are sold to consumers. Some examples of the feedback from the survey are provided below.

Box 2.2: Survey feedback regarding IoT cyber security incidents (quotes from businesses)

- "More products are being marketed which can only operate through apps which talk to the outside world before they deliver data back to the user. The apps create a marketing platform for companies wishing to reach their target audience. I don't see a let up to this. Strong cyber regulation should reduce the risk of there being an increase in breaches of vulnerability."
- "The IoT ecosystem is experiencing a disruptive-market surge, with endless new IoT devices reaching consumers and more and more 'old school' technologies becoming connected. These "old school" industries, such as the medical, industrial and even general consumer markets (e.g. smart watches, smart toys, smart dog collars, smart vacuums) do not possess the mentality of security-by-design and are having a hard time meeting consumers' expectations for easy integration and quick connectivity, combined with growing regulatory concerns for implementation of standards and best practices."
- "Most people can opt out of devices today, but that won't be the case later. Take-up of items is growing faster than cyber security improvements."
- "The number of devices will increase faster than the quality of security. Also, the longevity of devices is such that devices that are insecure today will remain active for a long time."

It is important to note that the data on the number of devices/connections and market projections available for the UK are limited, depending on product category. Most price estimates are in US dollars, and UK-specific projections are relatively sparse when compared to available global projections.

2.1 Big Ticket Items

This category refers to "smart" versions of popular, everyday household items, such as televisions, white goods and kitchen appliances. Some of these products can also be referred to as connected household utilities.[32] These devices are connected to the Internet to varying extents but may not have clear user interfaces. In other words, some devices may not have screens, or if they do, the options available for a user to interact or modify the device are limited. Such devices are often voice- or app-controlled, or have remedial functions that do not require extensive user interaction. Meanwhile, there is an abundance of activity taking place in the background, as the device communicates with other connected devices in the home, from the router to the light switches.

In 2017, 28% of households in the UK owned a smart TV, and indeed this was the most popular device. Devices such as wireless speakers, smart lighting systems, and connected home appliances such as dishwashers and refrigerators were not as widely adopted.[33] A survey conducted in 2018 revealed that 42% of UK households owned smart TVs, 20% had wearable devices, and 13% had smart speakers.[34] This trend continued in 2019, with 48% of consumers surveyed owning smart TVs, and it was predicted

[32] PwC. (n.d.). Disrupting Utilities.
[33] Winchcomb, T., Massey, S., & Beastall, P. (2017). Review of the Latest Developments in the Internet of Things. Cambridge Consultants.
[34] Parliamentary Office of Science & Technology. (2019). POSTNOTE 593: Cyber Security of Consumer Devices. Houses of Parliament.

that for those who only owned one consumer IoT device, that device was most likely to be a smart TV.[35,36]

Turning to routes for adoption, the research suggests that manufacturers and developers are generating substantial consumer interest around smart appliances, and the immense technological progress these devices represent. However, innovation does not necessarily mean consumers need or want to adopt these devices when their current, unconnected devices suffice. Indeed, "consumers have been underwhelmed by the idea of a robotic vacuum cleaner or being able to turn on their oven remotely," or, to take another example, a refrigerator that detects out-of-date products and synchronises the user's calendar.[37] It appears, according to the literature, that demand is simply not high enough for these innovations to significantly penetrate the home goods market.

Other barriers to adoption include cost, security concerns and ease of use (or a lack thereof). According to a 2019 techUK report, 59% of consumers across all age demographics believe IoT devices are too expensive and there are concerns regarding additional maintenance costs and complexity of operating these devices.[38] Furthermore, there is uneasiness regarding inadequate security, remote processing and device-to-device communication with minimal user interaction. This further dissuades potential customers, as the end consumer is held responsible for understanding the security risks relevant to their device and ensuring their device is secure. As one interviewee pointed out, users will consider the cost of learning how to operate a new device and to integrate it into their home in assessing how much convenience the device will realistically provide.

An additional barrier could be a consumer's housing situation. According to several interviewees for this study, users currently renting or in temporary accommodation are far less likely to purchase a smart big ticket item, and therefore this category tends to be most popular among homeowners. This factor may, it is argued, maintain the big ticket/connected white goods market's high-end status.

It should be noted that the use and acceptance of IoT devices varies among socio-demographic groups, and that ease of use and usefulness are two of the most important factors affecting whether a user will integrate a device into their home.[39] However, looking at future routes of adoption, an interviewee observed that in the last few years, older demographics have been developing the skills and competencies required to search the web for the products they want. Likewise, consumers in the 40-50 age group are buying smart home products on behalf of their retired parents who are living independently. This presents developers with an excellent opportunity to increase awareness among retired communities, both of the products and benefits available, but also of the key security features they should look out for.

2.2 Connecting the Home Items

Connected home devices build upon existing infrastructure embedded in the home; in other words, they allow users to control and monitor activity within their home, such as security systems, music, lights, and temperature. In many cases, they are the hubs through which device owners control the other connected devices and appliances in their home. However, smart speakers still fall behind smartphones in performing this role.[40]

[35] Ofcom. (2019). The Communications Market Report: Interactive Data.
[36] techUK. (2019). The State of the Connected Home: Edition Three.
[37] Winchcomb, T., Massey, S., & Beastall, P. (2017). Review of the Latest Developments in the Internet of Things. Cambridge Consultants.
[38] techUK. (2019). The State of the Connected Home: Edition Three.
[39] Tirado-Morueta, R., Aguaded-Gómez, J. I., & Hernando-Gómez, Á. (2018). The socio-demographic divide in Internet usage moderated by digital literacy support. Technology in Society, 55, 47-55.
[40] techUK. (2019). The State of the Connected Home: Edition Three.

With regard to market size, the literature suggests that the proliferation of connected home devices is increasing. This growth can be partially attributed to the "development of partnerships between smart home manufacturers and creators of smart speakers [which] enables smooth integration of smart home devices with the smart speaker."[41] This quote refers to manufacturers and developers responding to the tendency of users to control their network of smart home devices through smart speakers as a central hub, thereby taking advantage of these multifunctional devices' interoperability. At present, as one interviewee argued, smartphones are by a significant margin the most popular hub among consumers for controlling their other smart devices.

In addition, the research indicates that the growth of smart multi-function devices is due to the fact that they offer several services and enhancements on basic utilities. For example, being able to pick a song, order food, listen to an audiobook and check the weather – all via voice command – saves consumers time and effort, and appeals to a need for efficiency. However, a device's multi functionality does not guarantee that users will continue to use it. Considering voice-controlled devices specifically, a 2017 report found that there is only a 3% chance a user will be active in the second week of owning such a device.[42]

In terms of routes to adoption, the literature suggests that there are numerous socio-economic, as well as technical, factors contributing to the uptake in connected home items. On the socio-economic side, "the growth of the smart speaker market is primarily driven by the increased adoption of smart home technology, high disposable income, the popular trend of personalisation, and the rapid proliferation of multifunctional devices."[43] Interviewees for this study suggested that this multifunctional ability, such as the interoperability of smart devices — a smart speaker can be connected to and control other devices in the home — has led to improved natural language processing and voice recognition capabilities.[44]

The research suggests that with such a high potential for making life easier, smart speakers and home assistants are proving to be increasingly attractive consumer IoT products. Although cost is cited as a barrier to adoption, according to the research for smart security products, consumers are increasingly willing to adopt them, with up to 52% of a 2019 techUK survey's respondents stating they would pay more for the benefits that these technologies offer.[45] Familiarity with connected items, due in part to being raised with them from childhood or early adolescence, can also contribute to this growth. As with the other product categories, it is imperative for consumers to keep in mind that the most vulnerable IoT devices, according to interviewees working in cyber security, often cost less than £50.

In the coming years, a technical factor that could help minimise the burden on less advantaged users (e.g. vulnerable socio-economic groups, remote geographies, and older individuals) to learn how to use the device is voice control. For example, one interviewee mentioned major tech companies are working to embed voice control into the majority of their devices, which would allow less digitally literate populations to overcome operational complications by simply speaking to a smart speaker or assistant.[46]

2.3 Consumer Lifestyle Items

From smart watches and phones to connected children's toys, consumer lifestyle IoT devices have access to sensitive personal data, and therefore require meticulous design to protect such sensitive

[41] Kumar, R., & Rasal, A. (2018). Smart Speaker Market by Intelligent Virtual Assistant, End User, Distribution Channel, and Price – Global Opportunity Analysis and Industry Forecast, 2018-2025.
[42] VoiceLabs.co. (2017). The 2017 Voice Report: Executive Summary.
[43] VoiceLabs.co. (2017). The 2017 Voice Report: Executive Summary.
[44] VoiceLabs.co. (2017). The 2017 Voice Report: Executive Summary.
[45] techUK. (2019). The State of the Connected Home: Edition Three.
[46] Product Forge. (2018). IoT//GLA Meetup: Gary Clemo – Principal Technology Advisor at Ofcom.

data from being accessed and mishandled. Despite the privacy and security concerns, these devices are attractive to consumers because they promise convenience in one or more areas of daily life, are adaptable to different contexts, and provide personalised services.[47] Wearables, such as smart watches, can track health data such as number of steps, heart rate, sleeping patterns, and more. In time, this data could help users predict whether or not they will be more vulnerable to illness, for example.[48]

In terms of market growth, as the UK population becomes more health-conscious, users may be enticed to purchase these devices in order to track their physical health as they make lifestyle changes. Indeed, in 2015 it was predicted that the global smartwatch market could reach USD 18 billion by 2019.[49] In the UK "wearables are expected to be the most widespread device type by 2024 with approximately 28 million connections, and a move from using an additional device as a hub (e.g. a smartphone) to direct connectivity to the central network."[50] While such a move may promise additional convenience to users—for example, hands-free control of various devices at home—it also poses a key security concern: users are further separated from tangible control over each device, and direct connectivity to a central network means that if the device is hacked, attackers have instant access to all devices within a home. This could make it easier for attackers to conduct a DDoS attack, obtain user data, cause several devices to malfunction at once, or be held to ransom.

Aside from smartwatches, the UK toys and games market is projected to grow from £4 billion in 2017 to £5 billion in 2022, driven in part by innovation in connected toys "as millennials who grew up with technology begin having children."[51] An example of a connected toy is one that pairs a physical product with an app. However, the literature suggests that market growth depends on retention rates as well as initial purchases.

Due to increased privacy and security concerns – especially those concerning connected toys, wearables and speakers for children – as well as prominent legislation (such as the EU's General Data Protection Regulation), established to ensure data processors and controllers are more mindful of how information is gathered, what is gathered and why, consumers are ever more suspicious of their devices.[52,53] According to one estimate, around 10% of wearable owners no longer use their device(s), with 33% of these users abandoning their device within the first two weeks.[54] Of course, this is not the sole reason why users abandon their devices — other reasons could be functionality, and a lack of usefulness or relevance to daily life. Regarding the toys and games market in the UK, a report points to an emerging countertrend: parents diverting children away from screen-based play, and preferring to buy non-digital entertainment products such as board games and arts and crafts materials.[55]

Turning to routes for adoption, according to the research reviewed for this study, the most common users of these devices are young people (under 16s) who are generally quite comfortable using Internet-connected technology for recreational purposes and enjoy using new products with relative ease. In addition, the research suggests that wearable devices are popular among young professionals, with the highest smart device ownership in the UK appearing in the 25-44 age category.[56] However,

[47] Wilson, H. J., Shah, B., & Whipple, B. (2015) How People Are Actually Using the Internet of Things. Harvard Business Review.
[48] Digital Trends, (2020). The best blood pressure monitors for 2020.
[49] Gartner. (2016). Gartner Says Worldwide Wearable Devices Sales to Grow 18.4 Percent in 2016. Gartner.
[50] Winchcomb, T., Massey, S., & Beastall, P. (2017). Review of the Latest Developments in the Internet of Things. Cambridge Consultants.
[51] Cision. (2017). The UK Toys & Games Market 2017-2022.
[52] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[53] Hern, A. (2018). European Regulators Report Sharp Rise in Complaints After GDPR.
[54] Ericsson. (2016). Wearable technology and the internet of things, Consumer views on wearables beyond health and wellness.
[55] Cision. (2017). The UK Toys & Games Market 2017-2022.
[56] techUK. (2019). The State of the Connected Home: Edition Three.

the literature indicates that due to these devices' access to such personal data and possible naïveté when sharing information online, children and young people are at greater risk of falling prey to cyber criminals and hackers.[57] Educating the public on how their data is used or misused, and how devices are not always manufactured with ample security protections in place is a critical consideration.

2.4 Projections and future market trends

The IoT is constantly evolving and its definitions are becoming even more obscure; indeed, the existing projections and studies are quite nuanced, making the future of IoT device connections quite difficult to determine with any degree of certainty. As Ofcom has pointed out, projections with regard to market size, connections and device ownership do not take into account the myriad applications and categories of devices that have not yet been thought of or developed.[58] Indeed, it is highly dependent on the various demographic factors at play. There is no one type of device that the entire market will be predominantly interested in, so it is imperative that developers remain cognisant of how nuanced the demand among different groups will be.

The literature reviewed for this study points to some notable predictions. First, the number of "things" – connected devices that are not smartphones, laptops or tablets – is expected to outgrow computers in coming years.[59] At present, three out of every five consumers owns at least one smart home device although the type of device varies by age, as indicated earlier.[60] Indeed, interviewees agreed that a general popularisation of IoT products – more widespread acknowledgment and uptake beyond the small group of tech enthusiasts and affluent early adopters – will continue.

Second, the primary drivers for adoption of consumer IoT devices are heavily influenced by consumer expectations: devices should be easy to use, trustworthy, interoperable with other products in the home network, fun, and capable of making users' lives easier in some way. Again, it is important to consider the Gartner Hype Cycle, and the fate of businesses (manufacturers and retailers alike) that modify their marketing messaging, as well as the security of their products, versus those that do not. Interviewees for this study pointed out that if expectations among consumers become more realistic and balanced, manufacturers must take responsibility for servicing security throughout the lifetime of a consumer IoT product, and understanding whether or not they can meet their own profit goals whilst doing so. If a business cannot profit without taking shortcuts with regard to its products' security, and consumers become more mindful of how secure they want their devices to be, the business will eventually fail. Of course, it is likely that there will still be low-cost, low-security items on the market.

Third, due to IoT devices providing both physical capabilities and Internet connectivity, there is an emergence of new business models, most notably the as-a-service model. This model demonstrates how connected devices are more than speakers or watches; their Internet connectivity allows for a multitude of functions and features to benefit consumers.[61] As interviewees for this study pointed out, the rise of this new business model could prove promising for security developments, as companies using an as-a-service model rely more heavily on reputation and branding than they would if they simply developed and manufactured a product. This is due in part to the fact that consumers can more easily switch between service providers than when they invest in a physical product. As several interviewees argued, some major companies have moved away from one-off purchases, and instead offer subscription services, i.e. the user is purchasing the business's service, and the physical products are a part of this. Another consideration is the increase in remote working: consumers who spend a

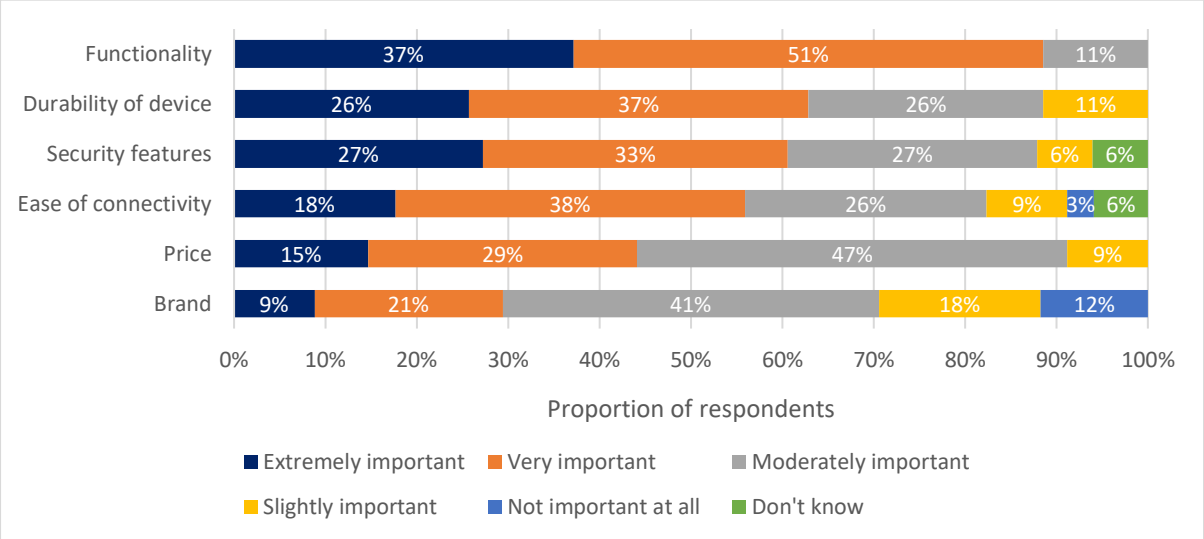
[57] al-Khateeb, H. M., & Epiphaniou, G. (2016). How technology can mitigate and counteract cyber-stalking and online grooming. Computer Fraud & Security, 2016(1), 14-18.
[58] Ofcom. (2019). Connected Nations 2019 UK Report.
[59] Lueth, K. L. (2014). IoT Market – Forecasts at a glance.
[60] techUK. (2019). The State of the Connected Home: Edition Three.
[61] Newman, Daniel. (2017). Why the as-a-service model works so well.

part or all of their work week at home may be attracted to consumer IoT devices that could improve their work environment, but also may be more wary of potential security risks that these devices pose.

According to the consumer survey conducted for this study, the most important factor consumers consider when purchasing an IoT device is functionality, with 88% regarding this as extremely or very important (see Figure 2.2). Interestingly, many respondents (47%) stated that price was only "moderately important", which may reflect some flexibility when assessing the cost of a device. In addition, security features were identified as the third most important factor (60% stating extremely or very important), behind functionality and durability (63% stating extremely or very important).

Consumers may acknowledge that security is crucial, but perhaps not know how to assess their device's security. As one participant in the research argued, the onus should not be on consumers to ensure their devices are secure in the first place, and manufacturers should provide ways to safeguard devices, rather than leaving it solely to the consumer. In addition, consumers may perceive functionality and security as interlinked; indeed, if a device is working well, it is less apparent that it is being compromised.

Figure 2.2: Consumer priorities when buying a consumer IoT device



Source: CSES Survey findings (consumer survey), Q20, N=35

At the root of consumer expectations is trust in the device, and while there is still an abundance of security and data privacy concerns, the trend of established appliance, entertainment and technology brands manufacturing their own smart devices may be leading to an unfounded increase in consumer trust.[62] Indeed, 32% of IT leaders cite security as the main barrier to success; although this is not the majority of IT leaders, it signifies a concern among members of this industry that security is and will become a significant barrier if it remains unaddressed.[63] As several interviewees mentioned, one of the key factors influencing the level of cyber security, or lack thereof, in consumer IoT devices is a lack of consumer awareness of what to look for in a device to ensure it is secure.

Similarly, without a unified standard or "stamp" to mark a device's security level, consumers have no clear way of determining whether or not the device they purchase will responsibly protect their data and remain secure throughout their use lives. However, there have been measures taken to raise consumer awareness of what constitutes a secure product; for example the NCSC published a one-pager on how to purchase secure IoT devices for Christmas presents.[64] This suggests that mass media

[62] techUK. (2019). The State of the Connected Home: Edition Three.
[63] Gartner. (2017). Leading the IoT.
[64] Levy, I. (2019). Staying smart with your Christmas gadgets.

publications should be more involved in informing audiences of practical cyber security measures they can take and products to look out for, rather than only reporting on incidents.

By 2023, home automation is expected to account for the largest share of the consumer IoT market. This applies to both big ticket and connecting the home items. According to one source, "the increasing demand for home monitoring in remote locations, growing adoption of home automation devices in applications such as security, HVAC (heating, ventilation and air conditioning) and energy management, among others, have been the key factors driving the growth of the consumer IoT market for home automation."[65] Still, another conclusion to be drawn is that policymakers should remain cognisant of the growth of cybercrime alongside the rapid, unpredictable growth of the IoT, as it appears to diminish consumer interest and trust in these devices. While, according to an interview conducted for this study, one of the key goals is to stimulate positive attitudes to IoT devices, this can only be achieved in the long-term if the products are secure and constantly maintained.

In conclusion, the evidence represented in the literature, the survey for this study, and stakeholder consultations, demonstrates that affordability, new technological innovations, and consumer awareness of IoT device security are significant aspects of future consumer IoT in the UK. Increasing device quality, and therefore trust, will greatly affect both the uptake of new and current devices on the market, and provide users with reliable technology that can simplify aspects of their daily lives.

[65] Research and Markets. (2019). Consumer IoT Market 2018 – Global Forecast to 2023: Market is Estimated to be USD 46.8 Billion by 2018 and is Projected to Reach USD 104.4 Billion.

3. Types and Impacts of Consumer IoT Vulnerabilities

Box 3.1: Key Findings: Types and impacts of consumer IoT vulnerabilities

- Cyber attacks are one of the most common types of crime in the UK.[66] The threat of cyber attacks is increasing as the number of devices connected to the Internet grows.
- There are a wide variety of attacks exploiting vulnerabilities in consumer IoT devices, such as spoofing, repudiation and Distributed Denial of Service (DDoS). The most common form of cyber attack belongs to the malware family, which can be delivered through botnets, as was the case for the Mirai botnet and its variants since 2016.
- Public-facing devices, such as routers and cameras are the most obvious targets for cyber-criminals.
- Default passwords are considered to be one of the most likely vulnerabilities to be exploited.
- Consumer IoT devices can lack security update options once the device has been manufactured, making them more prone to attack.
- The loss of consumer data and privacy breaches as a result of cyber attacks are seen to be very damaging by the majority of businesses consulted in this study. Compromised devices can lead affected individuals to not only be exposed to threats such as invasion of privacy, but also physical and psychological harm. Cyber attacks can also lead to reputational damage for manufacturers, as well as financial loss.
- Manufacturers' lack of knowledge in security-by-design, additional production costs and lack of consumer awareness do not encourage the integration of security features in IoT devices.
- The complexity of global supply chains introduces additional possibilities for vulnerabilities to make their way into manufactured devices.
- The future proliferation of 5G may potentially increase the avenues for consumer IoT cyber security attacks.

In the section below, we map out and identify the most common vulnerabilities that can be found in consumer IoT devices. We also assess the impact of these vulnerabilities, as well as the likelihood of these cyber security risks being realised.

3.1 Taxonomy of consumer IoT threats and vulnerabilities

Consumer IoT devices can provide economic and social benefits, and hence consumers and businesses are increasingly connecting items to the Internet, often without realising the potential risks that come with these IoT devices. According to the research reviewed for this study, the increase in devices that can be connected to the Internet has led to an increase in attacks not only against individual users, but also against critical infrastructure. There is widespread agreement across the literature that all consumer IoT devices are vulnerable to exploitation.[67]

> *"Whenever an appliance is described as "smart", it is vulnerable" – whether it is a fridge, a TV or a toothbrush" (Hyppönen's Law, Mikko Hyppönen)*

[66] National Crime Agency. (2016). Cyber Crime Assessment 2016.
[67] Houses of Parliament. (2019). Cyber security of consumer devices.

While each device category will have a variety of security gaps specific to the basic structure of the devices themselves, there are some common threats that all consumer IoT devices could face if basic minimum security features are not built in by design. The interviews that were conducted for this study found that hackers represent one of the main threats to the security of IoT devices. Frequently cited cyber security threats for consumer IoT devices in the literature involve attackers gaining access to sensitive data or systems, which can lead to the infringement of privacy and risking physical safety and security.[68,69] Through the literature reviewed it is possible to elaborate a taxonomy of different threats that are relevant to IoT devices (Table 3.1).

Table 3.1: Taxonomy of threats to consumer IoT devices

Threat groups	Examples and definitions
Physical attacks	Consumer IoT devices are physically located objects, which can be physically damaged or compromised.[70] Attackers may exploit a vulnerability in a device enabling them to execute commands. A cyber-security physical attack may be defined as a security breach in cyber space, which adversely affects physical space, and may breach privacy and lead to the unauthorised access to attacked devices. Examples would be the unauthorised switching on or off of lights, ventilation and heating.[71]
Distributed Denial of Service (DDoS)	A denial-of-service (DoS) attack is when an attacker uses a single computer to render a device or service unavailable to its intended users by flooding it with requests. A DDoS attack, on the other hand, utilises many sources (such as IoT devices) of attack traffic, often in the form of a botnet.[72] The study's interview programme revealed that DDoS is also one of the main cyber security threats relevant to IoT devices.
Unintentional damage (accidental)	Threats in this category might include devices using information from an unreliable source, such as a sensor producing unreliable readings. Automated smart home systems may be activated on the basis of the unreliable sensor readings.[73]
Failure / malfunctions	Consumer IoT devices are vulnerable to failures and malfunctions (such as software bugs). In some cases, this may result in a minor nuisance for the consumer (i.e. being unable to use the IoT device) or costlier damage (i.e. device might need to be reset by the user, erasing stored data). Exploiting failures can facilitate other threats. For example, if an IoT device has lost access to the Internet, it may search for other networks to connect to, allowing it to be hijacked. The absence of adequate patch pipelines is an ongoing failure for IoT devices, with some products being difficult to patch, even when vulnerabilities are known.[74]
Outages	Smart home devices (and other IoT devices) rely on a range of resources and services to provide sophisticated functionality. If any of these components face an outage (network or power outage), the functionality of the device itself might be affected.
Eavesdropping / interception / hijacking	Due to the large number of sensors on consumer IoT devices, a lot of personal data is collected (behaviours in the home, health, etc.). Smart devices also communicate with one another via wireless protocols, such as Wi-Fi, Z-wave,

[68] Loukas. (2015). Cyber-physical attacks: a growing invisible threat. Butterworth-Heineman.
[69] Heartfield et al. (2018). A Taxonomy of Cyber-Physical Threats and Impact in the Smart Home. Computers & Security, Vol 78, pgs 398–428.
[70] ENISA. (2014). Threat Landscape and Good Practice Guide for Smart Home and Converged Media; and IoT.
[71] Heartfield et al. (2018). A Taxonomy of Cyber-Physical Threats and Impact in the Smart Home. Computers & Security, Vol 78, pgs 398–428.
[72] Cloudflare. (n.d.). What is a Denial-of-Service (DoS) Attack?
[73] ENISA. (2014). Threat Landscape and Good Practice Guide for Smart Home and Converged Media; and IoT.
[74] Stanislav, M., et al. (2015). Hacking IoT: A case study on baby monitor exposures and vulnerabilities. Rapid7.

Threat groups	Examples and definitions
	Zigbee and Bluetooth which lack proper encryption. A lack of encryption in some IoT devices could lead to devices being compromised, as was the case with keyboards with the KeySniffer vulnerability.[75]
Nefarious activity	The exploitation of a vulnerability to access personal data, which can lead to financial loss, invasions of privacy and fraud.
Spoofing	Spoofing is when an attacker creates an Internet Protocol (IP) packet with a modified source address to hide their identity. A spoofing attack can stop or start the device without warning, or it can modify how the device collects and transfers user data. This can affect consumer security and privacy and re-route their personal data to an untrustworthy source.
Tampering	Tampering means modifying a sensor's software, thereby altering its data sharing permissions. This can open the door for hackers to install malware or spyware in the device, leading to long-term privacy invasion.
Repudiation of actions	A repudiation attack is when an application or IT system does not implement the appropriate controls to track and log users' activities, which in turn allows new user actions to be forged or manipulated undetected. This form of attack can be used to modify the authoring information of actions executed by an attacker in order to log wrong data files.[76] This can lead to data manipulation in the name of others, as with spoofing mail messages, and make the data stored in log files misleading or invalid. An example of a repudiation attack would be impersonating a senior manager's email, by accessing the company's email server.[77]
Information disclosure	This involves password/credential leaks or modification and can be especially problematic if only one password is required to access an entire home network, or if devices within the network share the same password.
Elevation of privilege	Provides a hacker with unauthorised access to a cloud service provider's system. Such privileges enable a hacker to commandeer and control a device.
Unsupported endpoint management	This mostly occurs on unsupported devices which will have known vulnerabilities or bugs after being on market for a long period of time.[78] Their outdated software or firmware leaves them prone to exploitation. Some devices may be so outdated that they are unable to encrypt user data or assign a "root of trust".

Cyber attacks can cause physical damage to connected devices if a hacker manipulates an internally compromised device to operate it maliciously. For example, a hacker could potentially compromise the thermostat on a fridge which would prevent it from operating properly and potentially cause damage.[79] It is therefore in the interests of consumers and businesses to safeguard against such attacks.[80] According to the research, there are vulnerabilities that have not yet been fully exploited but constitute a potential risk. For example, remote control of lights, or other connected "things", which might not have monetary or physically damaging effects, but can be used to facilitate harassment that instils fear and affects the mental wellbeing of victims.[81]

[75] All, A. (2016). New IoT Threat Exploits Lack of Encryption in Wireless Keyboards. eSecurity Planet.
[76] OWASP. (n.d.) Repudiation Attack.
[77] Pastore, M. A., & Dulaney, E. A. (2006). CompTIA security study guide. Indianapolis, IN: Wiley.
[78] Moor, J., Marshall, R., & Walsh, S. (2018). IoT Security Architecture and Policy for the Home – A Hub Based Approach. IoT Security Foundation.
[79] NNT. (2019). Cyber-Security of the Fridge: Assessing the Internet of Things Threat.
[80] Parliamentary Office of Science & Technology. (2019). POSTNOTE 593: Cyber Security of Consumer Devices. Houses of Parliament.
[81] Kim, S., Kimber, M., Boyle, M. H., & Georgiades, K. (2019). Sex differences in the association between cyberbullying victimization and mental health, substance use, and suicidal ideation in adolescents. The Canadian Journal of Psychiatry, 64(2), 126-135.

3.2 Exploitation of consumer IoT device vulnerabilities

It is estimated that there will be 21.5 billion IoT devices in 2025, up from 7 billion in 2018.[82] Furthermore, the International Data Corporation (IDC) predicts that connected IoT devices will be generating 79.4 zettabytes (ZB) of data in 2025.[83] As the number of IoT devices increases, so will the cyber-security risks. According to research from the Office of National Statistics (ONS), cyber attacks are involved in more than half of fraud cases in England and Wales and computer misuse is the fourth most frequent form of crime, which involves the use of viruses or other malware.[84, 85]

Hackers and other cyber-criminals exploit consumer IoT device vulnerabilities, not only to attack the device itself, but also as a jumping-off point for other types of threats (see Table 3.1). Since consumer IoT devices are connected to the Internet, this can serve as a means for malware to access the device itself and can compromise all other devices connected to the network.[86] This form of attack on an IoT device, called a 'man-in-the-middle attack', was recognised by an interviewee for this study as an additional threat to connected devices. Another way to exploit vulnerable consumer IoT devices is through botnets: a network of systems that control and distribute malware to gain private information and compromise the integrity of networks, often without the knowledge of the owner of the device.[87]

Multiple compromised consumer IoT devices may be used for Distributed Denial of Service (DDoS) attacks or cryptocurrency mining. A Denial of Service (DoS) attack, in particular, significantly threatens the wider network, especially if such an attack is distributed (DDoS). DDoS attacks on a company may limit resources, curtail revenue and yields, as well as causing customer dissatisfaction.[88] With regard to cryptocurrency mining, illicit mining occurs when malicious cyber actors gain access through malware to web-browsers, IoT devices and mobile devices, to steal their computer processing power and mine cryptocurrencies, which has a monetary value.[89] It is believed that cryptocurrency mining has become a more common threat in recent years; according to Symantec, cryptocurrency mining malware detections increased from nil to a few thousand between 2014-2017, to more than 150,000 in 2018.[90]

The first malware that targeted IoT devices ('Tsunami') was identified in 2002. In the 12 years that followed, most malware was similar in nature to 'Tsunami'. For example, 'Psyb0t' (2009) and 'Gafgyt' (2014), which targeted Linux machines and architecture, using common usernames and passwords to infect devices.[91] By 2015, attacks started becoming more complex, targeting multiple platforms at once and using social media click-fraud attacks (for example, via Instagram). This study's interview programme indicated that another way IoT devices may be exploited is through ransomware, a form of malware that encrypts the files of its victims and then demands a fee from the victim in order to unlock the information.[92]

In 2016, the 'Mirai' botnet made headlines around the world after it was used to implement one of the largest DDoS attacks which reached 1 billion TeraBytes Per Second (Tbps), with Tbps in this case

[82] Lueth, K. L. (2018). State of the IoT 2018: Number of IoT devices now at 7B — Market accelerating.
[83] International Data Corporation (IDC). (2019). The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast.
[84] Office for National Statistics. (2019). Crime in England and Wales: year ending December 2018.
[85] Office for National Statistics. (2020). Crime in England and Wales: year ending December 2019.
[86] Hypponen, M., et al. (2017). The Internet of (Vulnerable) Things: On Hypponen's Law, Security Engineering, and IoT Legislation. Technology Innovation Management Review, 7(4).
[87] BizIntellia. (2020). Trending: IoT malware attack.
[88] Alomari, E., Manickam, S., Gupta, B. B., Karuppayah, S., & Alfaris, R. (2012). Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art. International Journal of Computer Applications, 49(7), 24–32.
[89] CyberThreat Alliance. (2018). The Illicit Cryptocurrency Mining Threat.
[90] Symantec. (2018). Internet Security Threat Report (ISTR).
[91] F-Secure. (2019). IoT threat landscape: old hacks, new devices.
[92] Fruhlinger, J. (2018). Ransomware explained: How it works and how to remove it.

corresponding to the speed of malicious traffic during an attack. As attacks of this type increase in scale and frequency, they will further challenge service providers' ability to defend against them.[93]

According to the literature, after 2017, the number of IoT threats targeting devices increased significantly. Indeed, the malware family behind 39% of attacks is the Mirai botnet.[94] Malware has since become increasingly sophisticated and is targeting an increasing number of vulnerabilities in consumer IoT devices. For instance, in 2018 the ADB.Miner botnet used the Mirai code to infect devices with an exposed Android Debug Bridge (ADB), a command-line tool which facilitates communication with an Android device enabling the installing and debugging of apps, highlighting the expansion in the use of this type of malware code.[95] In 2018, the ADB botnet was able to infect 7,000 android devices, including 5,000 in only 24 hours.[96] Based on a mapping of IoT botnets since 2002, cyber security company F-Secure developed a list of common characteristics of IoT attacks.

Box 3.2: Common characteristics of IoT attacks[97]

- Target embedded computers in devices, such as closed-circuit cameras, routers and DVRs;
- Use hard coded or default passwords to gain access;
- Co-opt computing power into a botnet for illegal purposes, including DDoS attacks, spam and click-fraud;
- Build-on malware from previous threats (e.g. the Mirai bot, which has been the foundation of an increasing number of malware targeting IoT devices);
- Utilise more complicated forms of payloads, through which device vulnerabilities are exploited when triggered by the victim of an attack, such as malicious script in an email.

A selection of feedback provided by respondents in both the business and consumer surveys (Box 3.3) for this study illustrates a range of views on cyber vulnerabilities.

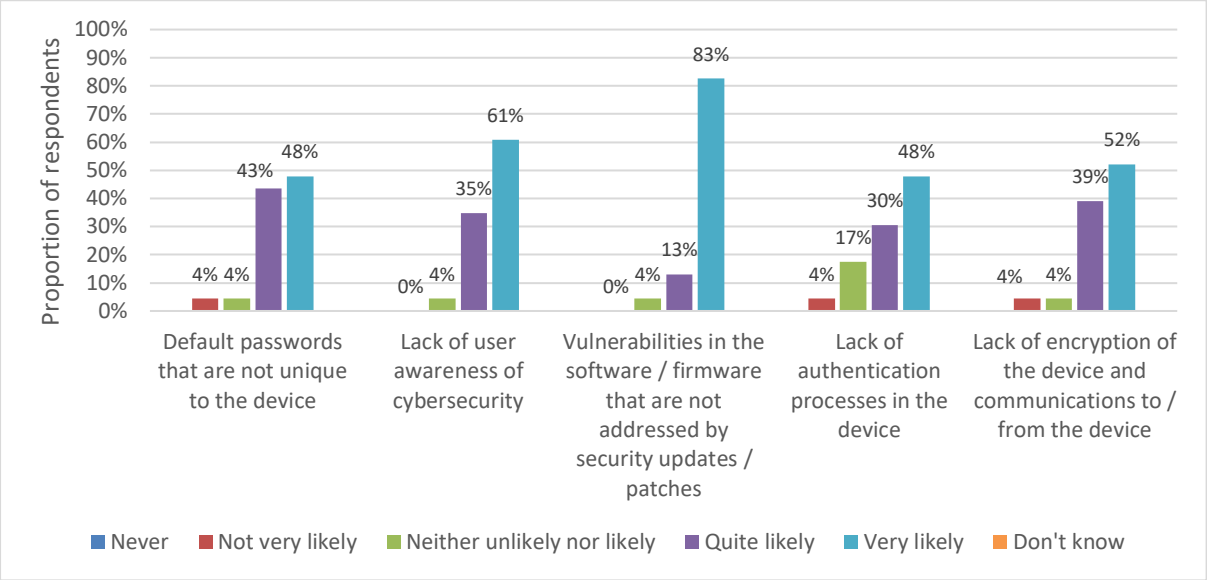
Box 3.3: Survey quotes from businesses and consumers on IoT cyber security vulnerabilities

- "Many vulnerabilities in consumer devices are not yet exploited."
- "The older age categories are likely to be have [sic.] greater concerns for their privacy and therefore happy to spend time inputting multiple security answers."
- "Those who are the youngest and the oldest may not understand the security requirements so it needs to be communicated in a very simple, clear way. Particularly those under 18 and those between over 45. All ages need to be made aware of how passwords should be unique, etc."
- "Too many IoT devices are being plugged into the Internet with no security software at all."

The business survey for this study also indicated that the majority of respondents see default passwords as being very likely to be exploited by attackers, as shown in Figure 3.1.

[93] Cloudflare. (2017). Inside the Infamous Mirai IoT Botnet: A Retrospective Analysis.
[94] Kaspersky. (2019). IoT under fire: Kaspersky detects more than 100 million attacks on smart devices in H1 2019.
[95] NJCCIC. (n.d). Cyber Threat Profiles: Cryptocurrency-Mining Malware.
[96] Osborne, C. (2018). ADB.Miner worm is rapidly spreading across Android devices.
[97] F-Secure. (2019). IoT threat landscape: old hacks, new devices.

Figure 3.1: Perceived likelihood of vulnerabilities being exploited in consumer IoT devices



Source: CSES Survey findings (businesses and other organisations), Q8, N=23

One interviewee for this study remarked that the most significant change in future will be the speed, scale, and the effort required by attackers to execute attacks, which will be more automated and complex, and some of them will incorporate elements of machine learning and AI. As such, there are different ways attacker exploit the different forms of vulnerabilities in IoT devices, and these will evolve and become more widespread in the future. Against this background, businesses involved in the manufacturing of IoT products and governments will need to develop a holistic approach to addressing the most common vulnerabilities.

3.3 Consumer IoT device vulnerabilities

As IoT devices use different types of technologies (software, hardware, operating systems, cloud services, etc.), there are many ways to exploit vulnerabilities. Vulnerabilities in IoT devices might be exploited, for example, through network software attacks, such as so-called 'worms' and remote attacks. Other attacks include DDoS and botnets as well as those perpetrated by individual hackers.[98] Moreover, the implementation of security controls is not always feasible due to the inherent limitations of IoT devices, for example resource and computational power limitations that might prohibit the use of access control mechanisms, encryption, key management structures and certificate schemes.[99]

Public-facing devices, such as routers, cameras and digital video recorders (DVRs) remain the most obvious target for cyber-criminals. Several interviewees for this study pointed to the likelihood that by connecting more devices to the Internet, these new interfaces will increase the possibilities and likelihood of new cyber attacks. It was argued that many IoT devices are also not built with 'security-by-design' features. The most vulnerable device in a home is likely to be the one that connects all other devices to the Internet. Thus, a study by the American Consumer Institute found that more than 8 out of 10 home and office routers were vulnerable to hacking.[100] The same study found that users

[98] Cruz, B., Gómez-Meire, S., Ruano-Ordás, D., Janicke, H., Yevseyeva, I., & Méndez, J. R. (2019). A Practical Approach to Protect IoT Devices against Attacks and Compile Security Incident Datasets. Scientific Programming, 2019, 1–11.
[99] Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the Internet of Things: Security and privacy issues. IEEE Internet Computing, 21(2), 34-42.
[100] The American Consumer Institute Center for Citizen Research. (2018). Securing IoT Devices: How Safe Is Your Wi-Fi Router?

might not even be aware that their routers have been compromised. With a technique called Domain Name System (DNS) hacking, hackers can redirect traffic to a phishing website, where consumers are prompted to disclose credit card numbers or login credentials.[101]

5G will accelerate the use of IoT devices as it will allow more low-power devices to become Internet-connected.[102] A Brookings Institute report highlights, however, that the proliferation of 5G will provide the following additional avenues for cyber security attacks: first, the 5G network is managed by software even more than 3G and 4G networks. The increased reliance of networks for virtualised functions in software, instead of using hardware appliances, increases cyber vulnerability. Second, there is a risk related to attaching billions of hackable smart devices to a network.[103] The threat will grow with increased number of devices. An additional vulnerability linked to the switch to the infrastructure of 5G is that even when it is possible to lock down the software vulnerabilities within a network, the network is also managed by software that itself can be prone to attack. An attacker who gains control of the software managing the networks can therefore also control the network.[104] However, cheaper and potentially less secure alternatives to 5G will remain in the market, so 5G in the long-term might be a more secure connection, albeit more costly.

The Open Web Application Security Project (OWASP) Internet of Things Project, launched in 2014, started as a way to help developers, manufacturers, enterprises and consumers make better decisions regarding the creation and use of the IoT. OWASP updated its top 10 list of vulnerabilities in 2018 and mapped the risks to avoid when building, deploying or managing IoT systems. The list brings together high priority vulnerabilities, which are applicable to consumer IoT devices. The European Telecommunications Standards Institute (ETSI), like OWASP, presents a list of vulnerabilities for consumer IoT such as 'no universal default passwords' (4.1) and 'keep software updated' (4.3).[105, 106] The interview programme carried out for this study further highlighted default passwords as one of the main consumer IoT device vulnerabilities.

Table 3.2: IoT Top 10 vulnerabilities

Type of vulnerability	Description
Weak, Guessable, or Hardcoded Passwords	Examples of weak passwords include passwords that are publicly available, have unchangeable credentials, include backdoors in firmware or software that grants unauthorised access to deployed systems. Other password vulnerabilities include passwords that can be easily guessed through brute-force, which is the submission of multiple password combinations until the correct one is selected.
Insecure Network Services	Insecure network services running on the device itself, especially those exposed to the Internet, that compromise the confidentiality, integrity, or availability of information or allow unauthorised remote control.
Insecure Ecosystem Interfaces	Insecure web, backend Application Programming Interface (API), cloud, or mobile interfaces in the ecosystem outside of the device which allow the device or its related components to be compromised. Common issues include a lack of authentication / authorisation, lacking or weak encryption, and a lack of input and output filtering.
Lack of Secure Update Mechanism	Lack of ability to securely update the device. This includes a lack of firmware validation on devices, a lack of secure delivery (un-encrypted in transit), lack

[101] Imperva. (n.d.) Domain name server (DNS) Hijacking.
[102] Jarman, B. (2019). 5G and Smart Homes: What You Need To Know.
[103] Wheeler, T., & Simpson, D. (2019). Why 5G requires new approaches to cyber security.
[104] Wheeler, T., & Simpson, D. (2019). Why 5G requires new approaches to cyber security.
[105] ETSI. (2019). CYBER; Cyber Security for Consumer Internet of Things. Valbonne-Sophia Antipolis: ETSI.
[106] ETSI. (2019). CYBER; Cyber Security for Consumer Internet of Things. Valbonne-Sophia Antipolis: ETSI.

Type of vulnerability	Description
	of anti-rollback mechanisms, and a lack of notifications of security changes due to updates.
Use of Insecure or Outdated Components	Use of outdated or insecure software components that could allow the device to be compromised. This includes insecure customisation of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain.
Insufficient Privacy Protection	Users' personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.
Insecure Data Transfer and Storage	Lack of encryption or access control to sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.
Lack of Device Management	Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.
Insecure Default Settings	Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.
Lack of Physical Hardening	Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.

Source: OWASP. (2018). IoT Top 10

An additional vulnerability identified by the interviews is the lack of avenues for consumers to disclose or report a vulnerability in one of their devices, which could prevent manufacturers from implementing the necessary security measures. However, as argued by several interviewees, the onus on implementing cyber security measures should not be on consumers but rather it should be the responsibility of producers of IoT devices to make their products both user-friendly and secure.

3.3.1 Vulnerabilities arising from insecure IoT device design

Technical problems are one of the main causes of consumer IoT vulnerabilities. It is unlikely that there will be a time when new vulnerabilities are no longer discovered; therefore, as many interviewees for this study pointed out, the security of an IoT device depends on systems being kept up to date. There is common agreement in the literature that software or operating system flaws cannot be entirely avoided and that many will be, or will become, vulnerable to exploitation.[107,108]

On a traditional computer, access controls are required to satisfy basic security requirements. Even if these controls contain bugs or may be rendered obsolete when faced with a novel attack, traditional computers can be updated and patched, or the system redesigned to address vulnerabilities. Moreover, it is also relatively difficult for producers to patch IoT devices, as well as costly. [109,110] The consumer watchdog Which? estimates that there are more than a billion Android devices in the world that are vulnerable to attack because they run the Android 6.0 Operating System (OS) or lower, which has not been supported by security updates throughout 2019.[111] To further illustrate the scale of this challenge, it is estimated that 42% of active Android users worldwide are on version 6.0 or earlier and

[107] Prpl Foundation. (2016). Security guidance for critical areas of embedded computing.
[108] National Cyber Security Centre (NCSC). (2017). Secure development and deployment.
[109] Kh, R. (2018). Patch Management is the Catalyst for Growth in the IoT Industry. Datafloq.
[110] Thales. (n.d). Implementing Cost-efficient Software Updates for Cellular IoT Deployments: Challenges, Considerations, Best Practices.
[111] Laughlin, A. (2020). More than one billion Android devices at risk of malware threats. Which?

at least 7% of UK mobile phones are using Android 6 or below.[112,113] Unlike traditional computers, however, many consumer IoT devices generally lack reasonable update and upgrade options once the device has left the manufacturer's warehouse.[114]

The findings across a variety of studies highlight the absence of a fast, reliable and safe patch pipeline among all consumer IoT devices. According to a study by Rapid7: "A commonly accepted way to effect a rapid rollout of patches (across consumer IoT devices) simply does not exist."[115] Even when a vulnerability is identified and can be fixed, these devices are difficult to patch for a number of reasons, and often specific to the device. These reasons include the lack of device interfaces which would make it easier for consumers to update the device themselves. For a majority of IoT devices, the constraints of remote updates may also outweigh their benefits, while their physical maintenance might be prohibitively costly or too time-consuming.[116] Moreover, users are often not informed when their device software undergoes an update, and therefore are not familiar with the software update process.[117]

Since it is difficult, or even impossible in some cases, to update the software on a consumer IoT device, some companies themselves cannot track cyber security vulnerabilities. For example, Gemalto carried out a study to assess the state of IoT security and found that globally, almost half (48%) of companies, still cannot detect if any of their IoT devices have been breached, despite companies increasing their focus on IoT security (spending on protection has grown from 11% of IoT budget in 2017 to 13% in 2018).[118] Further exacerbating this issue is the fact that the software used in many consumer IoT devices is not developed by the manufacturer of the product, but rather by a third-party. This can lead to additional complexity in product development and maintenance once on the market, as discussed in the following section. A prominent example is the Android OS which is developed and maintained primarily by Google but used by many different smartphone manufacturers.

3.3.2 Vulnerabilities arising from business models and economic incentives

In addition to outdated software, another significant source of vulnerability stems from the way the consumer IoT market is currently configured and the failure of manufacturers to learn from past vulnerabilities.

The research reviewed for this study suggests that there are two types of new entrants to the consumer IoT device market: first, large manufacturers that add connectivity to existing appliances (smart fridges, smart TVs for example); and secondly, small and medium-sized companies that are creating new devices from scratch. New developers of consumer IoT devices may have little experience in security engineering and smaller producers may have a smaller budget to dedicate to device security, which will affect device security as they could adopt generic hardware and firmware instead, with well-known or unknown unpatched vulnerabilities.[119]

Other research suggests that some IoT devices have limited capacity to include security features (i.e. encryption or security updates).[120] Even though technical problems in some devices (such as software or operating system bugs) have been identified and solved, the same issues continue to plague the

[112] Android.Developers. (2020). Distribution dashboard.
[113] DeviceAtlas. (2019). Blog: Mobile OS versions by country.
[114] Stanislav, M., et al. (2015). Hacking IoT: A case study on baby monitor exposures and vulnerabilities. Rapid7.
[115] Stanislav, M., et al. (2015). Hacking IoT: A case study on baby monitor exposures and vulnerabilities. Rapid7.
[116] Thales. (n.d). Efficient and Secure IoT Device Software Updates.
[117] Wallen, J. (2017). Most IoT devices are an attack waiting to happen, unless manufacturers update their kernels. Tech Republic.
[118] Gemalto. (2019). Almost half of companies still can't detect IoT device breaches, reveals Gemalto study.
[119] ENISA. (2014). Threat Landscape and Good Practice Guide for Smart Home and Converged Media; and IoT.
[120] Maple. (2017). Security and Privacy in the Internet of Things. Journal of Cyber Policy, 2, 155-184.

consumer IoT market, particularly because manufacturers continue to place un-patchable consumer IoT devices on the market.

The UK Government's 2018 Secure by Design report concluded that manufacturers lack sufficient economic incentive to incorporate security features into devices.[121] Previous research also found that manufacturers place security below other priorities, such as performance, costs and time-to-market.[122,123,124,125] A survey by McKinsey found that over 40% of companies said their customers are either unwilling to pay a premium for security, or expect security costs to decline over time.[126] Since consumers seem unwilling to pay for additional security measures, this does not encourage investment in security features.

Compounded with the lack of incentives described above, the previous research suggests that the heavy reliance on cloud computing for storage and the provision of services means that consumer IoT devices have known unpatched vulnerabilities, or unknown vulnerabilities which once discovered, will affect a wide range of devices. One explanation for this is that reusing cloud-based resources means that the ownership for developing and deploying patches and other security upgrades remains unclear, and therefore unallocated.[127] Further to this, a number of studies have identified the vulnerability of consumer IoT device supply chains, which to date has largely been overlooked.[128] Some of the comments from the respondents to the consumer and business survey on the question of the design features and business models behind the production of IoT devices in Box 3.4 seem to confirm the view on the pitfalls of existing IoT business models.

Box 3.4: Consumer and Business Survey feedback on cyber-security features in IoT products

- "Manufacturers have little incentive to incorporate security features, since doing so costs money, potentially makes the product more difficult for the customer to use, the market isn't demanding security features and consumer protection legislation doesn't mandate them"
- "The number of devices will increase faster than the quality of the security. Also, the longevity of devices is such that devices that are insecure today will remain active for a long time"
- "It is not just the IoT device which must follow good practice, the home user must also configure their network and firewall correctly. Broadband providers and router manufacturers need to be included in the scope of the IoT industry not just the end point device manufacturers"
- "Incidents will increase, usually due to basic human error. Testing needs to be vigilant before a product is released. Engineers should not be afraid to challenge decision makers when a product isn't safe or ready in terms of security"

Since consumer IoT devices are composed of different interconnected components that are designed, manufactured, and operated by entities that are usually located in different parts of the world, the integration of all these components makes the system vulnerable to cyber attacks. This may include hardware manufacturers, cloud providers, and the developers of operating systems and third-party applications. The complexity of global supply chains provides many opportunities for vulnerabilities to

[121] Department for Digital, Culture, Media and Sport (DCMS). (2018). Secure by Design: Improving the cyber security of consumer Internet of Things Report.
[122] ENISA. (2015). Threat landscape for smart home and media convergence.
[123] ENISA. (2016). Common position on cyber security.
[124] ENISA. (2015). Security and resilience of smart home environments.
[125] Joint Committee on the National Security Strategy. (2016-2017). Cyber security: UK national security in a digital world inquiry.
[126] Bauer, H. et al. (2017). Security in the Internet of Things. McKinsey & Company.
[127] Stanislav, M., et al. (2015). Hacking IoT: A case study on baby monitor exposures and vulnerabilities. Rapid7.
[128] Farooq, J., et al. (2019). IoT Supply Chain Security: Overview, Challenges, and the Road Ahead.

be introduced, either inadvertently or deliberately.[129] For example, companies need to be aware of vulnerabilities in their supply chain and understand that they might be using individual components that have poor levels of cyber security, preventing their final product from being 'secure by default' . This can lead to instances where the suppliers and the risks that they might bring to different components of an IoT system are not investigated. [130] It is not only difficult for retailers and final product manufacturers to validate the security claims of their products, but it is also difficult to establish responsibility for security.[131] Moreover, attackers can exploit complex supply chains by, for example, implanting malware into a software update or third-party application.[132,133]

Finally, there is a privacy and security risk created by businesses that engage in behavioural surplus data collection as a business model. Behavioural surplus is data going beyond the standard online product and service use and may include information about a person's location, profession, age.[134] Facebook and Google, for example, use it to make predictions about customer behaviour.[135] This risk can be further categorised into two areas. The first is the business model itself, under which data on user behaviour is collected – usually not personally identifiable data but rather meta-data – and used in aggregate for analysis, interpretation, tagging and flagging for targeted advertisement and predictions of user behaviour.

Every smart or IoT device, and even more so with personalised functionalities, is a potential source of such behavioural data.[136] The privacy implications are invisible to consumers, as is the supply chain of third parties involved, which are often allowed access to meta-data. This risk is hardly captured by legislation but these behavioural data are broadly used as a commodity. For example, the CEO of a company which produces autonomous vacuum cleaners, stated that the devices evolved in a way to incorporate cameras and tracking location in order to create floorplan maps of the houses they were cleaning; a by-product that he claimed was to be sold to tech giant companies.[137] The second aspect of this business model is that users who do not accept the terms and conditions might be offered limited device functionality or limited security features.

The vulnerabilities highlighted in the business model and incentives for organisations in the IoT market have thus shown the need for producers to implement a comprehensive system of checks on the design features of the IoT devices, both in their inputs such as the different device component integrated from external suppliers, as well as their output in the form of data collected from the device which can be sold to third parties as surplus data.

3.3.3 Vulnerabilities arising from human behaviours and behavioural data

While technical problems can usually be fixed, the literature reviewed for this study also emphasises vulnerabilities that are due to consumer attitudes and behaviours. A user of consumer IoT devices is likely to dedicate limited attention and have little capacity to identify vulnerabilities or threats against their devices.

[129] Royal Academy of Engineering. (2018). Cyber Safety and Resilience: Strengthening the Digital Systems that Support the Modern Economy.
[130] Farooq, J., et al. (2019). IoT Supply Chain Security: Overview, Challenges, and the Road Ahead.
[131] Steenmans, I. & Bras, I. (2018). Networked world: Risks and opportunities in the Internet of Things.
[132] National Cyber Security Centre (NCSC). (2018). The Principles of Supply Chain Security.
[133] Symantec. (2018). Internet Security Threat Report (ISTR).
[134] Yates, M. (2019). "Behavioral Surplus" Is Not Evil – It's Essential to Customer Experience. International Data Corporation (IDC).
[135] Carrigan, M. (2019). The institutionalisation of behavioral surplus: a quick recap on the Age of Surveillance Capitalism.
[136] Varian, H. R. (2014). Big data: New tricks for econometrics. Journal of Economic Perspectives, 28(2), 3-28.
[137] Wolfe, J. (2017). Roomba vacuum maker iRobot betting big on the 'smart' home. Reuters.

Several studies have exposed the vulnerability of using default passwords.[138,139] A study by F-Secure in 2018 revealed that threats targeting weak default credentials, unpatched credentials, or both, made up 87% of observed threats to IoT devices.[140] A considerable number of consumer IoT devices are shipped with default passwords, which are often easily guessable and are seldom changed by the user of the device (see Case Study box, below).[141] Users often do not know that devices have a default password, so might be unaware of the need to change it. If the process of changing the password is unclear, not possible or not obvious, then the credentials tend to remain in their default settings, exposing the device to unauthorised access once connected to the Internet.

Box 3.5: Case study – Connected security cameras and digital video recorders (DVRs)[142,143]

In 2017, a scanning attack used a type of malware (written to specifically target IoT devices) to crack the default passwords on a multitude of security cameras and DVRs that were connected to public Wi-Fi networks. This was accomplished by exploiting an open telnet server with a very simple default root password – '12345'. Once the attackers gained access to a device, it could be used for multiple purposes:

- Each infected device would act as a base for the further spread of the malicious code via the worm virus Linux Darlloz;
- Each infected device could be used to mine bitcoin, via a bitcoin miner installed on the device by the malware;
- All infected devices, in combination, could be used to form a botnet to launch a DDoS attack on any number of online targets;
- Unauthorised access / deletion / amendment of video, audio and other personal data collected by a connected security camera and DVR.

For many users, security models and the activity of their smart devices is opaque.[144] This is mainly because it is hard for users to determine if their devices are performing incorrectly or if their device has been compromised. As discussed in Section 3.2.1, responsibility for the security of a consumer IoT device is not always clear.

Consumer IoT devices often lack a full screen or keyboard interface that allows consumers to easily interact with the device. Increasing the usability of home IoT devices may require a more intuitive use of minimal buttons or actions and therefore embedding security into such restricted interfaces can be difficult.[145] The challenge therefore is to develop easy-to-use IoT interfaces that in turn can help users manage their security credentials more effectively but also keep software updated. This would help protect the wider network of home devices that are connected, reducing the number of devices that can be compromised. This is even more relevant when considering that a single consumer IoT device can compromise other devices, given that a "smart home is as vulnerable as its most vulnerable component".[146] Research is currently focusing on bridging the gap between security and usability in

[138] Heartfield et al. (2018). A Taxonomy of Cyber-Physical Threats and Impact in the Smart Home. Computers & Security, Vol 78, pgs 398–428.
[139] PenTestPartners. (2018). The most common IoT device security failings of 2017.
[140] F-Secure. (2019). IoT threat landscape: old hacks, new devices.
[141] NCC Group. (2017). Security of the IoT in the home.
[142] Ullrich, J. B. (2014). More Device Malware: This is why your DVR attacked my Synology Disk Station (and now with Bitcoin Miner!). SANS ISC InfoSec Forums.
[143] Ullrich, J. B. (2016). The Short Life of a Vulnerable DVR Connected to the Internet. SANS ISC InfoSec Forums.
[144] O'Hara. (2014). Privacy and the Internet of Things.
[145] NCC Group. (2017). Security of the IoT in the home.
[146] ENISA. (2014). Threat Landscape and Good Practice Guide for Smart Home and Converged Media; and IoT.

developing secure smart homes, where regular users can ensure the continued resilience of their IoT devices.[147]

The importance of human behaviour and the need for technology to be adaptive to this behaviour, and not vice versa, has been only recently recognised by industry and academia. Research examined for this study reveals the significant effects of hacking on trust and privacy considerations.[148] However, the traditional view in information security has been that users are the weakest link, providing a naïve explanation for user non-compliance with security policies or for the conscious and active bypassing of security controls. It is shown today that humans are 'boundedly rational' and have cognitive limitations, for example limited capacity, lack of information or time for optimising decisions.[149]

Thus, even if all vulnerabilities were to be eliminated, a reasonable level of 'everyday security' might still not be achievable due to the possibilities of human error. In order to optimise security, it is therefore crucial to limit the opportunities for human error, which are estimated to be responsible for 95% of security breaches.[150] Therefore, the security design of IoT devices needs to abandon the presupposition of 'fully-rational' consumers with adequate resources (time, attention, knowledge) to deal with security and instead recognise human decision-making characteristics in the design process.[151]

The collection of meta-data from a number of connected IoT devices can be aggregated and further used for building behavioural user profiles. The initial purpose of such collection is personalised, targeted advertisements; however, the risk escalates in an economy of scale where a plethora of sectors have interest in this behavioural data. Namely retailers, insurance companies, pharmaceutical companies, entertainment providers, education providers, transportation, energy, finance and other sectors, all have services and products which would benefit from a deeper understanding – or prediction – of user needs and behaviours. Associated risks originate from online behaviour and click trails, but with the proliferation of IoT devices it expands to environmental, physiological and biometric data. As an example, smart beds provide sleep tracking in order to enhance the quality of sleep, measuring amongst other things, respiration, posture and duration of sleep.[152]

IoT devices are able to collect significant amounts of personal data from users, which poses a risk should the device be compromised. Moreover, users often are not aware the extent to which their data might be collected by IoT devices.[153] Even at a meta-data level, if data is aggregated, a consumer's 'footprint' can be unique. For example, serious privacy concerns arise in the scenario where consumers connect their fitness tracker, diet app and smart thermostat with their smart bed, so that their daily physical activity, eating habits and house temperature are correlated with the quality of their sleeping patterns.

Other, more direct, privacy concerns are raised by visual data analytics. There are companies which specialise in 'emotion recognition technology' via video, for example through the cameras of smartphones or cars, which can recognise individuals' moods based on facial expressions.[154] The underlying AI algorithms are claimed to recognise 64 trillion possible emotional states within every

[147] Collen, A., Nijdam, N. A., Augusto-Gonzalez, J., Katsikas, S. K., et al. (2018). Ghost-safe-guarding home IoT environments with personalised real-time risk control. In International ISCIS Security Workshop (pp. 68-78). Springer, Cham.
[148] Bansal, G., & Zahedi, F. M. (2015). Trust violation and repair: The information privacy perspective. Decision Support Systems, 71, 62-77.
[149] Gigerenzer, G. & Selten, R. (Eds.) (2002). Bounded rationality: The adaptive toolbox. MIT press.
[150] Ahola, M. (2019). The Role of Human Error in Successful Cyber Security Breaches.
[151] Mersinas, K., Sobb, T., Sample, C., Bakdash, J. Z., & Ormrod, D. (2019). Training Data and Rationality. In ECIAIR 2019 European Conference on the Impact of Artificial Intelligence and Robotics (p. 225). Academic Conferences and publishing ltd.
[152] SleepNumber. (n.d). How it Works.
[153] Bannan, C. (2016). The IoT threat to privacy. Techcrunch.
[154] Koldony, L. (2016). Affectiva raises $14 million to bring apps, robots emotional intelligence. TechCrunch.

tenth of a second.[155] This data can be commodified for a variety of sectors like entertainment and gaming, capturing real-time reactions of individuals to inform and shape the company messages, products or advertisements accordingly.

Given the risk of human error, as noted in the workshop conducted in the context of this assignment, reducing the window of opportunity for human error should be a key objective of the measures aimed at tackling IoT cyber security vulnerabilities.

3.4 Likelihood of vulnerability exploitation and potential impacts

3.4.1 Potential impacts

Cyber attacks on consumer IoT devices can cause harm to individuals and undermine their security, safety and privacy. The research reviewed for this study indicates that the potential impact of consumer IoT vulnerabilities can range from a minor inconvenience, to serious financial loss or data breach, which can negatively affect consumers' health and safety, or compromise national security.

Interviews with tech and cyber security industry representatives highlighted that the cyber risks related to consumer IoT devices can be classified at the following levels: risks to individuals, risks to businesses and risks at a national or global level. Examples of each are provided here:

- **Personal level**: for example, privacy risks, financial loss, personal data being leaked, being locked out of their house, damage to property, consumer IoT-facilitated abuse, stalking or harassment.
- **Business level**: for example, loss of profits; risk of breaches of customer or other data; corporate espionage, such as theft of intellectual property; businesses taken offline, through a DDoS attack.
- **National / Global risks:** for example, network outages, disruption to essential services.

The interviewees for this study also highlighted the risk of failing to spend enough time thinking about the consequences of smart cities for the environment in which we live. For example, water treatment plants could be run by IoT but a malfunction could pollute the water, or streetlights could be attacked causing car accidents. Bringing such a connected system to a halt could have significant implications.

Box 3.6: Case studies: Risks associated with consumer IoT vulnerabilities

Personal risks: In 2013, the Polish Computer Emergency Response Team reported that attackers exploited a vulnerability in router firmware reportedly used in a number of commonly used router products.[156,157] The vulnerability, known as ZyNOS, was used to conduct a range of attacks, including a man-in-the-middle attack to steal bank credentials from users of the routers. The ZyNOS vulnerability allowed the attackers to download a file containing the router's configuration without authentication. Once access is gained, the attackers used a technique called DNS hijacking to take control of DNS servers, allowing them to redirect traffic to servers under their control. In this instance, the attackers rerouted traffic to banking websites and tricked users into providing usernames, passwords and even Transaction Authentication Numbers (TANs), allowing the theft of money from users' accounts. There is no indication of the extent of the financial theft via this attack.

Business risks: Designers at an architectural firm in Italy used smart drawing pads to send drawings and schematics within the office and to clients. These smart devices were connected to the office Wi-Fi and were still using the default login credentials that came with the pad's software.[158] As such,

[155] Levy-Rosenthal, P. (2019). New Patent Recognizes Emoshape Founder Patrick Levy-Rosenthal as the Inventor of the First Emotion Chip.
[156] CERT.Pl. (2014). Large-scale DNS redirection on home routers for financial theft.
[157] Constantin, L. (2014). Cybercriminals compromise home routers to attack online banking users. PCWorld News.
[158] DarkTrace. (2018). Global Threat Report 2017.

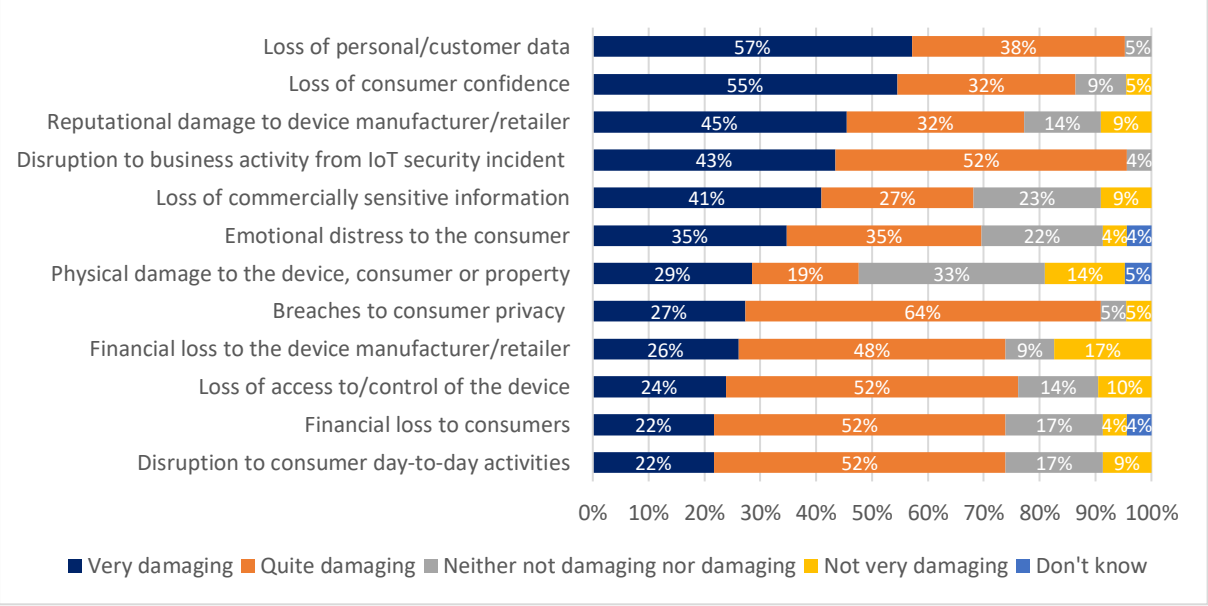
an attacker scanning the Internet for vulnerable devices identified the smart drawing pads and, using the default login credentials, gained access to those devices. Subsequently, the attacker utilised the smart drawing pads to send significant volumes of data to entertainment, government and design websites as part of a Denial of Service (DoS) attack on those websites.

Through this access, the attacker could potentially have gained unauthorised access to the company's confidential intellectual property, such as schematics. Furthermore, the company was inundated with superfluous requests for information, which impacted its own ability to operate, and could have been subject to legal implications had their infrastructure been responsible for damaging another network. Beyond the obvious vulnerability, this case also illustrates the challenges many businesses face with the established practice of Bring Your Own Device (BYOD) to work.

National Risks: The exploitation of IoT vulnerabilities, may have impacts at national or global levels. According to research, one of the main threats could theoretically lie within the use of high wattage domestic appliances such as air conditioners, to launch attacks on the power grids of countries, potentially shutting down their energy supply. Possible media through which the attack could be conducted might include botnets or manipulation of demand via IoT (MadIoT) to cause large-scale blackouts, by turning on or off all devices in a botnet and thus disrupting the demand for energy supply.[159]

A Gartner 2016 IoT Backbone Survey showed that 32% of IT leaders see security as a top challenge to the development of the IoT.[160] Furthermore, the business survey for this study reported that respondents were more likely to perceive loss of personal/consumer data (57%, N=21), loss of consumer confidence (55%, N=22) and reputational damage to the device manufacturer/ retailer (45%, N=22) as very damaging impacts from an IoT attack to their businesses. Figure 3.2 shows how respondents assessed the different impacts from IoT attacks, ranking them from the most to least damaging.

Figure 3.2: Perceived damage of different impacts of an IoT attack



Source: CSES Survey findings (businesses and other organisations), Q10, N=23

[159] Soltan, S., Mittal, P. & Poor, H.V. (2018). BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid, Princeton University, Paper for the 27th USENIX Security Symposium.
[160] Gartner. (2017). Leading the IoT.

In the business interviews for this study, commonly cited impacts on consumers included loss of service. The interviewees further highlighted how IoT device vulnerabilities could facilitate burglaries or residents being locked out of their homes. Other dimensions of impacts include the physical health impacts that could be brought by compromised IoT devices. In this study's consumer survey, it was reported that 17% of respondents who had experienced a cyber security issue with their devices experienced emotional distress. Interviewees also raised issues relating to the blurring line between wellbeing and medical devices, with the latter requiring checks from healthcare professionals, which might not occur if the device is being a treated as a lifestyle application. Environmental hazards would also be possible should devices designed for the upkeep of smart cities be attacked. An interviewee added that connected IoT devices could bring additional risks to vulnerable groups such as children.

Even though there have been many "real-world" cases exposing the cyber security of consumer IoT devices, the impact of vulnerabilities has mainly been demonstrated by security researchers in lab-based contexts, which means that the "real-world" impact of exploiting consumer IoT devices is difficult to estimate. Security companies track vulnerabilities and their potential impact through "honeypots" – decoy devices used to attract the attention of cybercriminals and analyse their activity. However, some of the concerns raised by participants in our survey have been manifested in the real world, as unauthorised surveillance, and uncontrolled generation and usage of data have been reported. For example, a family was "subjected to arbitrary interference with their privacy, family and home" when someone hacked into their baby-monitoring camera and threatened to kidnap their child.[161,162,163] And in 2016, residents in Finland were left in the cold after their homes heating systems suffered a DDoS attack.[164]

There is some evidence on the consequences – both monetary and other costs – for consumers due to IoT security breaches. Thus, the Mirai botnet mentioned previously is used for DDoS attacks, targeting the availability of public services and major Internet platforms such as Spotify and Twitter, which were temporarily unavailable to many users.[165] In 2019, Wikipedia suffered an IoT-based DDoS attack which was characterised as 'massive and very broad'.[166] Over 20 billion connected 'things' are expected to be in use by 2020; thus, attacks similar to the DDoS attacks of 2016 which affected many companies like Amazon, Paypal, Twitter, Spotify and Netflix are more likely to happen.[167] A Berkeley study which specifically examined compromised IoT devices under the Mirai botnet revealed small increases in electricity consumption, but significant increases in Internet bandwidth usage of infected devices and a consequent degrading of user experience as a result.[168] The 'plain' version of these botnets is not very effective nowadays, but hackers have been developing and modifying new versions of the tool. There is a good understanding of the potential propagation of such botnet attacks (the original creator of Mirai made the source code available).

In the case of Mirai, once a device is compromised, it does not stay idle, but continues to scan for new vulnerable devices to attack which – if compromised – join the hunt for more vulnerable devices. Thus, a single compromised device in a 'smart environment' can lead to a number of interconnected devices being infected very quickly. The Berkeley findings also suggest that compromised devices might come under 'command and control' hosts which allows the owner of a botnet to order infected IoT devices to launch an attack against a target, and can start flooding the victim with traffic. These attacks also have an economic impact on consumers: for almost 100,000 devices involved in the Mirai Dyn attack,

[161] ENISA. (2014). Threat Landscape and Good Practice Guide for Smart Home and Converged Media; and IoT.
[162] United Nations General Assembly. (1948). Universal declaration of human rights. UN General Assembly.
[163] Fieldstadt, E. (2018). Nest camera hacker threatens to kidnap baby, spooks parents. NBC News.
[164] Ashok, I. (2016). Hackers leave Finnish residents cold after DDoS attack knocks out heating systems. International Business Times.
[165] Conger, K. (2016). The Mirai botnet's Internet takedown opens up a new market for attackers and defenders. TechCrunch.
[166] Venkat. A. (2019). Wikipedia Investigates DDoS Attack. Bankinfosecurity.
[167] Gartner. (2017). Leading the IoT.
[168] Fong, K., Hepler, K., Raghavan, R., & Rowland, P. (2018). rIoT: quantifying consumer costs of insecure Internet of Things devices. University of California Berkeley, School of Information Report.

the Berkeley study estimates that the average costs were USD 1.08 per device, with a total cost borne by consumers of USD 115,307.91.[169]

3.4.2 Likelihood of vulnerability exploitation

In 2014 there was limited information on the likelihood of attacks on IoT devices as experts interviewed for ENISA's research at the time explained that the risk of criminal activity targeting smart home devices is relatively low given the relatively small number of smart homes. However, forecasts predicted that more consumer IoT devices will connect the home in the next 5-10 years, therefore increasing the likelihood of cyber attacks. This seems to have been proved true in recent years: as the number of IoT devices increased from 3.8 billion to 7 billion between 2015 and 2018, the number of new IoT-malware grew tenfold between 2016 and 2017 and then three-fold between 2017 and 2018.[170,171] Since the value of personal data, financial tokens and credentials stored in smart home devices will increase, so too will the financial motivation for crime.[172]

Indeed, more recent research by security companies widely agrees that cyber attacks on IoT devices have grown at an unprecedented rate. A number of studies by security companies, such as Symantec, Kaspersky and F-Secure, have analysed consumer IoT devices through honeypots to assess cyber security risks and threats.[173,174,175] The cyber attacks identified differ from one study to the other. Kaspersky honeypots detected more than 100m attacks on IoT devices in the first six months of 2019.[176] This figure was seven times higher than the first six months in 2018. The increase in the number of attacks between 2018 and 2019 was also reflected in the other studies by Symantec and F-Secure. Based on their analysis, Kaspersky noted that attacks on IoT devices are usually not sophisticated but stealth-like, as users might not notice their device being exploited. Highlighting the likelihood of vulnerabilities being exploited in consumer IoT devices, this study's consumer survey also revealed that 23% of respondents (N=35) had received a security warning notification from their IoT device and 11% reported their device having been infected by a virus, malware or ransomware.

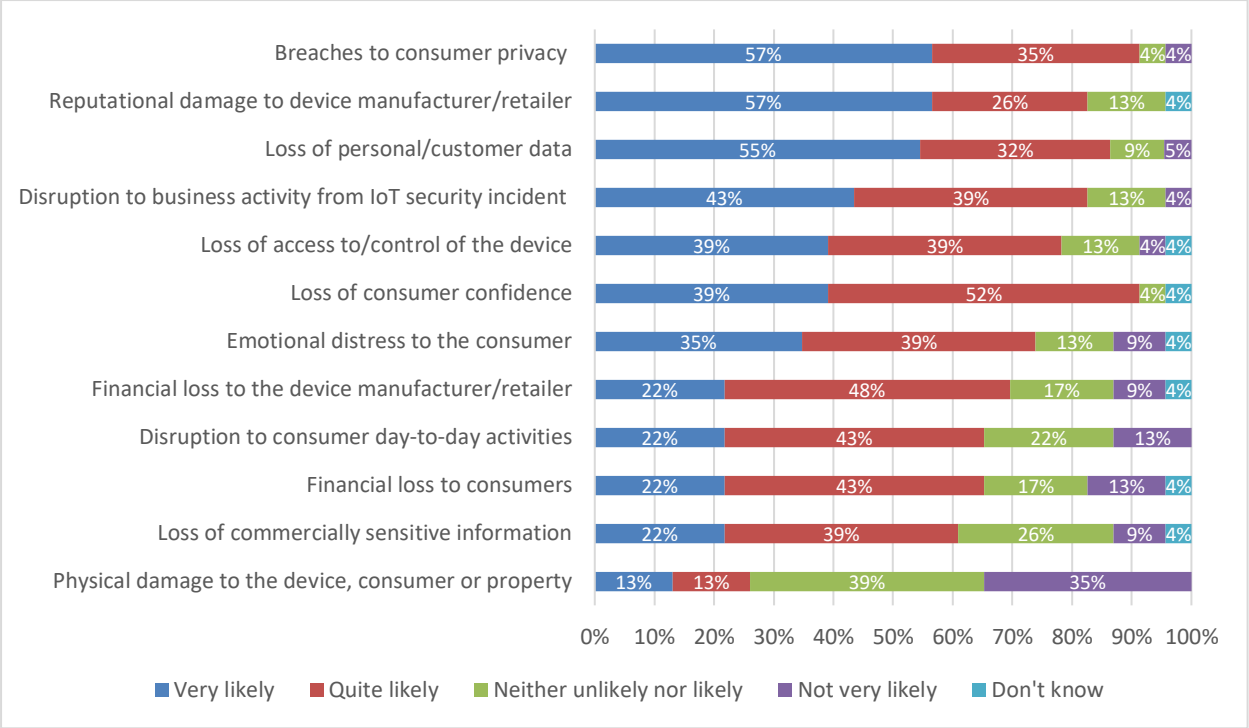
As for businesses, in terms of the likelihood of their IoT devices being hacked, a study amongst 400 US-based companies revealed that almost half of them (48%) reported suffering at least one IoT security breach. The monetary impact was estimated to be up to 13% of annual revenues for small companies and run into the tens of millions for larger companies.[177] In the UK, 46% of businesses report have experienced a cyber security breach in the last 12 months, affecting in particular 68% of small and medium-sized businesses and 75% of large businesses, although this was not only IoT-related attacks.[178]

According to research by Irdeto, eight out of every ten organisations experienced a cyber attack on their IoT devices in 2019.[179] Of those organisations, 90% experienced a negative impact as a result of this, including operational downtime, compromised customer data or end-user safety. This study's business survey revealed that respondents believe that breaches to consumer privacy, loss of personal data and reputational damage are very likely to be incurred following an IoT attack. Figure 3.3 shows

[169] Fong, K., Hepler, K., Raghavan, R., & Rowland, P. (2018). rIoT: quantifying consumer costs of insecure Internet of Things devices. University of California Berkeley, School of Information Report.
[170] Lueth, K. L. (2018). State of the IoT 2018: Number of IoT devices now at 7B — Market accelerating.
[171] Kaspersky. (2018). New IoT-malware grew three-fold in H1 2018. Kaspersky.
[172] ENISA. (2014). Threat Landscape and Good Practice Guide for Smart Home and Converged Media; and IoT.
[173] F-Secure. (2019). Attack Landscape H1 2019: IoT, SMB traffic abound.
[174] Kaspersky. (2019). IoT under fire: Kaspersky detects more than 100 million attacks on smart devices in H1 2019.
[175] Symantec Research Labs. (n.d.) Before Toasters Rise Up: A View Into the Emerging IoT Threat Landscape.
[176] Kaspersky. (2019). IoT under fire: Kaspersky detects more than 100 million attacks on smart devices in H1 2019.
[177] Businesswire. (2017). Survey: Nearly Half of U.S. Firms Using Internet of Things Hit by Security Breaches. Businesswire.
[178] Ipsos MORI. (2020). Cyber Security Breaches Survey 2020.
[179] Irdeto. (2019). New 2019 Global Survey: IoT-Focused Cyberattacks are the New Normal.

how business respondents assessed the likelihood of different impacts resulting from an attack, in particular highlighting which impacts from an IoT attack they perceived as 'very likely'.

Figure 3.3: Perceived likelihood of impacts of an IoT attack



Source: CSES Survey findings (businesses and other organisations), Q9, N=23

By comparing Figures 3.2 and 3.3, it is possible to identify a correlation between business' perception of damage for the different potential impact and their perceived likelihood. For example:

- 57% of respondents noted that loss of personal data would be very damaging and 55% believed it to be very likely.
- Similarly, 45% of respondent found the reputational damage brought by an IoT attack to be very damaging, with 57% qualifying it as very likely.
- The disruption of business activity as a result of an IoT attack was ranked fourth by respondents in both terms of potential damage and likelihood.
- This correlation between potentially 'very damaging' and 'very likely' attributes could contribute to developing a measure to calculate a hierarchy of the potential risk of each of the impacts, taking into account both their likelihood and potential damage. Such a cross-comparison would make it possible to better evaluate the potential risk of some impacts such as 'physical damage to the device, consumer or other property', which although reported frequently as very damaging (29%) was only reported as being very likely by 13% of respondents. Based on this approach and Tables 3.2 and 3.3, the most significant risk reported was loss of personal/customer data (57% rating as very damaging and 55% very likely, 38% quite damaging and 32% quite likely). The least risky impact would be 'physical damage to the device, consumer or other property' (the highest proportion of respondents finding it 'neither unlikely or likely' and 'not very likely', 39% and 35% respectively, and neither 'not damaging or damaging' or 'not very damaging', 33% and 14% respectively).
- As discussed in this report, the different impacts resulting from the exploitation of vulnerabilities in IoT devices vary in terms of their likelihood and potential damage they can incur on businesses. As these impacts can affect the personal data of consumers and subsequently damage consumers'

confidence and a producer's reputation, they also have the potential to affect business revenues. The risk of this can be explored by looking at the relationship between likelihood of an impact occurring and its potential impact.

4. Potential Impact of Government Regulation

Box 4.1: Key Findings: Potential Impact of Government Regulation

- As a result of potential regulation, manufacturers and other economic operators in the consumer IoT market will incur a range of administrative and substantive compliance costs. The extent of these costs depends on whether product labelling is mandated and whether product redesign costs are required. However, it is likely that compliance costs will not need to be passed on to consumers.
- Additional complexities have been identified, in particular related to the implementation of aspects of the second and third CoP guidelines (those related to vulnerability disclosure and software updates), and the practicalities of regulation.
- The primary benefit to the IoT market is likely to come in the form of positive economic effects, such as increasing sales volume as a result of increasing confidence in the security of consumer IoT devices. In addition, increased device security will help to mitigate the risks to manufacturers of cyber attacks against their products and the related negative impacts.
- Considering the impact of proposed regulation on the consumer, the main benefits will include: a reduction in the number of insecure consumer IoT devices; increased confidence and trust in the market leading to greater ownership and realisation of the benefits associated with the IoT. A key challenge is to ensure the burden for being informed about cyber security does not lie just with the consumer.
- Potential negative impacts on consumer access are possible, as a result of a possible increase in device prices and the potential for non-UK providers to exit the UK market. However, these are considered unlikely.
- No demographic group of consumers will experience specific negative impacts. However, certain consumer groups will realise greater positive impacts as a result of the implementation of the minimum security requirements.

This section examines the potential impact of the introduction of the minimum security baseline requirements for consumer IoT products proposed by the Government. More specifically, this section details the findings from the research on the possible impacts of the regulatory proposals on the consumer IoT market, before highlighting the potential direct and downstream impacts on consumers. The following box provides an overview of regulatory options proposed by DCMS in the 2019 public consultation.

Box 4.2: Regulatory Developments in the UK: Consumer IoT Security

Through 2018, DCMS engaged extensively with the topic of consumer IoT security, publishing the March 2018 Secure by Design report,[180] the October 2018 Code of Practice for Consumer IoT Security and response to the informal consultation.[181] Following this, DCMS launched a public consultation on regulatory proposals for consumer IoT security in May 2019 alongside a Consultation Stage Impact Assessment.[182] In particular, the Consultation Stage Impact Assessment detailed the nature of the security challenge posed by consumer IoT, the rationale for government intervention, the policy options under consideration and the anticipated impacts of those policy options. The policy options from the consultation are as follows:

- **Option A:** Mandate retailers to only sell consumer IoT products that have the IoT security label, with manufacturers to self-assess and implement the security label on their consumer IoT products.
- **Option B:** Mandate retailers to only sell consumer IoT products that adhere to the top three guidelines of the Code of Practice, with manufacturers to self-assess that their consumer IoT products adhere to the top three guidelines of the Code of Practice for Consumer IoT Security and the ETSI TS 103 645.
- **Option C:** Mandate retailers to only sell consumer IoT products that have the IoT security label that evidences compliance with all thirteen guidelines of the Code of Practice for Consumer IoT Security and ETSI TS 103 645, with manufacturers expected to self-assess and implement the security label on their consumer IoT products.

The top three guidelines stipulated in the Code of Practice for Consumer IoT Security are:

- **Guideline 1:** IoT device passwords must be unique and not resettable to any universal factory setting.
- **Guideline 2:** Manufacturers of IoT devices need to provide a public point of contact as part of a vulnerability disclosure policy.
- **Guideline 3:** Manufacturers of IoT devices need to explicitly state the minimum length of time for which the product will receive security updates.

The consultation on the above policy options, which concluded on 5 June 2019, aimed to collect the views of interested stakeholders on the issues detailed in the impact assessment through open-ended questions. In total, the consultation received responses from 60 stakeholders. On 3 February 2020, DCMS published its analysis of the responses to the consultation and provided formal responses in relation to each consultation question.[183]

[180] Department for Digital, Culture, Media & Sport (DCMS). (2018). Secure by Design: Improving the cyber security of consumer Internet of Things Report.
[181] Department for Digital, Culture, Media & Sport (DCMS). (2018). Code of Practice for consumer IoT security.
[182] Department for Digital, Culture, Media & Sport (DCMS). (2019). Mandating Security Requirements for Consumer 'IoT' Products, Consultation Stage Impact Assessment.
[183] Department for Digital, Culture, Media & Sport (DCMS). (2020). Consultation Outcome: Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation.

Through the Consultation Stage Impact Assessment, the Government noted that basic cyber security provisions are lacking from many consumer IoT devices and that manufacturers often implement security as an afterthought.[184] For instance, the ease with which the Mirai botnet infected a significant number of consumer IoT devices has been well documented, as has the fact that although many techniques exist for identifying IoT security weaknesses and protecting devices, the practical implementation of these security techniques in IoT contexts 'remains somehow ambiguous'.[185]

Moreover, significant information asymmetries exist that place the consumer at a disadvantage with regard to understanding the cyber security protection embedded in a particular consumer IoT device.[186] As argued in American economist George Akerlof's seminal paper, such information asymmetries can have drastic effects on the market.[187] In the consumer IoT market, this is becoming evident as manufacturers, developers, retailers and other economic operators not have an incentive to increase the security of their products on the market, which means other economic factors (e.g. quicker time to market, lower costs, larger profit margins etc.) are more prominent drivers of product development than security. As Akerlof posits, repetition and reinforcement of such behaviour could then result in adverse selection where consumers lose trust in consumer IoT devices and the willingness to buy the device diminishes.

This pattern has been observed in the information security market more generally[188,189] and is a viewpoint supported by the majority of stakeholders, including industry and academic stakeholders interviewed for this study. With the case for change established, the Consultation Stage Impact Assessment proposed options for regulation. However, the regulatory actions proposed could bring about a range of potential impacts, including costs and benefits for the consumer IoT market, but also for consumers. This section primarily considers the potential impact of introducing these aspects of the top three guidelines of the Code of Practice for IoT Security although insights related to Option A and the potential impact of labelling requirements are also discussed.

4.1 Potential Impact of Government Regulation on the Consumer IoT Market

This sub-section examines the potential impacts of the regulatory approach outlined above on the consumer IoT market. First, the anticipated costs for manufacturers, retailers and other economic operators involved in the consumer IoT market are presented, before the potential benefits to these stakeholders are discussed. Following this, additional impacts that could result from the regulatory approach are detailed.

4.1.1 Assessment of the costs of the proposed regulatory approach

In relation to these aspects of the top three guidelines set out in the Code of Practice for IoT Security, the key types of costs borne by all developers and manufacturers of consumer IoT products could include:

- Costs associated with familiarisation with the regulation;

[184] Blythe, J.M., Johnson, S.D., & Manning, M. (2020). What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices, Crime Sci (2020) 9:1.
[185] Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G. & Ghani, N. (2019). Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-scale IoT Exploitations, IEEE Communications Surveys & Tutorials, April 2019.
[186] Department for Digital, Culture, Media & Sport (DCMS). (2019). Mandating Security Requirements for Consumer 'IoT' Products, Consultation Stage Impact Assessment.
[187] Akerlof, G.A. (1978). The market for "lemons": Quality uncertainty and the market mechanism. In Uncertainty in economics (pp. 235-251). Academic Press.
[188] Anderson, R. (2001). 'Why information security is hard-an economic perspective.' In Computer security applications conference, 2001. Acsac. proceedings 17th annual, pp. 358_365. IEEE, 2001.
[189] ENISA. (2018). Economics of vulnerability disclosure.

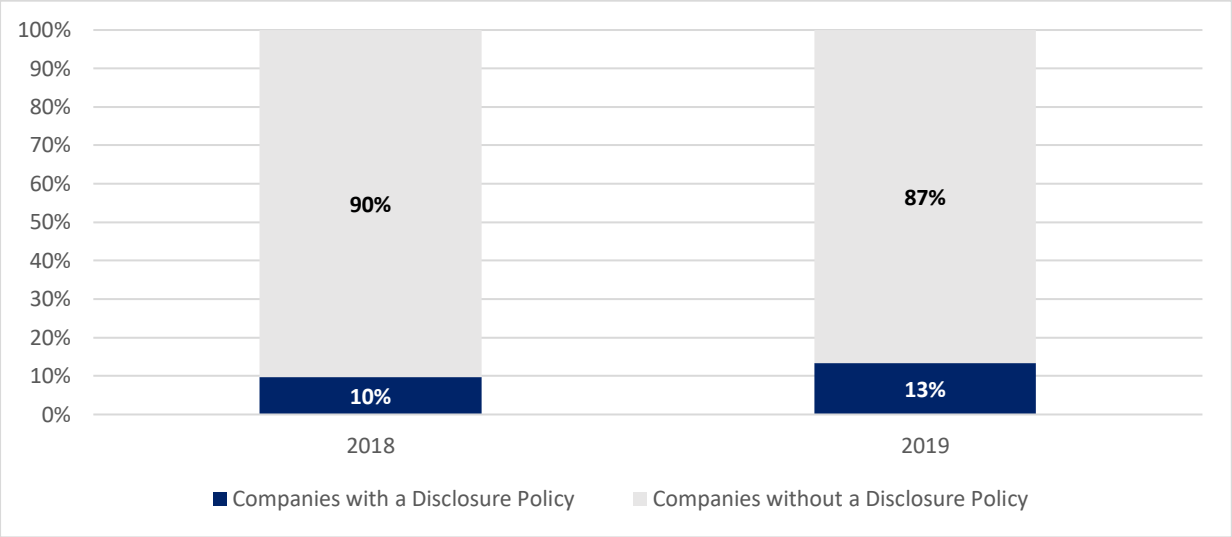
- Costs of compliance (e.g. developing a vulnerability disclosure policy etc.);
- Costs related to self-assessment of products against the requirements.

However, there are complexities that suggest additional costs will be incurred by all or some manufacturers, developers and other economic operators as a result of regulation. These complexities include the potentially variable impact of the regulatory approach on different product types and different market actors, the possible requirement for security labelling (as covered by Option A above) and the possible variables in the practical application of the regulation. Furthermore, business stakeholders interviewed for this study noted that, with these complexities in mind, reliable cost quantifications are difficult to provide.

With that said, there was a consensus amongst the interviewed stakeholders that implementing the first minimum baseline security requirement (concerning default passwords) would not bring significant difficulties or costs for the vast majority of businesses. These interviewees noted that some companies will be required to redesign products and processes and will incur additional costs as a result. For example, default passwords are commonly used to allow remote access and device management for customer support purposes. However, it was also argued that many developers and manufacturers already ensure products do not use default passwords and perceive this to be a basic requirement that should, in any case, be implemented as a market entry requirement.

Considering the second minimum baseline security requirement (concerning vulnerability disclosure policies), research from the IoT Security Foundation[190] indicates that in 2019, more than 85% of the consumer IoT companies surveyed globally would need to take action as they currently do not have vulnerability disclosure policies in place (see Figure 4.1).

Figure 4.1: Consumer IoT companies with vulnerability disclosure policies globally, 2018 and 2019



Source: IoT Security Foundation. (2020). Consumer IoT: Understanding the Contemporary Use of Vulnerability Disclosure – 2020 Progress Report

Regarding the reasons for this low adoption of vulnerability disclosure practices, the European Cybersecurity Agency (ENISA), in research on the economics of vulnerability disclosure, detailed key barriers to participating in or establishing vulnerability disclosure practices. Primarily, these barriers include: a lack of awareness or understanding; the costs of implementation and operation; a lack of

[190] IoT Security Foundation. (2020). Consumer IoT: Understanding the Contemporary Use of Vulnerability Disclosure – 2020 Progress Report.

management support; a lack of organisational or technical capacity; and legal barriers or uncertainty.[191]

To implement this requirement, companies would incur costs related to drafting a policy document, developing processes and procedures for vulnerability notification and management and ensuring a public point of contact is in place. Although complexities may exist with regard to vulnerability management in the supply chain (as discussed below), business interviewees agree that compliance with the second requirement would not be particularly burdensome. The same interviewees – including individual companies, industry associations, consumer associations and governmental stakeholders – recognised that the implementation of the third requirement (concerning software updates) would be more complex. This complexity is characterised by a key challenge related to supply chain management and a range of concerns related to the practicalities of implementation.

The complexity of supply chain management is reportedly an important issue for many manufacturers of consumer IoT devices. More specifically, the production of many consumer IoT devices involves a complex supply chain with software and hardware components often being developed in disparate jurisdictions by different organisations. As a result, businesses could incur costs related to supply chain management and, in particular, understanding and ensuring the regulatory compliance of such components. Interviewees for this study noted that this was particularly relevant in relation to the guidelines related to vulnerability disclosure and software updates.

Considering vulnerability disclosure, for example, it was noted by business stakeholders and others involved in standards development that this would represent a significant culture change for many consumer IoT manufacturers and their supply chains. This is due to the need to ensure there is a means to responsibly disclose vulnerabilities in all elements of a product and subsequently patch those vulnerabilities. With regard to software updates, companies could face issues in ensuring the regulatory compliance of components and other inputs supplied by third-party developers and manufacturers.[192,193] The concerns related to the practical implementation of the third requirement include:

- The required frequency and quality of software updates. On this specific point, business associations and companies interviewed for this study stated that manufacturers could potentially avoid the current software update requirements by providing limited, irregular or low-quality updates.
- Issues exist relating to situations where, for example, a company fails, leaving consumers without security updates. In such a situation, consumers are likely to assume that their device is still secure, but it is unclear what recourse they will have should any issues occur or whether the responsibility for ensuring the consumer IoT devices remain secure is reallocated.[194,195]

In addition to the above considerations, there are important horizontal impacts worth highlighting that could affect the costs borne by manufacturers and developers of consumer IoT products. First, industry stakeholders interviewed for this study noted that, considering the need for clarity on issues related to the practical implementation of the regulatory approach, legal certainty on compliance with the regulation may be a challenge. For example, legal certainty may be lacking in relation to the ability

[191] ENISA. (2018). Economics of vulnerability disclosure.
[192] techUK. (2019). Response to Department for Digital, Culture, Media & Sport Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security.
[193] UK Computing Research Committee (UKCRC). (2019). Response to DCMS, Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security.
[194] Open Rights Group. (2019). Response to the Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security.
[195] UK Computing Research Committee (UKCRC). (2019). Response to DCMS, Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security.

to confidently and sufficiently self-certify. As a result, businesses could be required to incur independent testing and certification costs.

Second, it has been noted that smaller businesses will face higher costs in relation to their revenues as a result of implementing the regulatory approach, as compared with larger businesses.[196] For example, industry stakeholders and cyber security experts interviewed for this study noted that start-ups and smaller companies may not have the capacity to implement a public contact point for vulnerability disclosure or have access to the technical expertise to sufficiently deal with identified vulnerabilities. Third, there are challenges related to how manufacturers tackle the issue of potentially different regulatory approaches across different jurisdictions.

Furthermore, tech industry stakeholders interviewed for the study noted that the costs and impacts of the proposed regulatory approach will probably not be uniform across different product types and categories, as they have different levels of cyber security maturity. Manufacturers stated that this is often driven by the inherently different nature of the cyber security risks facing each product type. For example, smartphones and connected toys pose a significant risk to privacy if successfully attacked, whereas smart white goods currently collect limited personal data. In place of privacy risks, it has been theorised but not practised, that smart white goods could be used to cause significant wider physical damage, such as shutting down power grids. Examples of the different potential impacts are provided in the below box.

Box 4.3: Case studies – Impacts of cyber attacks on consumer IoT devices

Local and national impacts: At the 2018 USENIX Security Symposium, researchers from Princeton presented a paper demonstrating that 'an Internet of Things (IoT) botnet of high wattage devices – such as air conditioners and heaters – gives a unique ability to adversaries to launch large-scale coordinated attacks on the power grid'[197]. More specifically, the researchers demonstrated that a new class of potential attacks called the Manipulation of demand via IoT (MadIoT) could be utilised to cause local power outages, large-scale blackouts and even manipulation of the operating cost of the power grid, potentially to the benefit of a few utilities. This could be done by increasing or reducing the demand for electricity by simultaneously turning on or off all devices in a botnet of compromised high-wattage devices.

Although illustrated in relation to the US power grid, cyber security industry interviewees with expertise in the smart utilities industry noted that similar attacks could be conducted in the UK.

Impacts on individuals / households: An example is the case of a hacked baby monitor.[198] In this case, an attacker took control of a monitor, which was placed in the child's bedroom and was linked to a receiver in the parent's room. The attacker used default factory passwords that had previously been leaked as a result of a data breach to gain control of the device. Once in control, the attacker used the voice functionality of the device to make the parents believe he was in their child's room and sent them threatening messages, while also having taken control of the camera function of the device to see what was happening inside of the house.

Beyond the costs related to the implementation of the three minimum baseline security requirements, business stakeholders also highlighted the costs and challenges related to the implementation of product labelling (i.e. Option A in the Consultation Stage Impact Assessment). In particular, industry associations and companies interviewed for this study highlighted significant costs related to

[196] Department for Digital, Culture, Media & Sport (DCMS). (2019). Mandating Security Requirements for Consumer 'IoT' Products, Consultation Stage Impact Assessment.
[197] Soltan, S., Mittal, P. & Poor, H.V. (2018). BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid, Princeton University, Paper for the 27th USENIX Security Symposium.
[198] Nord VPN. (2018). Hacker terrorizes family by hijacking baby monitor. (Article published December 2019).

amending labelling practices and processes, potentially across multiple products, and noted practical issues related to the placement of labels on smaller products.

In addition, these stakeholders highlighted the risk of wasted non-labelled stock, even if that stock is secured in line with the top three guidelines. However, it was noted by many stakeholders that both the risk of wasted non-labelled stock and the costs of product labelling could be mitigated by a well-designed implementation. In practice, this could be achieved through the implementation of a grace period where existing stock can be replaced by new stock that meets the requirements, including on labelling.

Furthermore, it is envisaged by representatives of the technology industry that 'static' labels could create issues: such static labels, as currently designed, convey no information on the potential risks attributable to a specific consumer IoT device. Moreover, static labels can cause difficulties should product changes be necessary and, thirdly, as the guidelines and industry practices will evolve over time, such static labels could be invalidated (for instance, many manufacturers and economic operators are moving away from passwords to other forms of authentication, such as biometrics or certificate-based authentication).[199]

4.1.2 Assessment of the benefits of the proposed regulatory approach

Beyond the costs associated with implementation, the primary benefit to the consumer IoT market could come in the form of positive economic effects. As a result of increased confidence and trust in the security of consumer IoT devices, manufacturers and developers could experience increases in revenue and profit due to increased consumer IoT products' sales volumes.

In a broader retail context, the importance of brand trust to consumer purchasing decisions is well established. For instance, PwC's 2018 Global Consumer Insights Survey[200] found that 35% of 22,000 respondents across 27 territories ranked 'trust in the brand' as among their top three reasons, besides price, for choosing a particular retailer.[201] In addition, the same survey found that, in an online retail scenario, the trust factor is prominent for consumers when trying to ensure security. For instance, the majority of respondents reported that they only use credible or legitimate websites (57%) and choose providers they trust to make payments (51%).[202] Although not specifically related to consumer IoT, parallels can be drawn with regard to the importance of consumer trust in purchasing decisions.

Many business representatives interviewed for this study also noted the importance of consumer trust. These stakeholders reported that this is a key driver of their investment in security, while also stating that investment in security drives gains in brand reputation, consumer trust and their value proposition. Moreover, these industry stakeholders stressed that they view security as a requirement for market entry. Although quantitative data on the relationship between product security and consumer trust and sales volume is limited, these findings suggest that improved security and improved consumer trust is likely to drive increased sales volumes for manufacturers and developers of consumer IoT devices. Furthermore, research on mobile shopping – that is, using smartphones to shop online – has found that risk and trust are strongly associated notions.[203] This research found that trust and perceived risk have an inverse relationship, meaning that increased overall trust reduces the level of consumer perceived risk. This is further supported by research on online purchasing

[199] techUK. (2019). Response to Department for Digital, Culture, Media & Sport Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security.
[200] PwC. (2018). Global Consumer Insights Survey 2018: Whom do consumers really trust?
[201] PwC. (2018). Global Consumer Insights Survey 2018: Whom do consumers really trust?
[202] PwC. (2018). Global Consumer Insights Survey 2018: Whom do consumers really trust?
[203] Marriott, H. R., & Williams, M. D. (2018). Exploring consumers perceived risk and trust for mobile shopping: A theoretical framework and empirical study. Journal of Retailing and Consumer Services, 42, 133-146.

behaviour, which concludes that both vendor and overall trust are significant predictors of behavioural intentions.[204,205]

This suggests that improving trust in consumer IoT manufacturers, by reducing vulnerabilities of devices, could have positive effects on consumer adoption and thus sales volume. In addition, data from the survey of consumers conducted for this study indicates that consumers currently have some reticence with regard to trusting their consumer IoT devices, suggesting the capacity for significant gains in the market. The majority of respondents (68%) stated that they trust the security of their consumer IoT device(s) to a small extent (31%) or to some extent (37%), with only 17% trusting their devices to a great extent.[206] In addition, positive impacts with regard to reducing vulnerabilities and thus increasing trust will continue long into the future as legacy equipment and infrastructure are steadily replaced with more secure products.

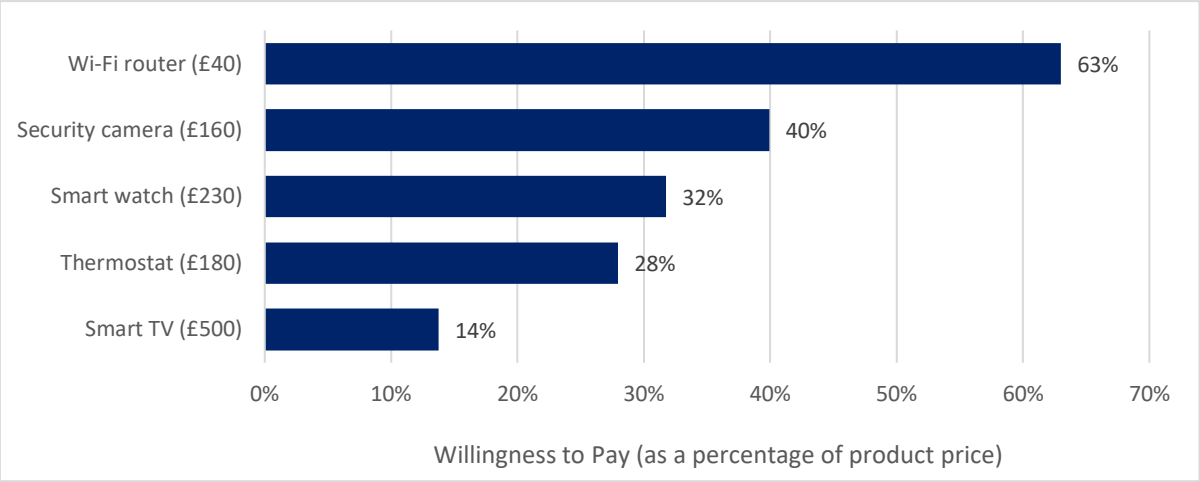
Furthermore, specifically with regard to vulnerability disclosure, ENISA has analysed the benefits of participating in vulnerability disclosure practices. ENISA found that organisations are driven to conduct vulnerability disclosure for one or more of the following reasons: for the security benefits; for the economic benefits; to raise awareness and engage with the community; to respond to customer demand; and/or for reasons of ethical and social responsibility.[207] Considering the economic benefits in particular, it is found that the implementation of vulnerability disclosure can reduce costs, such as development, marketing or security assurance costs,[208] as it allows organisations to benefit from the knowledge and effort of external security researchers at relatively low cost and effort.[209]

In addition to increasing sales volume, it is also worth considering recent research on the willingness to pay (WTP) which indicates that greater security positively affects consumers' WTP for IoT products. Although this may not necessarily drive increased profits for manufacturers and developers, for example because of the potential need to offset the costs of incorporating increased security or possible regulatory compliance costs, these findings illustrate the value of security to the consumer.

Increased confidence in the added value of security has the potential to incentivise improved security practices across the market. In 2020, researchers from University College London (UCL) published the results of an experiment to test WTP for security in relation to five types of consumer IoT devices (smart TVs, smart watches, Wi-Fi routers, security cameras and thermostats).[210] The researchers found that participants were willing to pay between 14% and 63% more on average for greater security (see below figure).

[204] Pappas, N. (2016). Marketing strategies, perceived risks, and consumer trust in online buying behaviour. Journal of Retailing and Consumer Services, 29, 92-103.
[205] Suki, N. M., & Suki, N. M. (2017). Modeling the determinants of consumers' attitudes toward online group buying: Do risks and trusts matters? Journal of Retailing and Consumer Services, 36, 180-188.
[206] Survey of consumers conducted for this study, Q19: To what extent do you trust the security of your consumer IoT device(s)? N=35.
[207] ENISA. (2018). Economics of vulnerability disclosure.
[208] Zhao, M., Laszka, A., & Grossklags, J. (2017). 'Devising effective policies for bug-bounty platforms and security vulnerability discovery.' Journal of Information Policy 7: 372 –418.
[209] National Telecommunications and Information Administration (NTIA). (2016). 'Vulnerability Disclosure Attitudes and Actions: A Research Report from the NTIA Awareness and Adoption Group.'
[210] Blythe, J.M., Johnson, S.D., & Manning, M. (2020). What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices, Crime Sci (2020) 9:1.

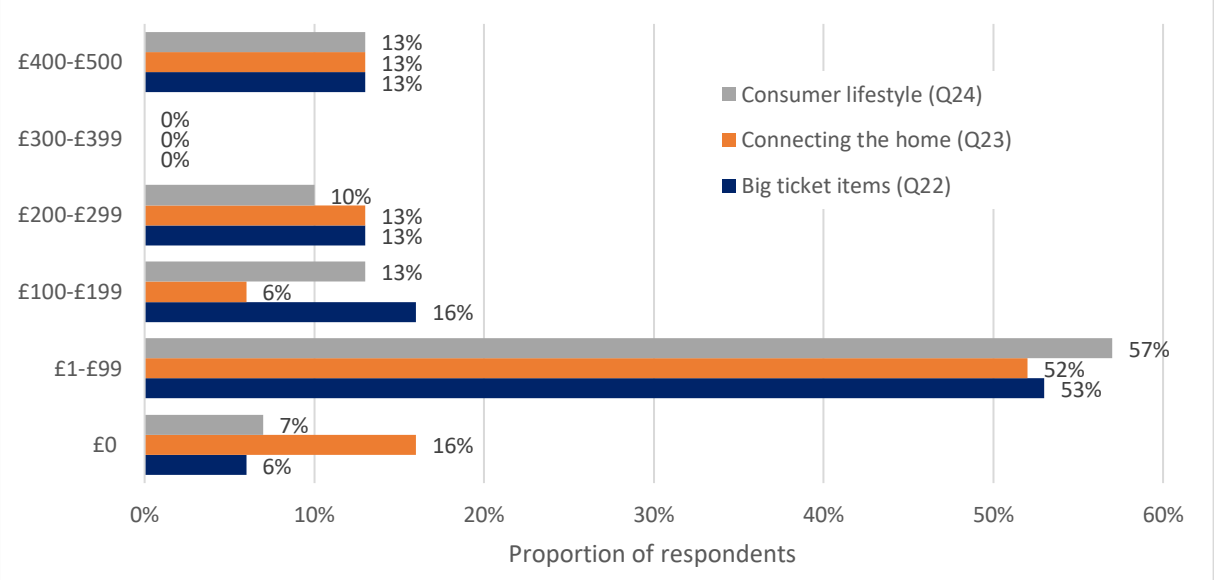
Figure 4.2: Mean amount participants reported that they were willing to pay for greater security for different types of IoT products, as a percentage of product price (cost of device shown in parentheses)



Source: Blythe, J.M., Johnson, S.D., & Manning, M. (2020). What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices

In addition, the survey of consumers conducted for this study examined WTP with regard to the three categories of consumer IoT items (i.e. "Big Ticket" items; "Connecting the Home" items; and "Consumer Lifestyle" items. See Section 2 for definitions). For all three categories, respondents noted a willingness to pay more for greater security features. On average, respondents were willing to pay £133.38 more for "Big Ticket" items (N=32); £118.81 for "Connecting the Home" items (N=31); and £123.43 for "Consumer Lifestyle" items (N=30). However, as illustrated in the chart below, the majority of respondents indicated figures in the £1-£99 bracket, suggesting that the average values are inflated by a small number of respondents that selected the maximum or near the maximum (i.e. £500) for all three questions. As such, it is more helpful to present the median values for each category: in this respect, respondents were willing to pay £65 more for big ticket items; £33 more for connecting the home items; and £45 more for consumer lifestyle items.

Figure 4.3: Additional amount consumers are willing to pay for greater security features in consumer IoT devices, by product category

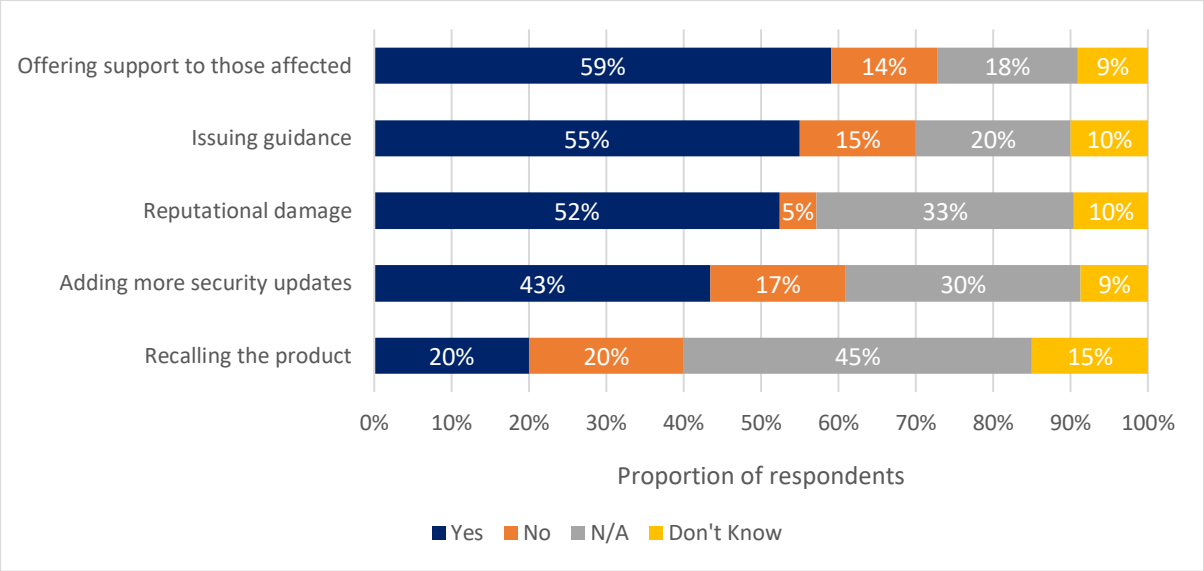


Source: CSES Survey findings (consumers), Q22 (N=32), Q23 (N=31), Q24 (N=30)

Research has also been conducted on the effect of security labels on WTP. One study conducted by UCL and the Australian National University tested the impact of five different security labels on WTP, as compared with no security labels, for four types of consumer IoT devices (security cameras, smart TVs, wearables and thermostats).[211] It was found that for all but one of the labelling options examined, participants were willing to pay more for devices that carried a security label. More specifically, for these four types of security label, the average WTP estimates (absolute cost and proportion of the product price) for the four devices examined were as follows: security cameras (£33.60, 34%); smart TVs (£65.71, 19%); wearables (£19.03, 27%); and thermostats (£35.76, 22%).[212] Furthermore, research conducted by Harris Interactive found that, overall, more than half of survey respondents (59%) were willing to pay a premium of 5% for a product with a security label compared to a product without.[213]

In addition, increased consumer IoT device security will act to mitigate the risks to manufacturers of cyber attacks against their products, including reputational damage, loss of consumer confidence and competitive disadvantage. The survey of manufacturers and other organisations conducted for this study examined the types of costs that businesses face as a result of a cyber attack, which could be reduced as a result of increased consumer IoT device security. Although many respondents either did not know what the impacts of a breach would be, or did not believe the response was applicable to them (between 27% and 60% across the available options, N=23), more than half of respondents (61%) indicated that their organisation would face some type of cost as a result of a consumer IoT breach. The following chart shows that these costs relate to offering support to affected consumers (59%), issuing guidance (55%) and reputational damage (52%). A further 43% expect costs related to increased security updates.

Figure 4.4: Costs faced by organisations as a result of a consumer IoT breach



Source: CSES Survey findings (business and other organisations), Q12, N=23

[211] Johnson, S.D., Blythe, J.M., Manning, M., & Wong, G.T.W. (2020). The impact of IoT security labelling on consumer product choice and willingness to pay.
[212] Johnson, S.D., Blythe, J.M., Manning, M., & Wong, G.T.W. (2020). The impact of IoT security labelling on consumer product choice and willingness to pay.
[213] Harris Interactive. (2019). Consumer Internet of Things Security Labelling Survey Research Findings.

4.1.3 Assessment of additional regulatory impacts

Although there are some clear costs and benefits related to the implementation of the Government's proposed regulatory approach, there are also a range of further impacts that could affect the market beyond the costs and benefits described above. Examples include enforcement costs, coherence with existing legislation and international cooperation, the potential of a "race to the bottom" and the potential impact on innovation.

Taking the first of these, at the time of the fieldwork for this study, a finalised enforcement approach had not yet been identified. For instance, it was noted by interviewees that penalties for non-compliance needed to be clarified as these can play an important role in driving business behaviour and could result in significant costs for businesses. However, research shows that the most effective enforcement strategies to achieve compliance employ a mix of persuasion and coercion. That is to say, punishment is more effective for 'rational agents', i.e. companies that would not comply voluntarily; but the effects of penalties can be uneven to organisations of different sizes and capabilities.[214] On the other hand, incentivisation can be effective for companies which want to comply but might lack the resources, and can be rewarded to go beyond compliance, as per the ENISA recommendations for funding schemes for SMEs and incentives for innovation and R&D activities in cyber security.[215]

Turning to coherence with existing legislation and international cooperation, vulnerability disclosure management needs to be considered in the context of criminal offences stipulated in the Computer Misuse Act 1990. ENISA, for example, has concluded that such legislation can have a 'chilling' effect, disincentivising security researchers with regard to vulnerability detection for fear of prosecution.[216] In addition, many consumer IoT manufacturers and retailers are subject to a range of existing legislation, including the General Data Protection Regulation (GDPR), the EU's Radio Equipment Directive (RED), the EU Cybersecurity Act and the EU's Directive concerning contracts for the sale of goods.

Furthermore, the international aspects of the market, as well as the prevailing cyber security risks, necessitate that the UK considers the international context of consumer IoT regulations. As highlighted above, the complexity of supply chain management for many manufacturers of consumer IoT devices poses significant challenges and any regulation will potentially affect UK companies selling to different jurisdictions. This highlights the need for continued engagement and alignment with international standards development; a point highlighted by all interviewed stakeholder groups. In this respect, relevant examples include the UK's involvement in the development of the draft European Standard on Cyber Security for Consumer Internet of Things (ETSI EN 303 645),[217] as well as the UK-Singapore IoT Secure by Design Statement[218] and the Statement of Intent regarding the security of the Internet of Things, signed by the Interior, Homeland Security and Public Safety Ministers of Australia, Canada, New Zealand, the United Kingdom and the United States.[219]

With regard to the potential "race to the bottom", stakeholders across all groups interviewed for this study envisage that companies may be tempted to focus on the top three guidelines at the expense of the core goal of embedding security by design practices in their development and manufacturing

[214] Gunningham, N. (2010). Enforcement and compliance strategies. The Oxford handbook of regulation, 120, pp.131-35.
[215] ENISA. (2019). Industry 4.0 – Cyber security Challenges and Recommendations.
[216] Guinchard, A. (2017). The Computer Misuse Act 1990 to Support Vulnerability Research? Proposal for a Defence for Hacking as a Strategy in the Fight against Cybercrime (March 27, 2017). 2017 Journal of Information Rights, Policy and Practice 2(2) 1. Available at SSRN: https://ssrn.com/abstract=2946763 or http://dx.doi.org/10.2139/ssrn.2946763.
[217] ETSI. (2019). Draft European Standard, Cyber; Cyber Security for Consumer Internet of Things, ETSI EN 303 645.
[218] British High Commission Singapore. (2019). Secure by Design – UK-Singapore IoT Statement, Joint Statement on cooperation between Singapore and the United Kingdom on the Internet of Things.
[219] Attorney General's Office and Home Office. (2019). Guidance: Statement of Intent regarding the security of the Internet of Things.

processes. As a result, the top three guidelines have the potential to become a security ceiling rather than a minimum requirement.[220] Furthermore, stakeholders perceive that labelling in this context could engender consumer overconfidence in product security.[221,222]

With this noted, many stakeholders recognised that this "race to the bottom" would be mitigated to some extent by Government efforts to encourage manufacturers to implement all thirteen Code of Practice guidelines and the timely inclusion of additional guidelines in regulation (through the proposed staged approach).[223] However, although the first three guidelines are considered to be relatively easy to implement, a cyber security expert interviewed for this study raised concerns with regard to the ease with which manufacturers and developers would be able to implement some of the remaining ten CoP guidelines. For example, guideline 10 on monitoring system telemetry data for security anomalies could pose challenges for many developers and manufacturers with regard to understanding what behaviour is normal compared with a security anomaly.

Last but not least, there is risk of regulation having a negative effect on innovation.[224] The primary mechanism for such an effect is perceived to be linked to the position of the UK market versus other jurisdictions, with:

- The need to comply with multiple regulatory regimes potentially hindering investment in innovation;
- The dissuasion of innovative companies and products entering the UK market from other jurisdictions due to the regulatory regime.

However, industry stakeholders and cyber security experts interviewed for this study noted that embedding security by design should not impact innovation and that engagement with EU and international standards processes and legislators will help mitigate any negative impact on innovation.

In summary, the implementation of aspects of the top three CoP guidelines will require manufacturers and developers of consumer IoT products to bear a range of administrative and substantive compliance costs. However, the general consensus is that although there may be a need for product redesign in some instances, such costs involved will not be significant and would likely not need to be passed on to consumers. That said, there are a range of complexities, particularly with regard to the second and third minimum security requirements (namely, those related to vulnerability disclosure and software updates) and the practicalities of the regulation. Considering security labelling specifically, the research suggests that the implementation for manufacturers and developers of consumer IoT products is likely to bear significant costs.

Set against these costs, however, significant benefits are envisaged as a result of the implementation of minimum security requirements. There is a potential for increased trust in the consumer IoT market, driving greater consumer IoT adoption and sales volumes. Furthermore, greater recognition of the added value of security, to the product and as perceived by the consumer, could drive further improvements in security and thus, trust, adoption and sales volume. Lastly, increased device security will act to mitigate the risks to manufacturers and developers of cyber attacks against their products,

[220] Open Rights Group. (2019). Response to the Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security.
[221] The Institute of Engineering and Technology. (2019). Response to DCMS, Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security.
[222] UK Computing Research Committee (UKCRC). (2019). Response to DCMS, Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security.
[223] Department for Digital, Culture, Media & Sport (DCMS). (2020). Consultation Outcome: Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation.
[224] Department for Digital, Culture, Media & Sport (DCMS). (2020). Consultation Outcome: Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation.

which can be costly considering potential reputational damage, loss of consumer confidence and competitive disadvantage.

4.2 Potential Impact of Government Regulation on consumers

Information on consumer IoT device security is often not available, accessible or easily understandable to consumers. As found by researchers in a review of consumer IoT devices, "manufacturers provide tool little publicly available information about the security features of their device" and rarely provide cyber hygiene advice.[225] As a result, consumers generally assume products are safe and secure.[226] The following section explores the potential impacts the proposed regulatory approach could have on consumers.

4.2.1 Assessment of the benefits to consumers of the proposed regulatory approach

As a result of the implementation of aspects of the top three CoP guidelines, consumers will probably accrue both direct personal benefit and indirect benefits related, for example, to improved economy-wide cyber security. These include the potential reduction in the number of insecure consumer IoT devices purchased and, as such, the number of breaches experienced by consumers.[227] This is true in the short term, as such a regulation will ensure new products brought to market are secure, but also in the long term, as the significant numbers of legacy devices are phased out.

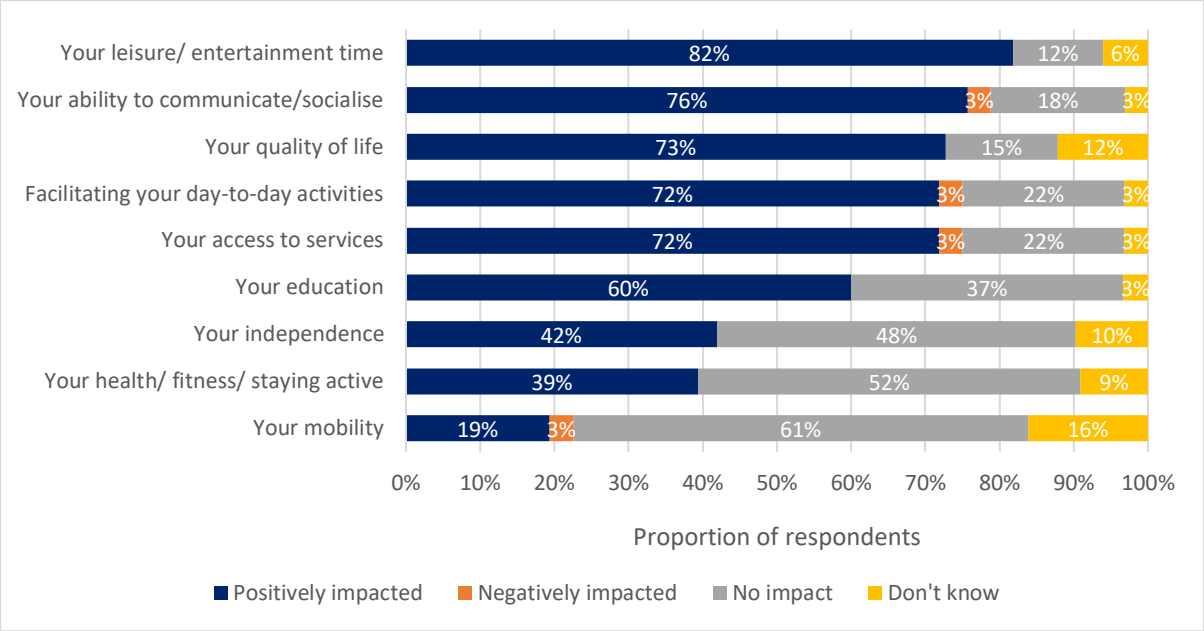
To understand the scale of this reduction, it is helpful to draw parallels with the Cyber Essentials scheme. Cyber Essentials is a certification scheme that aims to help organisations prevent the most common cyber attacks by implementing basic security measures. According to the Cyber Essentials website implementing the ten security measures can protect organisations against some 80% of cyber attacks. Although the scope of the Cyber Essentials scheme is much broader than consumer IoT devices and the top three CoP guidelines, this illustrates that many cyber attacks can be prevented by basic security measures.

Building on this, confidence and trust in the consumer IoT market should grow[228], driving greater purchasing of consumer IoT devices and greater realisation of the benefits associated with the IoT, including for example increased opportunities for education, social mobility, access to services and healthcare. The survey of consumers conducted for this study illustrates the extent of these positive impacts. As shown below, more than half the respondents stated that having access to a consumer IoT device positively impacted their leisure/entertainment time (82%, N=33), their ability to communicate and socialise (76%, N=33), their quality of life (73%, N=33), their completion of day-to-day activities (72%, N=32), their access to services (72%, N=32) and their education (60%, N=30).

Considering mobility and health, fitness and staying active, the data suggests that respondents with a long-term illness, health problem or disability are less likely to realise positive impacts. For example, 50% (N=27) of respondents without a disability or health problem stated positive impacts with regard to health, fitness and staying active, compared with only 11% (N=9) of respondents with such a health problem or disability. However, as the number of respondents with a long-term illness, disability or health problem was limited, this finding may not be representative.

[225] Blythe, J. M., Sombatruang, N. & Johnson, S. D. (2019). What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages? Journal of Cybersecurity, Research Paper, 2019, 1-10.
[226] Department for Digital, Culture, Media & Sport (DCMS). (2020). Consultation Outcome: Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation.
[227] Department for Digital, Culture, Media & Sport (DCMS). (2019). Mandating Security Requirements for Consumer 'IoT' Products, Consultation Stage Impact Assessment.
[228] techUK. (2019). Response to Department for Digital, Culture, Media & Sport Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security.

Figure 4.5: Positive impacts from use of consumer IoT, by type of impact[229]



Source: Survey findings (consumers), Q12 & 17, N=36

Assuming an increase in sales and adoption of consumer IoT as a result of more secure consumer IoT devices, research into IoT adoption and usage in Taiwan also suggests that consumer IoT might have a tipping point after which network externalities would occur. Network externalities can be defined in the following way: ''the value or effect that users obtain from a product or service [and which] will bring about more value to consumers with the increase of users, complementary products, or services''.[230] Assuming that value in this instance also includes security and a positive view of device usage, consumers are likely to experience both continued improvements in cyber security protection and shift their perceptions towards device usage benefits. Therefore, continued cyber security improvements in specific products, as well as the wider cyber environment, are likely to lead to increasing adoption of IoT devices by consumers.

Also important is the potential positive impact on consumer awareness of cyber security issues. Although, as described below, these impacts will be particularly prominent in the case of implementing security labels (i.e. Option A), implementing aspects of the top three CoP guidelines could also drive consumer awareness. The strengthened engagement of manufacturers and developers with cyber security issues, as a result of implementing basic security requirements, could improve the recognition of the added value security provides to their products and to their consumer base. This could increase the use of security as a market differentiator. As a result, greater coverage of cyber security within product marketing could drive increased awareness and understanding of consumer IoT security issues.

This increased consumer awareness could further result in consumer pressure to further the improvement of consumer IoT product security and thus the realisation of the benefits highlighted above. Additionally, if security awareness progresses into knowledge and the development of new consumer skills, then IoT device adoption might be achieved indirectly. More specifically, according to

[229] Combined results of question 12 (N=9) and question 17 (N=27) from the survey conducted for this study targeting consumers: 'How has having access to a consumer IoT device impacted on the following aspects of your life'. Question 12 was answered specifically by respondents who have, or who have members of their household, with a long-term illness, health problem or a disability which limit daily activities or work. Question 17 was asked to all other respondents.

[230] Katz, M. L., & Shapiro, C. (1985). Network externalities, competition, and compatibility. The American economic review, 75(3), 424-440.

the notion of perceived behavioural control, consumers have been observed to not adopt IoT technologies, regardless of intention, unless they perceive that they have the control and the resources to do so (knowledge or skills in this case).[231,232]

With regard to labelling, it is anticipated that this will result in better informed purchasing decisions, which, under Option A, could encourage manufacturers to implement some of the Code of Practice guidelines. For example, the labels could give consumers the information to assess relative security features at the point of purchase and potentially drive the market towards the deployment of devices with longer minimum support periods. However, there are differing viewpoints with other stakeholders stating that indicating the minimum length of time for which the product will receive security updates (i.e. through labelling) will in fact bring greater opportunities for built-in obsolescence. For instance, consumers might dispose of devices after the minimum support period, assuming they are no longer secure. Moreover, there is uncertainty over whether consumers will be in a position to make a well-informed assessment given the information that will be available to them at the point of purchase.

In addition, there are a range of factors external to the regulation that will support the realisation of consumer benefits over time, including general consumer IoT market trends, as highlighted by interviewed business stakeholders, and the continued development of other legislation. Business interviewees stated that the movement of companies towards as-a-service business models for consumer IoT will probably drive positive security impacts. For instance, in a range of sectors, such as car insurance, consumer IoT devices are more commonly being provided as part of a service offering. New roles are also emerging in the market, for example companies that install and configure whole consumer IoT systems and networks of products. In both scenarios, company brand and reputation become more prominent considerations and the onus for understanding and ensuring security is taken away from the consumer.

With regard to other legislative developments, a range of relevant EU legislation could affect the market: the GDPR may yield positive impacts on how economic operators approach the protection and security of personal data; the EU Cybersecurity Act is yet to make significant steps but could result in EU-wide certification frameworks relevant to the security of consumer IoT products; and the European Commission is currently assessing the impact of activating cyber security-related delegated acts contained within the Radio Equipment Directive.

4.2.2 Assessment of the challenges to consumers of the proposed regulatory approach

Beyond the benefits for consumers, there are also a range of potential negative impacts or challenges that could result from the implementation of the proposed regulatory approach.

A key issue to be considered is where the burden lies with regard to understanding and ensuring security. If Option A (i.e. security labelling) were to be adopted, business and consumer associations interviewed for this study highlighted that this would maintain the burden on the consumer in terms of needing to be informed and willing to take action. However, if manufacturers and developers are required to implement aspects of the top three CoP guidelines, those stakeholders will be required to take the burden for ensuring basic security, thereby removing this challenge for consumers. As highlighted above, future market trends could also support the removal of this burden from the consumer. Furthermore, it is anticipated that a labelling system could engender consumer overconfidence in the security of consumer IoT products. An assumption of security on the part of the

[231] Ajzen, I. (2011). "The theory of planned behaviour: reactions and reflections", Psychology & Health, Vol. 26 No. 9, pp. 1113-1127.

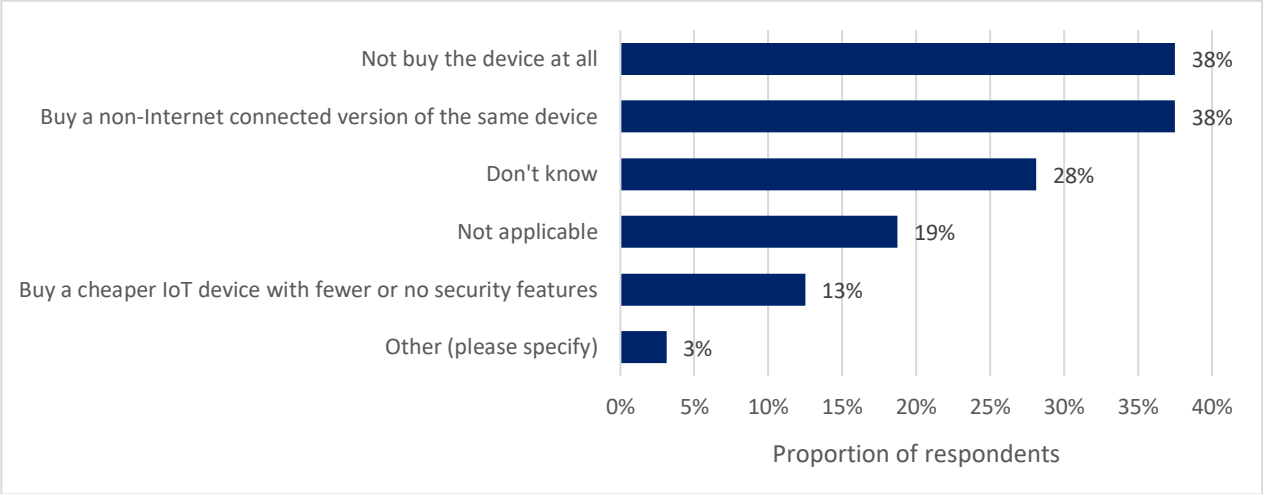
[232] Gao, L., & Bai, X. (2014). A unified perspective on the factors influencing consumer acceptance of Internet of Things technology. Asia Pacific Journal of Marketing and Logistics.

consumer could lead to challenges related to the legacy equipment and infrastructure, and company failures.

Although new products would have improved security following regulatory intervention, it will take a number of years before the significant range of insecure legacy equipment and infrastructure is updated. For example, research by DeviceAtlas found that many smartphones globally are using operating systems (OS) that are no longer supported by security updates.[233] Considering smartphones in the UK, for example, it has been found that at least 7% of such devices are running the Android 6 OS or below, which was released in October 2017 but did not receive a security update throughout 2019.[234] Until such insecure devices are no longer in use, an assumption of security on the part of the consumer could lead to poor security practices and greater risk of cyber attack. With regard to company failures, in the event that a manufacturer or developer of a consumer IoT product fails, consumers would probably continue to assume their devices are secure even though such device are no longer receiving security support. This could also increase the cyber risk for consumers.

Additionally, there is a potential for reduced consumer access to devices and thus to the benefits of consumer IoT through two mechanisms. First, some industry stakeholders interviewed for this study indicated that compliance costs may need to be passed on to the consumer, thereby increasing the price of some consumer IoT devices. Data from the survey of consumers conducted for this study illustrates that, although many stakeholders are willing to pay more for improved security (see evidence on WTP in Section 4.1.1), such a price increase could have a negative impact on those who are not able or willing to pay more. As shown in the following chart, respondents most commonly reported that they would not buy the device at all (38%, N=32) or buy a non-Internet connected equivalent (38%) if they were not willing to spend more on a consumer IoT device.

Figure 4.6: Consumer intentions if unwilling to spend more on a consumer IoT device



Source: CSES Survey findings (consumers), Q25, N=32

That said, the majority of IoT businesses interviewed for this study considered that it would be unlikely compliance costs would be significant enough to need to be passed on to consumers. As such, this would be unlikely to affect consumer access to IoT products.

Second, there is a potential for non-UK companies to choose not to comply with UK regulation and therefore stop selling to the UK market. This has the potential to reduce the purchasing options available to UK consumers. However, considering the maturity of the UK market, as well as the advancing regulatory developments on consumer IoT globally, but particularly in the EU (for instance,

[233] DeviceAtlas. (2019). Blog: Mobile OS versions by country.
[234] DeviceAtlas. (2019). Blog: Mobile OS versions by country.

the ETSI draft standard on consumer IoT security and the developments related to the RED), it is considered unlikely that manufacturers and developers will stop selling to the UK market.

As such, the general consensus across the surveys, the interviews conducted, and the literature reviewed is that the regulatory approach is unlikely to negatively affect access to consumer IoT products. The next sub-section examines how the potential impacts may be experienced differently across different demographic groups.

4.2.3 Assessment of the impacts across demographic groups

There is limited evidence from this study that certain demographic groups will experience specific negative impacts as a result of the implementation of aspects of the top three CoP guidelines. However, it has been found that certain consumer groups will experience greater positive impacts than others, in particular reflecting and reinforcing existing trends related to access to the benefits provided by consumer IoT products and technology more generally. This assessment primarily focuses on age, gender and household income.

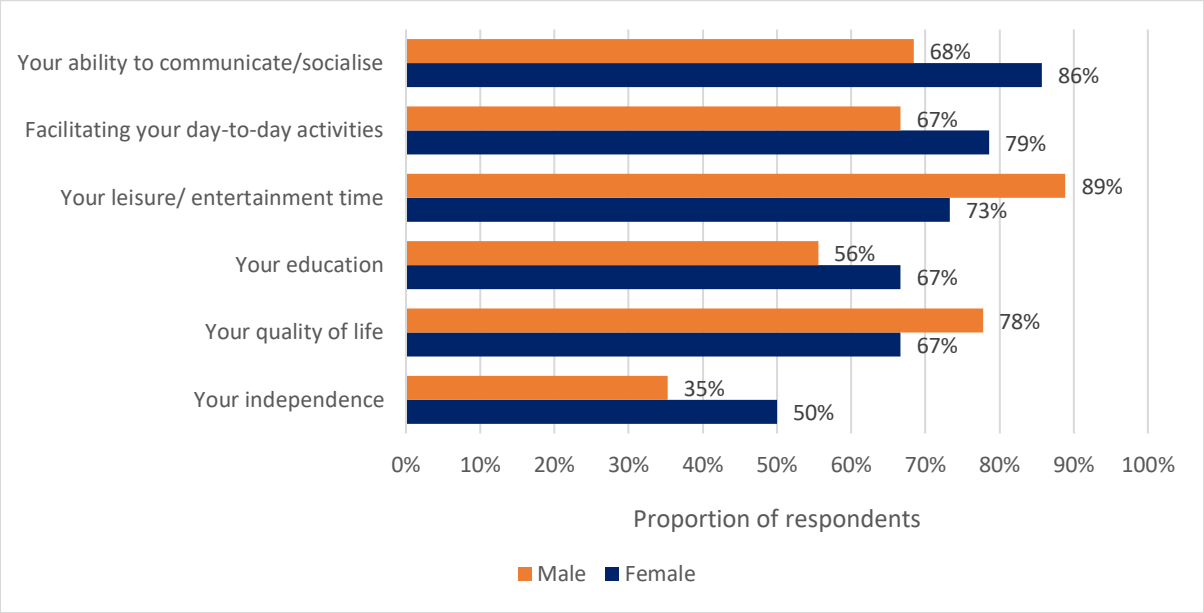
With regard to age, older consumers are perceived to be more concerned about security and privacy. For instance, a 2017 survey of consumer cyber security perceptions reportedly found that consumers over 55 pay more attention to cyber security issues than younger respondents. More specifically, in relation to password management, 70% of older consumers reported reusing passwords, compared with 80% of younger consumers. Although 32% of older consumers only changed their passwords when forced, this figure was 42% in younger consumers.[235] In addition, data on expectations of fraud also indicates older consumers are more mindful of security: for example, a survey of 1,767 US-based respondents found that individuals over 55 years of age were more likely to consider fraud to be inevitable (53%) compared with younger generations (ages 35-54: 44%; 24-34: 40%; and 18-23: 34%).[236]

However, the qualitative responses to the survey suggest there are differences in adoption, as well as understanding and education, on security within the older consumers group. Consumers over 65 are perceived to have lower reliance on technology and consumer IoT but also less knowledge and awareness of security than those younger than 65. As such, consumers over 65 are likely to experience a balance of positive impacts as lower adoption could result in the realisation of fewer benefits compared to other age groups, but regulation will also deliver security benefits that such consumers would not experience otherwise due to their lack of security knowledge. On the other hand, consumers aged 55-64, are likely to complement higher security caution with better security practices. Therefore, this group of consumers would potentially benefit to a lesser extent in terms of security gains than younger consumers who are less mindful of security issues.

Regarding gender, although many qualitative responses from the surveys and interviews conducted for this study considered the issues covered not to be gender sensitive, the data suggests that in fact, female and male respondents realise the benefits of consumer IoT products differently. For instance, as illustrated in the following chart, female respondents report higher positive impacts in relation to education (67% versus 56%, N=30), ability to communicate/socialise (86% versus 68%, N=33), independence (50% versus 35%, N=31) and facilitating day-to-day activities (79% versus 67%, N=32). On the other hand, male respondents report higher positive impacts in relation to quality of life (78% versus 67%, N=33) and leisure/entertainment time (89% versus 73%, N=33).

[235] Loeb, L. (2017). Article: Cybersecurity Awareness Varies By Demographic, Survey Reveals, Reporting on the First Data 2017 Consumer Cybersecurity Survey in SecurityIntelligence.
[236] First Data. (2018). Protecting Personally Identifiable Information Survey.

Figure 4.7: Positive impacts of consumer IoT, by gender



Source: CSES Survey findings (consumers), Q12 & Q17, N=33

In addition, gender has been found to act as a moderating factor on risk, with technology adoption by females more greatly influenced by overall perceived risk than males.[237] As such, perceptions of greater trust in the consumer IoT market, as engendered by the regulatory approach, are expected to diminish perceived risk and thus facilitate adoption more readily with female than male consumers.

Turning to socio-economic status, the existing research suggests that there is a possible link between security, the number of IoT devices and socio-economic status of households. For instance, parallels can be drawn with findings on the adoption of 'media technologies' by families with children. Research on this topic demonstrates a positive correlation between income levels and adoption of new digital technologies, namely, households with higher incomes provide a more 'media-rich' environment (57% of higher income households compared to 31% of lower income households).[238] In this context, 'media-rich' refers primarily to household ownership of new media (for example, personal computers, Internet access, mobile phones), but also includes old media (for example, books).

In addition, it has been found that lower income parents are more likely to provide older or cheaper versions of technological devices in the home.[239][240] However, while this research finds the relationship between income and access to media to be straightforward, it suggests that in families with children, parental education level can have a moderating effect on adoption of digital technology. For instance, less educated parents, even if they are from a lower income bracket, might be more likely to provide 'media-rich' homes for their children than more educated parents, who are more likely to encourage

[237] Hubert, M., Blut, M., Brock, C., Backhaus, C., & Eberhardt, T. (2017). Acceptance of smartphone-based mobile shopping: Mobile benefits, customer characteristics, perceived risks, and the impact of application context. Psychology & Marketing, 34(2), 175-194.

[238] Livingstone, S. (2007). 'Strategies of parental regulation in the media-rich home.' Computers in Human Behavior 23(3), 920–941.

[239] Livingstone, S., Mascheroni, G., Dreier, M., Chaudron, S., & Lagae, K. (2015). How parents of young children manage digital devices at home: The role of income, education and parental style.

[240] DeviceAtlas. (2019). Blog: Mobile OS versions by country. This research further illustrates the link between lower income and older / cheaper devices in relation to OS's in use that are no longer supported by security updates. The research finds that the situation is worse in lower income countries. In the UK, at least 7% of Android smartphones are running unsupported OS's, but this figure is much higher, for example, in India (at least 25%), Nigeria (at least 22%) and Egypt (nearly 40%) to name a few where data is available.

their children to undertake more 'traditional' (i.e. non-digital) activities.[241] The aforementioned findings, assuming that higher levels of education and higher income are to an extent positively correlated, indicate the complexity of predictions in the adoption of IoT devices, since the effects of education and income might cancel each other out. These findings are supported by the qualitative feedback from the surveys and interviews conducted for this study. More specifically, stakeholders indicated that higher income households are more likely to own more consumer IoT devices than lower income households and, secondly, higher income households are more likely to be conscious of security issues.

In terms of the potential impact of the minimum security requirements on different socio-economic groups, this study's findings suggest that higher income consumers will also realise greater benefits to more secure access than lower income households, due to a higher average number of devices owned. On the other hand, lower income groups will be likely to benefit from greater positive security effects than higher income groups due to the fact that the number of devices with poor security will be gradually minimised in these households.

In summary, the implementation of aspects of the top three CoP guidelines could have significant benefits to consumers of all types as a result of reductions in the number of insecure devices on the market, a greater realisation of the benefits of consumer IoT as a result of increased adoption, and improved cyber security awareness. These benefits may also be supported over time by external factors such as industry trends relating to emerging business models and roles, and the impacts of relevant EU legislation on the market.

Considering the challenges facing consumers, a key issue relates to ensuring the burden for being informed on cyber security does not lie only with the consumer. Should security labelling be introduced, the onus will remain on the consumer. However, if manufacturers and developers are required to implement aspects of the top three CoP guidelines, they will be responsible. Furthermore, security labelling could engender consumer overconfidence which can exacerbate challenges, such as the presence of vulnerable legacy equipment and infrastructure that will remain part of systems and networks for a number of years. Additionally, although considered unlikely, there are potential challenges related to reduced consumer access, which could be experienced as a result of increased devices prices, as manufacturers pass on compliance costs, or the potential for non-UK companies to choose not to comply with the regulation and therefore stop selling to the UK market.

Although consumer access is unlikely to be greatly affected, there are likely to be some differences in how the impacts of the regulatory approach are experienced by different demographic groups. There is limited evidence that particular demographic groups will experience specific negative impacts. However, the study suggests that certain consumer groups will experience greater positive impacts than others, reflecting and reinforcing existing trends related to access to the benefits of consumer IoT products and technology more generally.

[241] Livingstone, S. (2007). 'Strategies of parental regulation in the media-rich home.' Computers in Human Behavior 23(3), 920–941.

5. Overall Conclusions

Overall, the study confirms that there will be strong growth in future years in the overall adoption of consumer IoT devices. In the UK, the number of IoT connections is predicted to grow from 13 million in 2016 to over 150 million by 2024. But there will be differences in this respect between the three product categories considered in this study: 'Big Ticket' items (smart televisions, white goods, kitchen appliances), 'Connecting the Home' items (smart speakers, smart meters, other devices that are used to control and monitor activity within a home), and 'Consumer Lifestyle' items (wearables, toys, smartphones, etc.).

Future growth will depend on reducing the barriers to adoption of consumer IoT including concerns related to cost, security, privacy and ease of use. The affordability of technology, in particular, is a key consideration for potential consumers but trust in the security and privacy protection measures for consumer IoT devices are also significant drivers of adoption and market growth.

Emerging business models are also important. For instance, the study finds that economic operators are more readily moving to as-a-service business models, either by offering services to support the use of consumer IoT devices or by requiring the consumer to use an IoT device to participate in a service (examples include the car insurance industry providing 'black boxes' to monitor driving performance). It is anticipated that these emerging business models will require greater focus on cyber security, as reputation and brand are more important considerations for companies providing services rather than standalone devices.

As growth continues and perhaps accelerates in the adoption of consumer IoT devices, so too will the threat of cyber attacks arising from IoT vulnerabilities. Although the cyber threat landscape is constantly evolving and is becoming characterised by more sophisticated and complex threats, this study suggests that the majority of threats facing consumer IoT devices exploit simpler vulnerabilities, such as the use of default or hard coded passwords. That said, there are a wide range of cyber threat types relevant to consumer IoT devices, including Distributed Denial of Service (DDoS) attacks, spoofing and repudiation attacks.

The study finds that consumer IoT attacks are often not particularly difficult to implement, as there are a wide range of vulnerabilities commonly found in devices that can be exploited. In addition to the use of default passwords, such devices commonly have vulnerabilities relating to insecure network services, ineffective ecosystem interfaces, lack of device management and a lack of secure update mechanisms. Furthermore, many manufacturers and developers of consumer IoT devices do not have fast and reliable vulnerability disclosure management practices. More generally, the IoT market will change in the future (influenced by developments relating to 5G, cloud, changing business models) which will lead to the emergence of new cyber security vulnerabilities.

Cyber attacks exploiting consumer IoT vulnerabilities can have significant impacts both at the individual and business levels. This study's survey of consumers revealed that 23% of respondents had received a security warning notification from their IoT device and 11% reported their device having been infected by a virus, malware or ransomware. Attacks can result in privacy breaches, financial loss and service interruption. Consumer IoT products that are affected by security issues can lead to emotional distress for their users, as reported by 17% of the survey respondents who had experienced a cyber security issue. According to the study's business survey, the main impacts arising from IoT cyber vulnerabilities reported as being very damaging are 'reputational damage to the device manufacturer/ retailer' (45% of respondents), 'loss of consumer confidence' (55%) and 'loss of personal/customer data' (57%). From businesses' perspective, IoT cyber attacks can also lead to financial losses which for smaller companies can represent a significant proportion of their revenues.

Looking ahead, and in light of the prospect of continued rapid consumer IoT market growth, it is clearly important to develop effective ways of addressing the risks of cyber attacks.

Regarding the possible impact of potential future regulation on the consumer IoT market, the study finds that manufacturers and other economic operators will incur a range of compliance costs. The extent of these costs is difficult to quantify and will depend on the nature of the regulatory approach and the extent to which product redesign costs are required. Furthermore, there are additional complexities, for example in relation to supply chain management and thus the implementation of vulnerability disclosure practices or software updates. However, it is likely that these costs will not be significant and will therefore not be passed on to consumers.

At the same time, there should be positive economic effects, including increasing sales volumes, as a result of greater confidence and trust in the security of consumer IoT devices. Additionally, increased device security should act to mitigate the risks to manufacturers of cyber attacks on their products and the related negative impacts. There could also be significant benefits to consumers such as a reduction in the number of insecure consumer IoT devices, increased confidence and trust leading to increased ownership and greater realisation of the benefits associated with the IoT. A major challenge, however, is to ensure that the responsibility for being informed about cyber security does not lie just with the consumer.

The potential impact of regulatory intervention on certain demographic groups in terms of age, gender and household income suggests that certain groups will not experience specific negative impacts. However, certain consumer groups will benefit from greater positive impacts as a result of the implementation of the minimum security requirements, due to differences in rates of adoption. Overall, the study suggests that the benefits of regulation should outweigh the drawbacks and costs.

Appendix A: Bibliography

- Ahola, M. (2019). The Role of Human Error in Successful Cyber Security Breaches.
- Ajzen, I. (2011). "The theory of planned behaviour: reactions and reflections", Psychology & Health, Vol. 26 No. 9, pp. 1113-1127.
- Akerlof, G.A. (1978). The market for "lemons": Quality uncertainty and the market mechanism. In Uncertainty in economics (pp. 235-251). Academic Press.
- al-Khateeb, H. M., & Epiphaniou, G. (2016). How technology can mitigate and counteract cyber-stalking and online grooming. Computer Fraud & Security, 2016(1), 14-18.
- All, A. (2016). New IoT Threat Exploits Lack of Encryption in Wireless Keyboards. eSecurity Planet.
- Alomari, E., Manickam, S., Gupta, B. B., Karuppayah, S., & Alfaris, R. (2012). Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art. International Journal of Computer Applications, 49(7), 24–32.
- Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the Internet of Things: Security and privacy issues. IEEE Internet Computing, 21(2), 34-42.
- Anderson, R. (2001). 'Why information security is hard-an economic perspective.' In Computer security applications conference, 2001. Acsac. proceedings 17th annual, pp. 358_365. IEEE, 2001.
- Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., et al. (2017). Understanding the Mirai botnet. In Proc. USENIX Security Sympsion'17.
- Ashar, J. (2019). Regulatory proposal on mandatory IoT security label. GovTech Leaders.
- Ashok, I. (2016). Hackers leave Finnish residents cold after DDoS attack knocks out heating systems. International Business Times.
- Attorney General's Office and Home Office. (2019). Guidance: Statement of Intent regarding the security of the Internet of Things.
- Bannan, C. (2016). The IoT threat to privacy. Techcrunch.
- Bansal, G., & Zahedi, F. M. (2015). Trust violation and repair: The information privacy perspective. Decision Support Systems, 71, 62-77.
- Bauer, H. et al. (2017). Security in the Internet of Things. McKinsey & Company.
- BBC. (2020). One billion Android devices at risk of hacking. BBC.
- BizIntellia. (2020). Trending: IoT malware attack.
- Blythe, J. M., Sombatruang, N. & Johnson, S. D. (2019). What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages? Journal of Cybersecurity, Research Paper, 2019, 1-10.
- Blythe, J.M., Johnson, S.D., & Manning, M. (2020). What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices, Crime Sci (2020) 9:1.
- British High Commission Singapore. (2019). Secure by Design – UK-Singapore IoT Statement, Joint Statement on cooperation between Singapore and the United Kingdom on the Internet of Things.
- Busch, J. (2019). Yes, Your Video Baby Monitor Can Be Hacked. No, You Don't Have to Stop Using It.
- Businesswire. (2017). Survey: Nearly Half of U.S. Firms Using Internet of Things Hit by Security Breaches. Businesswire.

- Capgemini. (2017). Consumer Security and the IoT.
- Carrigan, M. (2019). The institutionalisation of behavioral surplus: a quick recap on the Age of Surveillance Capitalism.
- CERT.Pl. (2014). Large-scale DNS redirection on home routers for financial theft.
- Cimpanu, C. (2017). Smart Drawing Pads Used for DDoS Attacks, IoT Fish Tank Used in Casino Hack.
- Cision. (2017). The UK Toys & Games Market 2017-2022.
- Claburn, T. (2015). Your Audi As Amazon Package Drop.
- Cloudflare. (2017). Inside the Infamous Mirai IoT Botnet: A Retrospective Analysis.
- Cloudflare. (n.d.). What is a Denial-of-Service (DoS) Attack?
- Collen, A., Nijdam, N. A., Augusto-Gonzalez, J., Katsikas, S. K., et al. (2018). Ghost-safe-guarding home IoT environments with personalised real-time risk control. In International ISCIS Security Workshop (pp. 68-78). Springer, Cham.
- Conger, K. (2016). The Mirai botnet's Internet takedown opens up a new market for attackers and defenders. TechCrunch.
- Constantin, L. (2014). Attack campaign compromises 300,000 home routers, alters DNS settings. PCWorld News.
- Constantin, L. (2014). Cybercriminals compromise home routers to attack online banking users. PCWorld News.
- Cruz, B., Gómez-Meire, S., Ruano-Ordás, D., Janicke, H., Yevseyeva, I., & Méndez, J. R. (2019). A Practical Approach to Protect IoT Devices against Attacks and Compile Security Incident Datasets. Scientific Programming, 2019, 1–11.
- CyberThreat Alliance. (2018). The Illicit Cryptocurrency Mining Threat.
- DarkTrace. (2018). Global Threat Report 2017.
- Daube, N. (2019). Regulating the IoT: Impact and new considerations for cyber security and new government regulations, Help Net Security.
- Department for Digital, Culture, Media & Sport (DCMS). (2018). Code of Practice for Consumer IoT Security.
- Department for Digital, Culture, Media & Sport (DCMS). (2018). Secure by Design: Improving the cyber security of consumer Internet of Things Report.
- Department for Digital, Culture, Media & Sport (DCMS). (2019). Mandating Security Requirements for Consumer 'IoT' Products, Consultation Stage Impact Assessment.
- Department for Digital, Culture, Media & Sport (DCMS). (2020). Consultation Outcome: Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation.
- DeviceAtlas. (2019). Blog: Mobile OS versions by country.
- Digital Trends, (2020). The best blood pressure monitors for 2020.
- Draktrace. (2018). Global Threat Report 2017.
- ENISA. (2014). Threat Landscape and Good Practice Guide for Smart Home and Converged Media; and IoT.
- ENISA. (2015). Security and resilience of smart home environments.

- ENISA. (2015). Threat landscape for smart home and media convergence.
- ENISA. (2016). Common position on cyber security.
- ENISA. (2018). Economics of vulnerability disclosure.
- ENISA. (2019). ENISA Threat Landscape Report 2018.
- ENISA. (2019). Industry 4.0 – Cyber security Challenges and Recommendations.
- Ericsson. (2016). Wearable technology and the internet of things, Consumer views on wearables beyond health and wellness.
- ETSI. (2019). CYBER; Cyber Security for Consumer Internet of Things. Valbonne-Sophia Antipolis: ETSI.
- ETSI. (2019). Draft European Standard, Cyber; Cyber Security for Consumer Internet of Things, ETSI EN 303 645.
- F-Secure. (2019). Attack Landscape H1 2019: IoT, SMB traffic abound.
- F-Secure. (2019). IoT threat landscape: old hacks, new devices.
- Farooq, J., et al. (2019). IoT Supply Chain Security: Overview, Challenges, and the Road Ahead.
- Fieldstadt, E. (2018). Nest camera hacker threatens to kidnap baby, spooks parents. NBC News.
- First Data. (2018). Protecting Personally Identifiable Information Survey.
- Fong, K., Hepler, K., Raghavan, R., & Rowland, P. (2018). rIoT: quantifying consumer costs of insecure Internet of Things devices. University of California Berkeley, School of Information Report.
- Fruhlinger, J. (2018). Ransomware explained: How it works and how to remove it.
- Fruhlinger, J. (2018). The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the Internet. CSO UK.
- Gao, L., & Bai, X. (2014). A unified perspective on the factors influencing consumer acceptance of Internet of Things technology. Asia Pacific Journal of Marketing and Logistics.
- Gartner. (2016). Gartner Says Worldwide Wearable Devices Sales to Grow 18.4 Percent in 2016. Gartner.
- Gartner. (2017). Leading the IoT.
- Gartner. (n.d.). Gartner Hype Cycle: Interpreting technology Hype.
- Gemalto. (2019). Almost half of companies still can't detect IoT device breaches, reveals Gemalto study.
- Gigerenzer, G. & Selten, R. (Eds.) (2002). Bounded rationality: The adaptive toolbox. MIT press.
- Google. (2019). Transparency Report: Android ecosystem security.
- Guinchard, A. (2017). The Computer Misuse Act 1990 to Support Vulnerability Research? Proposal for a Defence for Hacking as a Strategy in the Fight against Cybercrime (March 27, 2017). 2017 Journal of Information Rights, Policy and Practice 2(2) 1. Available at SSRN: https://ssrn.com/abstract=2946763 or http://dx.doi.org/10.2139/ssrn.2946763.
- Gunningham, N. (2010). Enforcement and compliance strategies. The Oxford handbook of regulation, 120, pp.131-35.
- Harris Interactive. (2019). Consumer Internet of Things Security Labelling Survey Research Findings.

- Heartfield et al. (2018). A Taxonomy of Cyber-Physical Threats and Impact in the Smart Home. Computers & Security, Vol 78, pgs 398–428.
- Hern, A. (2018). European Regulators Report Sharp Rise in Complaints After GDPR.
- Hikvision. (n.d.). Network Traffic Camera User Manual. Hikvision.
- Houses of Parliament. (2019). Cyber security of consumer devices.
- Huber, N. (2019). A Hacker's Paradise? 5G and cyber security. Financial Times.
- Hubert, M., Blut, M., Brock, C., Backhaus, C., & Eberhardt, T. (2017). Acceptance of smartphone-based mobile shopping: Mobile benefits, customer characteristics, perceived risks, and the impact of application context. Psychology & Marketing, 34(2), 175-194.
- Hypponen, M., et al. (2017). The Internet of (Vulnerable) Things: On Hypponen's Law, Security Engineering, and IoT Legislation. Technology Innovation Management Review, 7(4).
- Imperva. (n.d.) Domain name server (DNS) Hijacking.
- InfoSecurity. (2017). Global Threat Report 2017. Info Security North America.
- International Data Corporation (IDC). (2019). The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast.
- International Telecommunication Union (ITU). (2015). ITU defines vision and roadmap for 5G mobile development.
- IoT Security Foundation. (2020). Consumer IoT: Understanding the Contemporary Use of Vulnerability Disclosure – 2020 Progress Report.
- Ipsos MORI. (2020). Cyber Security Breaches Survey 2020.
- Irdeto. (2019). New 2019 Global Survey: IoT-Focused Cyberattacks are the New Normal.
- Jarman, B. (2019). 5G and Smart Homes: What You Need To Know.
- Johnson, S.D., Blythe, J.M., Manning, M., & Wong, G.T.W. (2020). The impact of IoT security labelling on consumer product choice and willingness to pay.
- Joint Committee on the National Security Strategy. (2016-2017). Cyber security: UK national security in a digital world inquiry.
- Karas, B. (2017). Hikvision Backdoor Confirmed. IPVM.
- Kaspersky. (2018). New IoT-malware grew three-fold in H1 2018. Kaspersky.
- Kaspersky. (2019). IoT under fire: Kaspersky detects more than 100 million attacks on smart devices in H1 2019.
- Katz, M. L., & Shapiro, C. (1985). Network externalities, competition, and compatibility. The American economic review, 75(3), 424-440.
- Kh, R. (2018). Patch Management is the Catalyst for Growth in the IoT Industry. Datafloq.
- Kim, S., Kimber, M., Boyle, M. H., & Georgiades, K. (2019). Sex differences in the association between cyberbullying victimization and mental health, substance use, and suicidal ideation in adolescents. The Canadian Journal of Psychiatry, 64(2), 126-135.
- Koldony, L. (2016). Affectiva raises $14 million to bring apps, robots emotional intelligence. TechCrunch.
- Kumar, R., & Rasal, A. (2018). Smart Speaker Market by Intelligent Virtual Assistant, End User, Distribution Channel, and Price – Global Opportunity Analysis and Industry Forecast, 2018-2025.

- Laughlin, A. (2020). More than one billion Android devices at risk of malware threats. Which?
- Le@rn CCTV. (n.d.). How to hack Hikvision camera (the easy way).
- Levy-Rosenthal, P. (2019). New Patent Recognizes Emoshape Founder Patrick Levy-Rosenthal as the Inventor of the First Emotion Chip.
- Levy, I. (2019). Staying smart with your Christmas gadgets.
- Livingstone, S. (2007). 'Strategies of parental regulation in the media-rich home.' Computers in Human Behavior 23(3), 920–941.
- Livingstone, S., Mascheroni, G., Dreier, M., Chaudron, S., & Lagae, K. (2015). How parents of young children manage digital devices at home: The role of income, education and parental style.
- Loeb, L. (2017). Article: Cybersecurity Awareness Varies By Demographic, Survey Reveals, Reporting on the First Data 2017 Consumer Cybersecurity Survey in SecurityIntelligence.
- Loukas. (2015). Cyber-physical attacks: a growing invisible threat. Butterworth-Heineman.
- Lueth, K. L. (2014). IoT Market – Forecasts at a glance.
- Lueth, K. L. (2018). State of the IoT 2018: Number of IoT devices now at 7B — Market accelerating.
- Manyika et al. (2015). Unlocking the Potential of the Internet of Things, McKinsey Global Institute.
- Maple. (2017). Security and Privacy in the Internet of Things. Journal of Cyber Policy, 2, 155-184.
- Marriott, H. R., & Williams, M. D. (2018). Exploring consumers perceived risk and trust for mobile shopping: A theoretical framework and empirical study. Journal of Retailing and Consumer Services, 42, 133-146.
- Mersinas, K., Sobb, T., Sample, C., Bakdash, J. Z., & Ormrod, D. (2019). Training Data and Rationality. In ECIAIR 2019 European Conference on the Impact of Artificial Intelligence and Robotics (p. 225). Academic Conferences and publishing ltd.
- Mishra, R. (2020). 15 Examples of Internet of Things Technologies in Use Today.
- Moor, J., Marshall, R., & Walsh, S. (2018). IoT Security Architecture and Policy for the Home – A Hub Based Approach. IoT Security Foundation.
- National Crime Agency. (2016). Cyber Crime Assessment 2016.
- National Cyber Security Centre (NCSC). (2016). Password Guidance: Simplifying Your Approach.
- National Cyber Security Centre (NCSC). (2017). Secure development and deployment.
- National Cyber Security Centre (NCSC). (2018). The Principles of Supply Chain Security.
- National Telecommunications and Information Administration (NTIA). (2016). 'Vulnerability Disclosure Attitudes and Actions: A Research Report from the NTIA Awareness and Adoption Group.'
- NCC Group. (2017). Security of the IoT in the home.
- Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G. & Ghani, N. (2019). Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-scale IoT Exploitations, IEEE Communications Surveys & Tutorials, April 2019.
- Newman, Daniel. (2017). Why the as-a-service model works so well.
- Newman, L. H. (2016). What We Know About Friday's Massive East Coast Internet Outage. Wired.
- NIST. (2017). NIST Special Publication 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management. NIST.

- NJCCIC. (n.d). Cyber Threat Profiles: Cryptocurrency-Mining Malware.
- NNT. (2019). Cyber-Security of the Fridge: Assessing the Internet of Things Threat.
- Nord VPN. (2018). Hacker terrorizes family by hijacking baby monitor. (Article published December 2019).
- O'Hara. (2014). Privacy and the Internet of Things.
- Ofcom. (2017). Connected Nations 2017: Data analysis.
- Ofcom. (2019). Connected Nations 2019 UK Report.
- Ofcom. (2019). The Communications Market Report: Interactive Data.
- Office for National Statistics. (2019). Crime in England and Wales: year ending December 2018.
- Office for National Statistics. (2019). Internet access – households and individuals, Great Britain: 2019, Release date: 12 August 2019.
- Office for National Statistics. (2020). Crime in England and Wales: year ending December 2019.
- Ofgem. (n.d.). Electricity generation: facts and figures.
- Open Rights Group. (2019). Response to the Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security.
- Osborne, C. (2018). ADB.Miner worm is rapidly spreading across Android devices.
- OWASP. (n.d.) Repudiation Attack.
- Pagilery, J. (2017). FTC sues maker of routers, baby monitors over security. CNN Business.
- Pappas, N. (2016). Marketing strategies, perceived risks, and consumer trust in online buying behaviour. Journal of Retailing and Consumer Services, 29, 92-103.
- Parliamentary Office of Science & Technology. (2019). POSTNOTE 593: Cyber Security of Consumer Devices. Houses of Parliament.
- Pastore, M. A., & Dulaney, E. A. (2006). CompTIA security study guide. Indianapolis, IN: Wiley.
- PenTestPartners. (2018). Blog: Internet of Things, Breaking up is hard to do… with IoT, authored by Ken Munro, 6 July 2018.
- PenTestPartners. (2018). The most common IoT device security failings of 2017.
- Petrov, C. (2019). Internet of Things Statistics 2020 [The Rise of IoT]. Techjury.
- Poremba, S. (2020). Will Weak Passwords Doom the Internet of Things (IoT)? Security Intelligence.
- Product Forge. (2018). IoT//GLA Meetup: Gary Clemo – Principal Technology Advisor at Ofcom.
- Prpl Foundation. (2016). Security guidance for critical areas of embedded computing.
- PwC. (2018). Global Consumer Insights Survey 2018: Whom do consumers really trust?
- PwC. (n.d.). Disrupting Utilities.
- Rayner, T. & Sims, G. (2019). Stock Android vs. Android One vs. Android Go. Android Authority.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- Research and Markets. (2019). Consumer IoT Market 2018 – Global Forecast to 2023: Market is Estimated to be USD 46.8 Billion by 2018 and is Projected to Reach USD 104.4 Billion.
- Root@Nasro. (2014). Information Security Blog: How I saved you're A** from the ZyNOS Attack.

- Royal Academy of Engineering. (2018). Cyber Safety and Resilience: Strengthening the Digital Systems that Support the Modern Economy.
- Security Camera King. (2009). How does a security camera system work?
- Soltan, S., Mittal, P. & Poor, H.V. (2018). BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid, Princeton University, Paper for the 27th USENIX Security Symposium.
- Stanislav, M., et al. (2015). Hacking IoT: A case study on baby monitor exposures and vulnerabilities. Rapid7.
- Statista. (2016). IoT Devices.
- Steenmans, I. & Bras, I. (2018). Networked world: Risks and opportunities in the Internet of Things.
- Suki, N. M., & Suki, N. M. (2017). Modeling the determinants of consumers' attitudes toward online group buying: Do risks and trusts matters? Journal of Retailing and Consumer Services, 36, 180-188.
- Symantec Research Labs. (n.d.) Before Toasters Rise Up: A View Into the Emerging IoT Threat Landscape.
- Symantec. (2018). Internet Security Threat Report (ISTR).
- Tanczer, L., Lopez Neira, I., Parkin, S., Patel, T. and Danezis, G. (2018). Gender and IoT Research Report: The rise of the Internet of Things and implications for technology-facilitated abuse.
- Team Cymru Threat Intelligence Group. (2014). SOHO Pharming, A Team Cymru EIS Report: Growing Exploitation of Small Office Routers Creating Serious Risks.
- techUK. (2019). Response to Department for Digital, Culture, Media & Sport Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security.
- techUK. (2019). The State of the Connected Home: Edition Three.
- Thales. (n.d). Efficient and Secure IoT Device Software Updates.
- Thales. (n.d). Implementing Cost-efficient Software Updates for Cellular IoT Deployments: Challenges, Considerations, Best Practices.
- The American Consumer Institute Center for Citizen Research. (2018). Securing IoT Devices: How Safe Is Your Wi-Fi Router?
- The Cybersecurity and Infrastructure Security Agency (CISA). (2017). ICS Advisory (ICSA-17-124-01): Hikvision Cameras. CISA.
- The Information. (2018). How Amazon's Latest Security Device Let People Spy on You, authored by Reed Albergotti, 11 May 2018.
- The Institute of Engineering and Technology. (2019). Response to DCMS, Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security.
- Tirado-Morueta, R., Aguaded-Gómez, J. I., & Hernando-Gómez, Á. (2018). The socio-demographic divide in Internet usage moderated by digital literacy support. Technology in Society, 55, 47-55.
- UK Computing Research Committee (UKCRC). (2019). Response to DCMS, Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security.
- Ullrich, J. B. (2014). More Device Malware: This is why your DVR attacked my Synology Disk Station (and now with Bitcoin Miner!). SANS ISC InfoSec Forums.
- Ullrich, J. B. (2016). The Short Life of a Vulnerable DVR Connected to the Internet. SANS ISC InfoSec Forums.

- Union for the Coordination of the Transmission of Energy (UCTE). (2004). Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy, UCTE Report, April 2004.
- United Nations General Assembly. (1948). Universal declaration of human rights. UN General Assembly.
- University College London (UCL). (2018). Tech Abuse: How internet-connected devices can affect victims of gender-based domestic and sexual violence and abuse.
- US National Institute for Standards and Technology (NIST). (2017). Digital Identity Guidelines, Authentication and Lifecycle Management, NIST Special Publication 800-63B, Computer Security.
- Varian, H. R. (2014). Big data: New tricks for econometrics. Journal of Economic Perspectives, 28(2), 3-28.
- Venkat. A. (2019). Wikipedia Investigates DDoS Attack. Bankinfosecurity.
- Verababyspot. (2020). Nest Cam Baby Monitor Review: Everything You Need to Know.
- VoiceLabs.co. (2017). The 2017 Voice Report: Executive Summary.
- Wallen, J. (2017). Most IoT devices are an attack waiting to happen, unless manufacturers update their kernels. Tech Republic.
- Wheeler, T., & Simpson, D. (2019). Why 5G requires new approaches to cyber security.
- Wilson, H. J., Shah, B., & Whipple, B. (2015) How People Are Actually Using the Internet of Things. Harvard Business Review.
- Winchcomb, T., Massey, S., & Beastall, P. (2017). Review of the Latest Developments in the Internet of Things. Cambridge Consultants.
- Wolfe, J. (2017). Roomba vacuum maker iRobot betting big on the 'smart' home. Reuters.
- Woodlock, D. (2017). "The Abuse of Technology in Domestic Violence and Stalking," Violence Against Women, vol. 23, no. 5, pp. 584-602.
- Xing, L. et al. (2014). Upgrading Your Android, Elevating My Malware: Privilege Escalation Through Mobile OS Updating. Indiana University Bloomington, and Microsoft Research.
- Yates, M. (2019). "Behavioral Surplus" Is Not Evil – It's Essential to Customer Experience. International Data Corporation (IDC).
- Young, A. (2020). How Do Wireless Security Cameras Work? Safewise.
- Zhao, M., Laszka, A., & Grossklags, J. (2017). 'Devising effective policies for bug-bounty platforms and security vulnerability discovery.' Journal of Information Policy 7: 372 –418.

Appendix B: Survey Data

Survey of business and other organisations

1. Please confirm that in addition to having read our privacy policy, you consent to your personal data being processed in accordance with GDPR. By selecting "yes", you also confirm that you are happy to proceed with the survey (participation in the survey is voluntary and you can change your mind at any time).

Answer Choices	Responses*	
Yes	100%	51
No	0%	0

**answered 51, skipped 0*[242]

2. Please tick the box that best describes your organisation:

Answer Choices	Responses*	
Consumer association	2%	1
Industry association	15%	7
Private sector organisation	64%	30
Research organisation	2%	1
Public authority	0%	0
Civil society organisations (e.g. NGO or charity)	2%	1
Consumer of IoT devices (individual)	0%	0
Other (please specify)	15%	7

** answered 47, skipped 4*

3. Which sector best describes your organisation's main activity?

Answer Choices	Responses*	
Agriculture, forestry and fishing	0%	0
Mining and quarrying	0%	0
Manufacturer	11%	5
Electricity, gas, steam and air conditioning supply	0%	0
Water supply; sewerage, waste management and remediation activities	0%	0
Construction	0%	0
Wholesale and retail trade; repair of motor vehicles and motorcycles	0%	0
Transportation and storage	5%	2
Accommodation and food service activities	0%	0
Information technology and communication	52%	23
Financial and insurance activities	5%	2
Real estate activities	0%	0
Professional, scientific and technical activities	9%	4
Administrative and support service activities	0%	0
Public administration and defence; compulsory social security	2%	1

[242] One respondent responded 'No' to Question 1. This respondent was taken directly to the end of the online survey without being asked any further questions. As such, this respondent has not been included in the sample size.

Answer Choices	Responses*	
Education	7%	3
Human health and social work activities	0%	0
Arts, entertainment and recreation	0%	0
Other (please specify)	9%	4

** answered 44, skipped 7*

4. What is the size of your organisation?

Answer Choices	Responses*	
Micro (less than 10 employees)	19%	7
Small (10-49 employees)	11%	4
Medium (between 50 and 249 employees)	11%	4
Large (250 or more employees)	58%	21
Not applicable	0%	0

** answered 36, skipped 15*

5. What is your organisation's relationship with consumer Internet of Things (IoT) devices? (Please select all that apply)

Answer Choices	Responses*	
Manufacturer of consumer IoT devices	22%	8
Component supplier for consumer IoT devices	17%	6
Importer/ distributor of consumer IoT devices	8%	3
Seller/ retailer of consumer IoT devices	19%	7
Reseller of consumer IoT devices (online or in-store)	6%	2
User of consumer IoT devices	28%	10
Don't know	6%	2
Not applicable	0%	0
Other (please specify)	42%	15

** answered 36, skipped 15*

6. Which of the following types of consumer IoT products does your organisation have an interest in? (Please select all that apply)

Answer Choices	Responses*	
Connected children's toys and baby monitors	31%	11
Connected safety-relevant products such as smoke detectors and door locks	0%	0
Smart TVs	39%	14
Wearable health trackers	39%	14
Smart home thermostats	36%	13
Smart lighting	42%	15
Smart security systems (e.g. smart doorbell and smart video camera, etc.)	42%	15
Connected domestic appliances (e.g. smart washing machines, smart fridges, etc.)	36%	13
Consumer tablets or laptops	47%	17

Answer Choices	Responses*	
Smart pet products (e.g. smart collars)	36%	13
Connected devices used in the personal home garden (but not industrial agriculture)	33%	12
Other devices which can connect to the Internet through Bluetooth or Internet-connected apps	69%	25
Smartphone	44%	16
Other (please specify)	31%	11

** answered 36, skipped 15*

7. In your opinion, how frequently do the following vulnerabilities occur in consumer IoT devices? Please rank each vulnerability.

	Never		Not very frequently		Neither frequently nor infrequently		Quite frequently		Very frequently		Don't know		Total	Weighted Average
Lack of authentication processes in the device	4%	1	9%	2	9%	2	35%	8	43%	10	0%	0	23	4.04
Lack of user awareness of cyber security	0%	0	0%	0	4%	1	17%	4	74%	17	4%	1	23	4.78
Default passwords that are not unique to the device	0%	0	4%	1	13%	3	39%	9	35%	8	9%	2	23	4.3
Lack of encryption of the device and communications to/from the device	4%	1	4%	1	9%	2	48%	11	26%	6	9%	2	23	4.13
Vulnerabilities in the software /firmware that are not addressed by security updates/ patches	4%	1	4%	1	22%	5	22%	5	43%	10	4%	1	23	4.09
Other (please specify) – *open-ended text box*													4	

** answered 23, skipped 28*

8. In your view, what is the likelihood of these vulnerabilities being exploited in consumer IoT devices? Please rank each vulnerability.

	Never		Not very likely		Neither unlikely nor likely		Quite likely		Very likely		Don't know		Total	Weighted Average
Lack of authentication processes in the device	0%	0	4%	1	4%	1	43%	10	48%	11	0%	0	23	4.35
Lack of user awareness of cyber security	0%	0	0%	0	4%	1	35%	8	61%	14	0%	0	23	4.57
Default passwords that are not unique to the device	0%	0	0%	0	4%	1	13%	3	83%	19	0%	0	23	4.78
Lack of encryption of the device and	0%	0	4%	1	17%	4	30%	7	48%	11	0%	0	23	4.22

	Never		Not very likely		Neither unlikely nor likely		Quite likely		Very likely		Don't know		Total	Weighted Average
communications to/from the device														
Vulnerabilities in the software/firmware that are not addressed by security updates/ patches	00%	0	4%	1	4%	1	39%	9	52%	12	0%	0	23	4.39
Other (please specify) – *open ended text box*													3	

**Answered 23, skipped 28*

9. In your view, how likely are the following impacts to occur as a result of a cyber security incident on a consumer IoT device?

	Never		Not very likely		Neither unlikely nor likely		Quite likely		Very likely		Don't know		Total	Weighted Average
Breaches to consumer privacy (e.g. unauthorised access to smart cameras/ speakers)	0%	0	4%	1	4%	1	35%	8	57%	13	0%	0	23	4.43
Financial loss to consumers	0%	0	13%	3	17%	4	43%	10	22%	5	4%	1	23	3.87
Loss of access to/ control of the device	0%	0	4%	1	13%	3	39%	9	39%	9	4%	1	23	4.26
Loss of personal/ customer data	0%	0	5%	1	9%	2	32%	7	55%	12	0%	0	22	4.36
Loss of commercially sensitive information	0%	0	9%	2	26%	6	39%	9	22%	5	4%	1	23	3.87
Physical damage to the device, consumer or other property	0%	0	35%	8	39%	9	13%	3	13%	3	0%	0	23	3.04
Reputational damage to the device manufacturer/ retailer	0%	0	0%	0	13%	3	26%	6	57%	13	4%	1	23	4.52
Loss of consumer confidence	0%	0	0%	0	4%	1	52%	12	39%	9	4%	1	23	4.43
Financial loss to the manufacturer/ retailer	0%	0	9%	2	17%	4	48%	11	22%	5	4%	1	23	3.96
Emotional distress to the consumer	0%	0	9%	2	13%	3	39%	9	35%	8	4%	1	23	4.13
Disruption to business activity as a result of an IoT cyber security incident (e.g. Distributed Denial of Service attack)	0%	0	4%	1	13%	3	39%	9	43%	10	0%	0	23	4.22
Disruption to the consumer's day-to-day activities	0%	0	13%	3	22%	5	43%	10	22%	5	0%	0	23	3.74

Other (please specify) – *open-ended text box*	2	

**Answered 23, skipped 28*

10. In your view, how damaging would the following impacts be to society as a whole (i.e. in terms of the size of impact, thinking about the economic cost and number of people affected)?

	Not damaging at all		Not very damaging		Neither not damaging nor damaging		Quite damaging		Very damaging		Don't know		Total	Weighted Average
Breaches to consumer privacy (e.g. unauthorised access to smart cameras/ speakers)	0%	0	5%	1	5%	1	64%	14	27%	6	0%	0	22	4.14
Financial loss to consumers	0%	0	4%	1	17%	4	52%	12	22%	5	4%	1	23	4.04
Loss of access to/ control of the device	0%	0	10%	2	14%	3	52%	11	24%	5	0%	0	21	3.9
Loss of personal/ customer data	0%	0	0%	0	5%	1	38%	8	57%	12	0%	0	21	4.52
Loss of commercially sensitive information	0%	0	9%	2	23%	5	27%	6	41%	9	0%	0	22	4
Physical damage to the device, consumer or other property	0%	0	14%	3	33%	7	19%	4	29%	6	5%	1	21	3.76
Reputational damage to the device manufacturer/ retailer	0%	0	9%	2	14%	3	32%	7	45%	10	0%	0	22	4.14
Loss of consumer confidence	0%	0	5%	1	9%	2	32%	7	55%	12	0%	0	22	4.36
Financial loss to the manufacturer/ retailer	0%	0	17%	4	9%	2	48%	11	26%	6	0%	0	23	3.83
Emotional distress to the consumer	0%	0	4%	1	22%	5	35%	8	35%	8	4%	1	23	4.13
Disruption to business activity as a result of an IoT cyber security incident (e.g. Distributed Denial of Service attack)	0%	0	0%	0	4%	1	52%	12	43%	10	0%	0	23	4.39
Disruption to the consumer's day-to-day activity	0%	0	9%	2	17%	4	52%	12	22%	5	0%	0	23	3.87
Other (please specify) – *open-ended text box*													2	

**Answered 23, skipped 28*

11. Where possible, please quantify and provide details of the following for your organisation:

Answer Choices	Responses	
The number of compromised consumer IoT devices in the UK:	90%	9
The cost on an annual basis, as a result of cyber security breaches in consumer IoT devices in the UK:	90%	9
The cost to the consumers of a cyber security incident on their consumer IoT devices per incident:	100%	10

**Answered 10, skipped 41*

12. Would your organisation face any of the following costs as a result of a consumer IoT breach?

	Yes		No		Not applicable		Don't know		Total	Weighted Average
Adding more security updates	43%	10	17%	4	30%	7	9%	2	23	2.04
Recalling the product	20%	4	20%	4	45%	9	15%	3	20	2.55
Reputational damage	52%	11	5%	1	33%	7	10%	2	21	2
Offering support to those affected	59%	13	14%	3	18%	4	9%	2	22	1.77
Issuing guidance	55%	11	15%	3	20%	4	10%	2	20	1.85
If possible, please quantify and explain this cost: – *open-ended text box*									20	

**Answered 23, skipped 28*

13. In the next 5-10 years, do you think that the number of cyber security incidents affecting consumer IoT devices in the UK will:

Answer Choices	Responses*	
Increase	100%	22
Decrease	0%	0
Stay the same	0%	0
Don't know	0%	0
Please explain your answer: – *open-ended text box*		13

**Answered 22, skipped 29*

14. In the next 5-10 years, what do you think will drive this change in the threat landscape to consumer IoT devices?

Open comment question.

Answered	**16**
Skipped	**35**

Box 1: Defining the three minimum security requirements

Minimum security requirements: The Government advocates a minimum baseline of security standards, consistent with aspects of the top three guidelines set out in the Code of Practice for Consumer IoT Security and ETSI EN 303 645, the first globally applicable standard on the cyber security of IoT. These are outlined below:

1. IoT device passwords must be unique and not resettable to any universal factory setting;

2. Manufacturers of IoT products shall provide a public point of contact as part of a vulnerability disclosure policy;

3. Manufacturers will explicitly state the minimum length of time for which the device will receive security updates.

15. To what extent would the three minimum security requirements for consumer IoT devices have an impact on different **age groups** within the UK? (See box 1 above)

	Not at all		To a small extent		To a moderate extent		To a great extent		Don't know		Total	Weighted Average
Under 18	10%	2	25%	5	15%	3	45%	9	5%	1	20	3.6
18 to 24	5%	1	20%	4	30%	6	40%	8	5%	1	20	3.65
25 to 34	0%	0	35%	7	15%	3	45%	9	5%	1	20	3.7
35 to 44	0%	0	35%	7	15%	3	45%	9	5%	1	20	3.7
45 to 64	0%	0	25%	5	30%	6	35%	7	10%	2	20	3.75
65 or older	11%	2	26%	5	16%	3	37%	7	11%	2	19	3.58
Please explain why: – *open-ended text box*											13	

**Answered 20 skipped 32*

16. To what extent would the three minimum security requirements for consumer IoT devices have an impact on different **gender groups** within the UK? (See box 1 above)

	Not at all		To a small extent		To a moderate extent		To a great extent		Don't know		Total	Weighted Average
Female	20%	4	10%	2	5.00%	1	35%	7	30%	6	20	4.1
Male	20%	4	10%	2	10.00%	2	35%	7	25%	5	20	3.95
Other	20%	3	6.67%	1	7%	1	33%	5	33%	5	15	4.2
Please explain why: – *open-ended text box*											8	

**Answered 20 skipped 32*

17. To what extent would the three minimum security requirements for consumer IoT devices have an impact on different household income groups within the UK? (See box 1 above)

	Not at all		To a small extent		To a moderate extent		To a great extent		Don't know		Total	Weighted Average
Below £25,000 per annum	5%	1	11%	2	11%	2	32%	6	42%	8	19	4.68
£25,000-£50,000 per annum	5%	1	11%	2	16%	3	26%	5	42%	8	19	4.58
£50,001-£75,000 per annum	5%	1	15%	3	20%	4	20%	4	40%	8	20	4.35
£75,001-£100,000 per annum	5%	1	15%	3	20%	4	20%	4	40%	8	20	4.35

	Not at all		To a small extent		To a moderate extent		To a great extent		Don't know		Total	Weighted Average
Above £100,000 per annum	10%	2	15%	3	20%	4	15%	3	40%	8	20	4.15
Please explain why: – *open-ended text box*											10	

**Answered 20, skipped 32*

18. What other impacts on users of consumer IoT devices do you foresee if the three minimum security requirements for consumer IoT devices are mandated?

Open comment question

Answered	**7**
Skipped	**45**

Survey of consumers

1. Please confirm that in addition to having read our privacy policy, you consent to your personal data being processed in accordance with GDPR. By selecting "yes", you also confirm that you are happy to proceed with the survey (participation in the survey is voluntary and you can change your mind at any time).

Answer Choices	Responses*	
Yes	100%	57
No	0%	0

** answered 57, skipped 0*[243]

2. What is your age?

Answer Choices	Responses	
18 to 24	10%	5
25 to 34	15%	7
35 to 44	10%	5
45 to 54	13%	6
55 to 64	17%	8
65 to 74	19%	9
75 or older	15%	7
Prefer not to say	2%	1

** answered 48, skipped 9*

3. What gender do you identify as?

Answer Choices	Responses	
Female	42%	20
Male	56%	27
Other (please specify)	0%	0
Prefer not to say	2%	1

[243] One respondent responded 'No' to Question 1. This respondent was taken directly to the end of the online survey without being asked any further questions. As such, this respondent has not been included in the sample size.

Other:	0%	0

** answered 48, skipped 9*

4. What is your annual household income?

Answer Choices	Responses	
Under £25,000 per annum	34%	16
Between £25,000-£50,000 per annum	21%	10
Between £50,001-£75,000 per annum	9%	4
Between £75,001-£100,000 per annum	11%	5
Over £100,000 per annum	2%	1
Prefer not to say	23%	11

** answered 47, skipped 10*

5. What is your ethnic group?

Answer Choices	Responses	
White (English / Welsh / Scottish / Northern Irish / British)	77%	36
White (Irish)	0%	0
White (Gypsy or Irish Traveller)	0%	0
White (Any other White background)	6%	3
Mixed/ Multiple ethnic groups (White and Black Caribbean)	0%	0
Mixed/ Multiple ethnic groups (White and Black African)	2%	1
Mixed/ Multiple ethnic groups (White and Asian)	0%	0
Mixed/ Multiple ethnic groups (Any other Mixed / Multiple ethnic background)	0%	0
Asian/ Asian British (Indian)	9%	4
Asian/ Asian British (Pakistani)	0%	0
Asian/ Asian British (Bangladeshi)	0%	0
Asian/ Asian British (Chinese)	0%	0
Asian/ Asian British (Any other Asian background)	0%	0
Black/ African/ Caribbean/ Black British (African)	2%	1
Black/ African/ Caribbean/ Black British (Caribbean)	0%	0
Black/ African/ Caribbean/ Black British (Any other Black/ African/ Caribbean background)	0%	0
Other ethnic group (Arab)	2%	1
Other ethnic group (Any other ethnic group)	0%	0
Prefer not to say	0%	0
Other:	2%	1

** answered 47, skipped 10*

6. What is the highest level of education you have completed?

Answer Choices	Responses	
Degree, or Degree equivalent, and above (e.g. undergraduate and postgraduate)	53%	25
Higher education below degree level	21%	10
A level or equivalent	4%	2
GCSEs or equivalent	17%	8

Answer Choices	Responses	
No qualification	2%	1
Other (please specify)	2%	1

** answered 41, skipped 10*

7. Do you, or anyone in your household, have any long-term illness, health problem or disability which limits yours/their daily activities or the work you/they can do?

Answer Choices	Responses	
Yes	29%	14
No	63%	30
Prefer not to say	8%	4

** answered 48, skipped 9*

If a respondent selected 'Yes' in response to Q7, they were asked questions 8-13 and not questions 14-18. Respondents that selected 'No' or 'Prefer not to say' to Q7 were taken directly to question 14.

8. What Internet of Things device(s) do you or members of your household currently own? Please select all that apply.

	You		Other members of your household		Total
Connected children's toys and baby monitors	0%	0	100%	1	1
Smart TVs	71%	5	57%	4	7
Wearable health trackers	75%	3	75%	3	4
Smart home thermostats	67%	2	67%	2	3
Smart lighting	100%	2	0%	0	2
Smart security systems (e.g. smart door bell and smart video camera, etc.)	100%	1	0%	0	1
Connected domestic appliances (e.g. smart washing machines, smart fridges, etc.)	50%	1	50%	1	2
Consumer tablets or laptops	100%	9	56%	5	9
Smart pet products (e.g. smart collars)	0%	0	0%	0	0
Connected devices used in the personal home garden (but not industrial agriculture)	100%	3	33%	1	3
Other devices which can connect to the Internet through Bluetooth or Internet-connected apps	100%	6	50%	3	6
Smartphone	100%	8	63%	5	8
Other (please specify) – *open-ended text box*					1

** answered 9, skipped 48*

9. How frequently do you use the following consumer Internet of Things devices?

	Never		A few times a month		A few times a week		Everyday		Don't know		N/A (I do not own this device)		Total	Weighted Average
Connected children's toys and baby monitors	50%	4	13%	1	0%	0	0%	0	0%	0	38%	3	8	3.88
Smart TVs	0%	0	0%	0	14%	1	86%	6	0%	0	0%	0	7	5.86

	Never		A few times a month		A few times a week		Everyday		Don't know		N/A (I do not own this device)		Total	Weighted Average
Wearable health trackers	17%	1	0%	0	0%	0	67%	4	0%	0	17%	1	6	5.5
Smart home thermostats	17%	1	0%	0	17%	1	17%	1	0%	0	50%	3	6	6
Smart lighting	14%	1	0%	0	0%	0	29%	2	14%	1	43%	3	7	6.29
Smart security systems (e.g. smart door bell and smart video camera, etc.)	17%	1	0%	0	0%	0	17%	1	0%	0	67%	4	6	6.5
Connected domestic appliances (e.g. smart washing machines, smart fridges, etc.)	25%	2	0%	0	13%	1	0%	0	13%	1	50%	4	8	5.75
Consumer tablets or laptops	0%	0	0%	0	11%	1	89%	8	0%	0	0%	0	9	5.89
Smart pet products (e.g. smart collars)	20%	1	0%	0	0%	0	0%	0	0%	0	80%	4	5	6.6
Connected devices used in the personal home garden (but not industrial agriculture)	33%	3	11%	1	0%	0	22%	2	0%	0	33%	3	9	4.67
Other devices which can connect to the Internet through Bluetooth or Internet-connected apps	0%	0	0%	0	0%	0	75%	6	0%	0	25%	2	8	6.5
Smartphone	0%	0	0%	0	0%	0	100%	8	0%	0	0%	0	8	6
Other (please specify) – *open-ended text box*													2	

** answered 9, skipped 48*

10. What do you, or others in your household, use consumer IoT devices for? (Please select all that apply)

	You		Other members in your household		Total
Monitoring health/fitness	75%	3	75%	3	4
Managing health conditions	67%	4	50%	3	6
Studying/education	100%	3	67%	2	3
To help move around the house	100%	1	100%	1	1
To help communicate/socialise	88%	7	63%	5	8
Accessing services online (e.g. booking appointments, getting prescriptions, paying bills, booking train tickets)	100%	8	50%	4	8
To help stay independent	100%	3	67%	2	3
For entertainment purposes	75%	6	63%	5	8
To manage things in the house (e.g. changing temperature, turning lights on/off)	80%	4	80%	4	5
To monitor the home (e.g. smart cameras, smart security, baby monitors)	100%	1	100%	1	1
Other (please specify) – *open-ended text box*					0

** answered 9, skipped 48*

11. To what extent has having access to consumer IoT devices helped you or other members of your household, with day-to-day activities in relation to any disability/illness?

	You		Other members of your household		Total
Not helped at all	100%	2	50%	1	2
Somewhat helped	0%	0	0%	0	0
Helped to some extent	100%	4	0%	0	4
Helped to a great extent	50%	1	50%	1	2
Don't know	100%	2	50%	1	2
Prefer not to say	0%	0	0%	0	0
Please explain your answer: – *open-ended text box*					0

** answered 9, skipped 48*

12. How has having access to a consumer IoT device impacted on the following aspects of your life:

	Negatively impacted		Positively impacted		No impact		Don't know		Total	Weighted Average
Your health/ fitness/ staying active	0%	0	11%	1	78%	7	11%	1	9	3
Your quality of life	0%	0	89%	8	0%	0	11%	1	9	2.22
Your access to services	11%	1	78%	7	11%	1	0%	0	9	2
Your education	0%	0	63%	5	38%	3	0%	0	8	2.38
Your ability to communicate/socialise	11%	1	67%	6	22%	2	0%	0	9	2.11
Your independence	0%	0	44%	4	44%	4	11%	1	9	2.67
Your mobility	0%	0	0%	0	89%	8	11%	1	9	3.11
Your leisure/ entertainment time	0%	0	78%	7	11%	1	11%	1	9	2.33
Facilitating your day-to-day activities	11%	1	78%	7	11%	1	0%	0	9	2

** answered 9, skipped 48*

13. How has having access to a consumer IoT device impacted on the following aspects, for other members of your household:

	Negatively impacted		Positively impacted		No impact		Don't know		Total	Weighted Average
Their health/ fitness/ staying active	11%	1	11%	1	22%	2	56%	5	9	3.22
Their quality of life	11%	1	44%	4	11%	1	33%	3	9	2.67
Their access to services	0%	0	67%	6	0%	0	33%	3	9	2.67
Their education	0%	0	38%	3	13%	1	50%	4	8	3.13
Their ability to communicate/socialise	11%	1	67%	6	0%	0	22%	2	9	2.33
Their independence	0%	0	67%	6	11%	1	22%	2	9	2.56
Their mobility	11%	1	0%	0	67%	6	22%	2	9	3
Their leisure/ entertainment time	0%	0	75%	6	0%	0	25%	2	8	2.5
Facilitating their day-to-day activities	0%	0	75%	6	13%	1	13%	1	8	2.38

** answered 9, skipped 48*

Respondents that selected 'No' or 'Prefer not to say' to Q7 were not asked questions 8-13. They were taken directly to Q14. Respondents that selected 'Yes' to Q7 were not asked questions 14-18. From Q13, they were taken directly to Q19.

14. What Internet of Things device(s) do you, or other members of your household, currently own? Please select all that apply.

	You		Other members of your household		Total
Connected children's toys and baby monitors	67%	4	50%	3	6
Smart TVs	93%	13	36%	5	14
Wearable health trackers	100%	9	22%	2	9
Smart home thermostats	83%	5	50%	3	6
Smart lighting	88%	7	25%	2	8
Smart security systems (e.g. smart door bell and smart video camera, etc.)	83%	5	33%	2	6
Connected domestic appliances (e.g. smart washing machines, smart fridges, etc.)	83%	5	17%	1	6
Consumer tablets or laptops	100%	25	32%	8	25
Smart pet products (e.g. smart collars)	0%	0	100%	1	1
Connected devices used in the personal home garden (but not industrial agriculture)	83%	5	50%	3	6
Other devices which can connect to the Internet through Bluetooth or internet-connected apps	100%	21	33%	7	21
Smartphone	100%	25	40%	10	25

** answered 28, skipped 29*

15. How frequently do you use the following consumer IoT devices?

	Never		A few times a month		A few times a week		Everyday		Don't know		N/A (I do not own this device)		Total	Weighted Average
Connected children's toys and baby monitors	5%	1	5%	1	0%	0	15%	3	5%	1	70%	14	20	7.05
Smart TVs	9%	2	0%	0	5%	1	45%	10	0%	0	41%	9	22	6.32
Wearable health trackers	14%	3	0%	0	0%	0	41%	9	0%	0	45%	10	22	6.23
Smart home thermostats	14%	3	5%	1	0%	0	24%	5	0%	0	57%	12	21	6.29
Smart lighting	10%	2	0%	0	0%	0	30%	6	5%	1	55%	11	20	6.65
Smart security systems (e.g. smart door bell and smart video camera, etc.)	21%	4	0%	0	0%	0	16%	3	0%	0	63%	12	19	6.21
Connected domestic appliances (e.g. smart washing machines, smart fridges, etc.)	14%	3	5%	1	5%	1	5%	1	0%	0	71%	15	21	6.52
Consumer tablets or laptops	4%	1	4%	1	0%	0	82%	23	7%	2	4%	1	28	5.86
Smart pet products (e.g. smart collars)	15%	3	0%	0	0%	0	5%	1	0%	0	80%	16	20	6.85
Connected devices used in the personal home garden (but not industrial agriculture)	5%	1	14%	3	5%	1	5%	1	0%	0	71%	15	21	6.71
Other devices which can connect to the Internet through Bluetooth or internet-connected apps	4%	1	19%	5	15%	4	46%	12	0%	0	15%	4	26	5.38

	Never		A few times a month		A few times a week		Everyday		Don't know		N/A (I do not own this device)		Total	Weighted Average
Smartphone	4%	1	0%	0	4%	1	88%	22	0%	0	4%	1	25	5.84
)ther (please specify) – *open-ended text box*													0	

** answered 28, skipped 29*

16. What do you, or others in your household, use consumer IoT devices for? Please select all that apply.

Answer Choices	Responses	
Monitoring your health/fitness	39%	11
Managing health conditions	11%	3
Studying/education	36%	10
To help move around the house	4%	1
To help communicate/socialise	68%	19
Accessing services online (e.g. booking appointments, getting prescriptions, paying bills, booking train tickets)	68%	19
To help stay independent	25%	7
To entertain yourself	82%	23
To manage things in the house (e.g. changing temperature, turning lights on/off)	25%	7
To monitor the home (e.g. smart cameras, smart security, baby monitors)	18%	5
Other (please specify) – *open-ended text box*	4%	1

** answered 28, skipped 29*

17. How has having access to a consumer IoT device impacted on the following aspects of your life:

	Negatively impacted		Positively impacted		No impact		Don't know		Total	Weighted Average
Your health/ fitness/ staying active	0%	0	50%	12	42%	10	8%	2	24	2.58
Your quality of life	0%	0	67%	16	21%	5	13%	3	24	2.46
Your access to services	0%	0	70%	16	26%	6	4%	1	23	2.35
Your education	0%	0	59%	13	36%	8	5%	1	22	2.45
Your ability to communicate/socialise	0%	0	79%	19	17%	4	4%	1	24	2.25
Your independence	0%	0	41%	9	50%	11	9%	2	22	2.68
Your mobility	5%	1	27%	6	50%	11	18%	4	22	2.82
Your leisure/ entertainment time	0%	0	83%	20	13%	3	4%	1	24	2.21
Facilitating your day-to-day activities	0%	0	70%	16	26%	6	4%	1	23	2.35

** answered 27, skipped 29*

18. How has having access to a consumer IoT device impacted on the following aspects, for other members of your household:

	Negatively impacted		Positively impacted		No impact		Don't know		Total	Weighted Average
Their health/ fitness/ staying active	0%	0	23%	5	45%	10	32%	7	22	3.09

Their quality of life	0%	0	48%	10	29%	6	24%	5	21	2.76
Their access to services	0%	0	43%	9	24%	5	33%	7	21	2.9
Their education	0%	0	38%	8	29%	6	33%	7	21	2.95
Their ability to communicate/socialise	0%	0	62%	13	14%	3	24%	5	21	2.62
Their independence	5%	1	14%	3	43%	9	38%	8	21	3.14
Their mobility	0%	0	5%	1	50%	10	45%	9	20	3.4
Their leisure/ entertainment time	0%	0	52%	11	24%	5	24%	5	21	2.71
Facilitating their day-to-day activities	0%	0	29%	6	43%	9	29%	6	21	3

** answered 23, skipped 34*

Selective questioning, as determined by Q7, no longer applies. The following questions were asked to all respondents.

19. To what extent do you trust the security of your consumer IoT device(s)?

Answer Choices	Responses	
Not at all	11%	4
To a small extent	31%	11
To some extent	37%	13
To a great extent	17%	6
Don't know	3%	1
Please explain your answer: – *open-ended text box*		22

** answered 35, skipped 22*

20. What features do you take into account while buying a consumer IoT device(s)? Please indicate the importance of each of the features listed below.

	1 (Not important at all)		2 (Slightly important)		3 (Moderately important)		4 (Very important)		5 (Extremely important)		Don't know		Total	Weighted Average
Price	0%	0	9%	3	47%	16	29%	10	15%	5	0%	0	34	3.5
Security features	0%	0	6%	2	27%	9	33%	11	27%	9	6%	2	33	4
Brand	12%	4	18%	6	41%	14	21%	7	9%	3	0%	0	34	2.97
Durability of device	0%	0	11%	4	26%	9	37%	13	26%	9	0%	0	35	3.77
Functionality	0%	0	0%	0	11%	4	51%	18	37%	13	0%	0	35	4.26
Ease of connectivity (e.g. pairing with existing devices)	3%	1	9%	3	26%	9	38%	13	18%	6	6%	2	34	3.76

** answered 35, skipped 22*

21. Are there any other features you would take into account while buying a consumer IoT device?

Open comment question

Answered	**12**
Skipped	**45**

22. How much more would you consider spending on 'big ticket' consumer IoT devices in exchange for greater security features? (e.g. Smart TVs, smart domestic appliances, smart boilers, etc.) Respondents were asked to select a number on a sliding scale from £0-£500

Answer Choices	Average Number	Total Number	Responses	
Scale from £0-£500	133.375	4268	100.00%	32

** answered 32, skipped 25*

23. How much more would you consider spending on 'connecting the home' consumer IoT devices for greater security features? (e.g. home assistants, smart speakers, smart lighting, smart doorbell, etc.) Respondents were asked to select a number on a sliding scale from £0-£500

Answer Choices	Average Number	Total Number	Responses	
Scale from £0-£500	118.8064516	3683	100.00%	31

** answered 31, skipped 26*

24. How much more would you consider spending on 'consumer lifestyle' consumer IoT devices for greater security features? (e.g. Smart handheld devices, smart watches, smart phones, smart toys etc.) Respondents were asked to select a number on a sliding scale from £0-£500

Answer Choices	Average Number	Total Number	Responses	
Scale from £0-£500	123.4333333	3703	100.00%	30

** answered 30, skipped 27*

Supplementary table for Qs 22-24.

Responses (£)	Big ticket – Q22		Connecting the home – Q23		Consumer lifestyle – Q24	
0	2	6%	5	16%	2	7%
1-49	10	31%	11	35%	13	43%
50-99	7	22%	5	16%	4	13%
100-149	3	9%	1	3%	3	10%
150-199	2	6%	1	3%	1	3%
200-249	2	6%	4	13%	2	7%
250-299	2	6%	0	0%	1	3%
300-349	0	0%	0	0%	0	0%
350-399	0	0%	0	0%	0	0%
400-449	0	0%	0	0%	0	0%
450-500	4	13%	4	13%	4	13%
Total	32	100%	31	100%	30	100%

25. If you would not consider spending more on consumer IoT devices, what would you do instead? Please select all that apply.

Answer Choices	Responses	
Buy a non-Internet connected version of the same device	38%	12
Buy a cheaper IoT device with fewer or no security features	13%	4
Not buy the device at all	38%	12

Don't know	28%	9
Not applicable	19%	6
Other (please specify)	3%	1

** answered 32, skipped 25*

26. Have you experienced any of the following cyber security issues with any of your consumer IoT devices? Please select all that apply.

Answer Choices	Responses	
Unauthorised access to your consumer IoT device	3%	1
Your consumer IoT device becoming infected with a virus, ransomware or malware	11%	4
Unauthorised access to your home network through your consumer IoT device	3%	1
I received a security warning or notification from the IoT device	23%	8
I have not experienced any cyber security issues with any of my consumer IoT devices that I am aware of	74%	26
Any other cyber security issues (please explain):	0%	0

** answered 35, skipped 22*

Respondents that selected the option 'I have not experienced any cyber security issues with any of my consumer IoT devices that I am aware of' in response to Q26 were not asked questions 27-33.

27. Which of your consumer IoT device(s) were affected? Please select all that apply.

Answer Choices	Responses	
Connected children's toys and baby monitors	0%	0
Smart TVs	14%	1
Wearable health trackers	0%	0
Smart home thermostats	14%	1
Smart lighting	0%	0
Smart security systems (e.g. smart door bell and smart video camera, etc.)	0%	0
Connected domestic appliances (e.g. smart washing machines, smart fridges, etc.)	0%	0
Consumer tablets or laptops	71%	5
Smart pet products (e.g. smart collars)	0%	0
Connected devices used in the personal home garden (but not industrial agriculture)	0%	0
Other devices which can connect to the Internet through Bluetooth or internet-connected apps	14%	1
Smartphone	14%	1
Other (please specify) – *open-ended text box*	0%	0

** answered 7, skipped 50*

28. Did you experience any of these issues happening to the same device more than once?

Answer Choices	Responses	
Yes	0%	0
No	71%	5
Not sure	29%	2
Please specify which one(s): – *open-ended text box*	0%	0

** answered 7, skipped 50*

29. Please select one consumer IoT device that caused you the most concern as a result of a cyber security issue:

Answer Choices	Responses	
Connected children's toys and baby monitors	0%	0
Smart TVs	0%	0
Wearable health trackers	17%	1
Smart home thermostats	0%	0
Smart lighting	0%	0
Smart security systems (e.g. smart door bell and smart video camera, etc.)	0%	0
Connected domestic appliances (e.g. smart washing machines, smart fridges, etc.)	0%	0
Consumer tablets or laptops	67%	4
Smart pet products (e.g. smart collars)	0%	0
Connected devices used in the personal home garden (but not industrial agriculture)	0%	0
Other devices which can connect to the Internet through Bluetooth or internet-connected apps	0%	0
Smartphone	17%	1
Please explain what happened with your device: – *open-ended text box*		4

** answered 6, skipped 51*

30. What action(s) did you take to deal with the issue for that particular device? Please select all that apply for the consumer IoT device that you said caused you the most concern as a result of a cyber security issue.

Answer Choices	Responses	
No action taken	0%	0
Asked friends or family for advice	0%	0
Changed/ reset your password	71%	5
Disconnected device from the Internet	0%	0
Reset device to factory settings	14%	1
Installed security updates	14%	1
Contacted device manufacturer (i.e. consumer service)	14%	1
Contacted the retailer	0%	0
Stopped using the device but not thrown it away	0%	0
Returned the device to the store where it was purchased	0%	0
Took the device to a repair shop	14%	1
Gave the IoT device to friends/ family	0%	0
Gave the IoT device to charity or other non-profit	0%	0
Sold the device on	0%	0
Contacted the police/ victim support service (i.e. Action Fraud)	0%	0
Discarded the device	0%	0
Destroyed the device	0%	0
Other (please specify) – *open-ended text box*	14%	1

** answered 7, skipped 50*

31. How confident were you that the action that you had taken had resolved the issue for that particular device?

Answer Choices	Responses	
Not confident at all	0%	0
Confident to some extent	57%	4
Very confident	29%	2
Don't know	0%	0
Not applicable	14%	1
Please explain your answer: – *open-ended text box*		2

** answered 7, skipped 50*

32. Which of the following impacts did you experience as a result of the cyber security issue? Please select all that apply.

Answer Choices	Responses	
Financial loss (i.e. costs were incurred as a result of the incident, such as hacking or attempted hacking of online bank accounts)	0%	0
Identity theft	0%	0
Disruption of other IoT devices	0%	0
Loss of personal data	0%	0
Disrupted access to your home network	17%	1
Invasion of privacy (e.g. unauthorised access to smart cameras or smart speakers)	0%	0
Emotional distress	17%	1
Physical harm	0%	0
Affected the functionality of your device	50%	3
Affected your independence/ ability to complete daily tasks	0%	0
Time lost to resolving the issue	50%	3
Loss of trust in the brand/ IoT device/ device retailer	33%	2
Lost access to my IoT device	17%	1
Physical damage to the device/other property	0%	0
Other (please specify): – *open-ended text box*	0%	0

** answered 6, skipped 51*

33. Based on your experience of a cyber security issue on your consumer IoT device(s), please indicate the extent to which you agree with the following statements:

	Strongly disagree		Disagree		Neither agree nor disagree		Agree		Strongly agree		Total	Weighted Average
The experience did not change my attitude to securing my device	0%	0	29%	2	29%	2	29%	2	14%	1	7	3.29
I am more aware of the security of my consumer IoT device	0%	0	0%	0	29%	2	57%	4	14%	1	7	3.86
I now check the IoT security features before I buy a product	0%	0	0%	0	29%	2	57%	4	14%	1	7	3.86
I do not buy IoT devices anymore	67%	4	0%	0	33%	2	0%	0	0%	0	6	1.67

	Strongly disagree		Disagree		Neither agree nor disagree		Agree		Strongly agree		Total	Weighted Average
I have taken steps to improve the security of my IoT device	0%	0	0%	0	17%	1	67%	4	17%	1	6	4
I am less trusting of consumer IoT devices	17%	1	50%	3	17%	1	17%	1	0%	0	6	2.33
Please explain the reasons for your answer: – *open-ended text box*											1	

** answered 7, skipped 50*

Selective questioning, as determined by Q26, no longer applies. Q34 was asked to all respondents.

34. Please use this space to share any other comments or insights about your use of consumer IoT devices:

Open comment question

Answered	**5**
Skipped	**52**

Appendix C: Case Studies

Case study 1: Consumer IoT-facilitated abuse

'Technology-facilitated abuse' describes the exploitation of technology to harass, stalk, control or otherwise abuse.[244] As the prevalence of "smart" devices has increased in recent years, the cases of abuse facilitated by these consumer IoT devices has also risen.[245] To illustrate, awareness of the use of consumer IoT devices for stalking and domestic abuse has risen to the extent that a team of UCL researchers are conducting research into the evolving IoT privacy and security risks in the context of domestic violence and abuse.[246] This research group noted in 2018 that the use of IoT devices in the context of technology-facilitated abuse have 'been barely explored'[247]. In this context, this case study combines a real-life example of vulnerability exploitation of a smart doorbell whilst illustrating the wider potential impacts.[248]

The attack: Vulnerability, exploitation and mitigation

In January 2018, the owner of a smart doorbell found out that his ex-partner had been accessing and downloading video from his smart doorbell to monitor the targeted individual through an app linked to the doorbell.

The **vulnerability exploited in this instance relates to how the manufacturer of the smart doorbell managed password changes and authentication of users**. If someone had previously been legitimately or illegitimately logged into the account linked to the smart doorbell via a smartphone, it was not possible for the owner to terminate that login session by taking reasonable steps. In this incident, for example, the targeted individual changed the account password related to his smart doorbell twice, as well as his Wi-Fi key[249], but the attacker was still able to access the account related to the smart doorbell via an app on his smartphone. This was possible because the password change function did not require re-authentication of all devices connected to the account, thus highlighting a flaw in password policy.

Following notification of the vulnerability to the manufacturer, the attacker's access was immediately revoked, and the target was given a new doorbell. Furthermore, the smart doorbell was reportedly updated to ensure that any password changes require new authentication from all devices. However, even following this fix, it was reported that the app did not remove authentication for all devices and require new logins immediately. Instead, it took an hour following the password change, which is considered 'not a security best practice'[250].

[244] Woodlock, D. (2017). "The Abuse of Technology in Domestic Violence and Stalking," Violence Against Women, vol. 23, no. 5, pp. 584-602.
[245] Tanczer, L., Lopez Neira, I., Parkin, S., Patel, T. and Danezis, G. (2018). Gender and IoT Research Report: The rise of the Internet of Things and implications for technology-facilitated abuse.
[246] University College London (UCL) webpage, Gender and IoT. The team comprises researchers from University College London's (UCL) Departments for Science, Technology, Engineering and Public Policy (STEaPP) and Computer Science and is supported by London VAWG Consortium, Privacy International and the PETRAS IoT Research Hub.
[247] Tanczer, L., Lopez Neira, I., Parkin, S., Patel, T. and Danezis, G. (2018). Gender and IoT Research Report: The rise of the Internet of Things and implications for technology-facilitated abuse.
[248] The Information. (2018). How Amazon's Latest Security Device Let People Spy on You, authored by Reed Albergotti, 11 May 2018.
[249] PenTestPartners. (2018). Blog: Internet of Things, Breaking up is hard to do… with IoT, authored by Ken Munro, 6 July 2018.
[250] The Information. (2018). How Amazon's Latest Security Device Let People Spy on You, authored by Reed Albergotti, 11 May 2018.

In terms of best practice, the Digital Identity Guidelines[251] published by the US National Institute of Standards and Technology (NIST) recommend, for example, the following should be built into the authentication approach of product developers:

- 'Verifiers SHALL force a change [of authenticator, e.g. a password] if there is evidence of compromise of the authenticator'.
- If an authenticator is lost, the user 'SHALL repeat the identity proofing process'.
- 'Periodic reauthentication of [login] sessions SHALL be performed to confirm the continued presence of the [user]'.

Although this attack and the vulnerability exploited does not link directly to one of the Code of Practice guidelines, it does illustrate the importance of a secure approach to authentication and password policy. This is the same goal the first guideline (no default passwords) is working towards.[252]

The impact

Through this unauthorised access, the attacker was able to view and download video from the doorbell to track the owner's movements. It was also found that, on multiple occasions, the attacker rang the doorbell remotely via the app in the middle of the night with the intention of disturbing the target.[253] The impacts related to this attack, as well as similar targeted attacks, are likely to only affect an individual or household.

Such attacks could have significant implications for the targeted individuals[254], including:

- **Privacy risks:** e.g. monitoring movements, being watched or listened to through cameras and microphones installed in devices etc.;
- **Loss of control of device** (e.g. an attacker could remove authentication of legitimate users to prevent access, or conduct anti-social behaviours, such as ringing the doorbell in the middle of the night); and
- **Risk of theft** (e.g. an attacker could utilise the smart doorbell to intercept deliveries to the property or monitor when the property is empty before attempting to gain access).

Beyond smart doorbells and door locks, media outlets have reported on the use of a wide range of consumer IoT devices for domestic abuse and stalking (including smart home assistants, smart thermostats, smart watches, webcams, smart TVs, fitness trackers, smart lighting and more).[255]

[251] US National Institute for Standards and Technology (NIST). (2017). Digital Identity Guidelines, Authentication and Lifecycle Management, NIST Special Publication 800-63B, Computer Security.
[252] Department for Digital, Culture, Media & Sport (DCMS). (2018). Code of Practice for Consumer IoT Security.
[253] The Information. (2018). How Amazon's Latest Security Device Let People Spy on You, authored by Reed Albergotti, 11 May 2018.
[254] University College London (UCL). (2018). Tech Abuse: How internet-connected devices can affect victims of gender-based domestic and sexual violence and abuse.
[255] See, for example: Evening Standard. (2018). Abusive partners use home technology to stalk and abuse women, study shows; The New York Times. (2018). Thermostats, Locks and Lights: Digital Tools of Domestic Abuse; The Times. (2018). Husband used smart-home device to spy on wife.

Case study 2: Connected Security Cameras and DVRs

Security cameras are a necessary tool for monitoring and surveillance, whether it is on personal (such as a home or on-site storage facility) or public property (such as hospitals, highways, libraries, etc.) In the past, video feeds would be transmitted via cables to a DVR (digital video recorder), and viewers could then watch the footage on a computer or monitor. DVRs are responsible for the compression, storage and streaming of any recorded footage from one to several cameras.[256] Innovations in the manufacture and programming of these devices has allowed them to be completely wireless, relying instead on Wi-Fi to transmit video and audio feeds to a receiver, which connects to a user's computer or smartphone.[257] While this provides users with a simpler set-up, both in the home and public spaces where there may be a network of cameras, the fact that these devices transmit signals via an Internet connection opens them up to a range of cyber security risks.

The Attack: Vulnerability, Exploitation and Mitigation

In 2017, a scanning attack used a type of malware to crack the default passwords on a multitude of security cameras and DVRs that were connected to public Wi-Fi networks. This was accomplished in two ways.

First, the backdoor on older versions of this specific company's IP cameras allowed anyone to send specific commands to these devices to obtain full administrative access. From there, they could set their own usernames and passwords, and control the device. The fact that this could be achieved remotely demonstrated how it required a low skill level to exploit these cameras, exposing just how vulnerable they were. The company denied it "would intentionally contribute to the placement of 'backdoors' in its products".[258] However, in later public statements, the company declared this access was a test code that the camera programmers forgot to remove from the devices.[259]

Second, DVRs were also prone to attacks. Attackers only needed to guess a very simple default username and password on any Internet-connected DVR device, and enter it in an online portal. Essentially, 'this attack can target devices that are behind a firewall, as long as they have basic remote access enabled.' The set credentials were "admin/12345", which is too simple and therefore very easy to guess.[260]

The first guideline of the UK's Code of Practice for Consumer IoT Security — No Default Passwords — states that "all IoT device passwords shall be unique and not resettable to any universal factory default value."[261] "Unique" in this case refers to an individual authenticator that is difficult to guess. At the manufacturer and retailer level, users could be provided with guides on how to create and change their passwords, thereby restoring some user autonomy when using emerging technology. The NCSC's guide to setting passwords provides some key suggestions on how to create a strong password.

- **Length:** Passwords should not be too short, as they "yield to brute force attacks as well as to dictionary attacks using words and commonly chosen passwords", but also not so long that they are difficult for users to remember.[262,263]

[256] Security Camera King. (2009). How does a security camera system work?
[257] Young, A. (2020). How Do Wireless Security Cameras Work? Safewise.
[258] Karas, B. (2017). Hikvision Backdoor Confirmed. IPVM.
[259] Le@rn CCTV. (n.d.). How to hack Hikvision camera (the easy way).
[260] Le@rn CCTV. (n.d.). How to hack Hikvision camera (the easy way).
[261] Department for Digital, Culture, Media & Sport (DCMS). (2018). Code of Practice for Consumer IoT Security.
[262] NIST. (2017). NIST Special Publication 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management. NIST.
[263] National Cyber Security Centre (NCSC). (2016). Password Guidance: Simplifying Your Approach.

- **Complexity:** While a randomly-generated password may be inherently complex, a user-generated password should be a series of letters, numbers and symbols. However, a highly complex password is less likely to be memorable, and "it is more likely that they will be written down or stored electronically in an unsafe manner".[264,265]

Although the company has since remedied these vulnerabilities and introduced password changing guidance in their user manuals,[266] other smart security camera companies may not be as vigilant. This is especially concerning when one of the key IoT device types compromised in the Mirai botnet DDoS attack were security cameras. This attack used the 61 most common default username/password combinations to access IoT devices.[267] Since CCTV and security cameras were often placed in elevated, inaccessible locations, addressing the vulnerability was difficult. In addition, owners of older devices have been urged to update the security software or upgrade altogether.[268]

Impacts

The most vulnerable groups in this sort of attack are the device users and members of the general public who are being surveyed and recorded. According to an IPVM report on this vulnerability, "millions of cameras have these vulnerabilities given the company's own regular declarations of shipping tens of millions of cameras."[269] CISA, a department within the US Department of Homeland Security, cites "escalating privileges or assuming the identity of an authenticated user and obtaining sensitive data" as primary impacts.[270] Possible secondary consequences of a security camera hack include unauthorised viewing and manipulation of footage to target specific individuals, or shutting them down to leave facilities prone to intrusions and burglaries.

Or, as exhibited by the 2016 Mirai DDoS attack, amassing an army of connected cameras by simply guessing the default log-in credentials can lead to a shut-down of Internet access to a significant geographical region.[271]While it directly impacts users' privacy and security by obtaining access to any data stored on the videos themselves, each exploited DVR or camera also becomes a gateway for a virus to attack other devices in the network. Once access is granted, all the data stored on the home network, from any number of devices, is accessible to attackers.[272] For cameras and DVRs installed in public facilities, this is even more problematic given the quantity of people and devices that pass through each day.

[264] NIST. (2017). NIST Special Publication 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management. NIST.
[265] National Cyber Security Centre (NCSC). (2016). Password Guidance: Simplifying Your Approach.
[266] Hikvision. (n.d.). Network Traffic Camera User Manual. Hikvision.
[267] Fruhlinger, J. (2018). The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the Internet. CSO UK.
[268] Karas, B. (2017). Hikvision Backdoor Confirmed. IPVM.
[269] Karas, B. (2017). Hikvision Backdoor Confirmed. IPVM.
[270] The Cybersecurity and Infrastructure Security Agency (CISA). (2017). ICS Advisory (ICSA-17-124-01): Hikvision Cameras. CISA.
[271] Newman, L. H. (2016). What We Know About Friday's Massive East Coast Internet Outage. Wired.
[272] Winchcomb, T., Massey, S., & Beastall, P. (2017). Review of the Latest Developments in the Internet of Things. Cambridge Consultants.

Case study 3: Operating System software updates

The Attack: Vulnerability, Exploitation and Mitigation

One of the primary vulnerabilities shared among consumer IoT devices is age. The older a device, the less likely it is to be supported by advanced software updates, and the more likely it is to lack the key security provisions that newer models may have. Furthermore, if there is a malicious app on a device of any age that has established a set of privileges (such as access permissions and settings adjustments), and the device upgrades its operating system, the privileges will be escalated.[273] Users may not realise their device contains a virus or harmful application that is accessing their data, and simply ascribe any malfunctions to the device's age.

The third security guideline— IoT producers should state "the minimum length of time for which a device will receive software updates and the reasons for the length of the support period"—would, at the very least, keep device users informed of when their device is no longer as secure as it was upon date of purchase.[274] According to Google data, 42% of worldwide users of Android OS are using a version with no security patches issued in 2019.[275] Moreover, this version had the highest percentage of devices with at least one Potentially Harmful Application (PHA) installed.[276] By keeping users notified of when their device will no longer receive the latest security updates, they can make more informed purchases.

That being said, on the OS provider's website, it appears this information is disclosed: "phones will receive at least two years of OS upgrades".[277] However, this specific platform is for higher-end devices. Although there are pre-installed apps from the device's service provider on each version of this OS, in cases where an app depends on the device's hardware—such as the camera—updates do not come directly from the provider, but rather from device manufacturers themselves. In other words, updates to these apps and the OS as a whole will depend on the manufacturer, their quality assurance and their transparency with consumers about the frequency of security and overall OS updates.[278]

Impacts

This is certainly among the more widespread vulnerabilities in terms of its potential impact. Those directly affected include individual device owners (mainly handheld devices and wearables). Meanwhile, manufacturers may be indirectly impacted if consumers demand security update information, or no longer trust them due to their device being hacked or not having sufficient security information provided in their user manuals.

Certain demographic groups may be more prone to exploitation than others. As mentioned in section 4.1.1., some countries have a higher percentage of users who are running on this older OS or earlier; most notably, developing countries tend to present this trend compared to higher income nations such as the UK.[279] Given cyber attacks are not restricted by national barriers, geographical differences must be considered alongside social factors. The variation of socioeconomic status among users in different regions could affect their ability to access newer, more secure devices that still receive security updates.

[273] Xing, L. et al. (2014). Upgrading Your Android, Elevating My Malware: Privilege Escalation Through Mobile OS Updating. Indiana University Bloomington, and Microsoft Research.
[274] Department for Digital, Culture, Media & Sport (DCMS). (2018). Code of Practice for Consumer IoT Security.
[275] BBC. (2020). One billion Android devices at risk of hacking. BBC.
[276] Google. (2019). Transparency Report: Android ecosystem security.
[277] Android. (n.d.). Android One. Android.
[278] Rayner, T. & Sims, G. (2019). Stock Android vs. Android One vs. Android Go. Android Authority.
[279] DeviceAtlas. (2019). Blog: Mobile OS versions by country.

Cost is a key factor here; although a newer version of this OS explicitly states the frequency of device updates, this does not necessarily mean lower-end products carry this guarantee as well. Consumers who are unable to afford the latest versions of smartphones, even if these do contain key security provisions, will hang on to their older devices much longer. Similarly, if a device owner is not as educated about the necessary security information to look out for, they may not make informed purchases and accept a device with an older OS.

Manufacturers should therefore always disclose the minimum period of time in which the device will continue to receive updates, urge consumers to make note of that end date, and provide them with a list of actions to take when this period ends. For those who may not fully comprehend the technical details around the security updates, "the need for each update should be made clear to consumers and an update should be easy to implement."[280]

[280] Department for Digital, Culture, Media & Sport (DCMS). (2018). Code of Practice for Consumer IoT Security.

Case study 4: Hacked Baby Monitor and Camera

The case study focuses on a baby monitor that is produced by an American tech company, which manufactures smart home appliances, which also produces smart thermostats, smoke detectors and security systems. The company is well regarded in the market because its products are reported as being compact, quiet and quick to install.[281] Beyond its camera providing a video-link to what it is filming, the camera in the baby monitor detects sounds and movements within a room and can further be used to monitor room temperature and humidity. Moreover, the camera in the baby monitor can act as a two-way sound transfer, where people on both ends can communicate.

The Attack: Vulnerability, Exploitation and Mitigation

Digital passwords have become an intrinsic part of everyday life, as an increasing number of devices, services or other functionalities require the use and encryption of a digital password. This is true for objects, such as baby monitors, whose secure features might be overlooked, and are difficult to patch, but who are integral part of consumers' daily lives.[282] Moreover, these devices are increasingly being connected and run through the Internet. These developments ensure that connected devices are increasingly more prone to being hacked by external actors, to which the baby monitor discussed in this case study is not an exception.[283] When queried about an attack to one of its devices, the manufacturer responded by saying that such attacks were possible when customers used passwords that were previously leaked due to a data breach.

In this case study, the attacker was able to use the two-way sound transfer mechanism of the device to send threatening voice messages to parents. The hacker exploited the vulnerability further to gain access to the camera, which gave them a view inside the victim's home. In order to prevent this, the manufacturer advised customers to change their factory default passwords and report back whenever they observe any suspicious behaviour.[284] This demonstrates that some IoT products are still being brought to market with default passwords, which could have been the vulnerability responsible for the attack.

In order to remedy this and prevent similar attacks in the future, the UK's Code of Practice for Consumer IoT Security – in its 'No Default Passwords' recommendation – states that 'all IoT device passwords shall be unique and not resettable to any universal factory default value'.[285] A unique password makes it more difficult for attackers to guess and prevents them from gaining access to multiple devices using the same login credentials.

Impacts

The main victim in this type of attack were the members of the household that is directly targeted. Impacts include emotional distress, violation of privacy and access to personal information. A ramification of this form of attacks could be that users stop using the features that allow them to access the cameras of their devices remotely, as having this feature enabled in devices facilitates attacks.[286]

Attacks of this type, however, also expose the manufacturers of the device to public scrutiny. Consequences for manufacturers might include the exposure to legal liabilities, as was the case with the US Federal Trade Commission suing a manufacturer of IoT devices when it was found that they

[281] Verababyspot. (2020). Nest Cam Baby Monitor Review: Everything You Need to Know.
[282] Stanislav, M., et al. (2015). Hacking IoT: A case study on baby monitor exposures and vulnerabilities. Rapid7.
[283] Nord VPN. (2018). Hacker terrorizes family by hijacking baby monitor. (Article published December 2019).
[284] Poremba, S. (2020). Will Weak Passwords Doom the Internet of Things (IoT)? Security Intelligence.
[285] Department for Digital, Culture, Media & Sport (DCMS). (2018). Code of Practice for Consumer IoT Security.
[286] Busch, J. (2019). Yes, Your Video Baby Monitor Can Be Hacked. No, You Don't Have to Stop Using It.

used hackable default passwords in their routers and baby monitors.[287] Moreover, the use of connected baby monitors, if not secured, can increase the possibility and impact of botnet attacks which can use them along with other devices in distributed denial of service (DDoS) attacks. This not only affect the performance of the devices but is also capable of shutting down major Internet platforms and affecting Internet traffic, as was the case with the Mirai botnet.[288]

[287] Pagilery, J. (2017). FTC sues maker of routers, baby monitors over security. CNN Business.
[288] Newman, L. H. (2016). What We Know About Friday's Massive East Coast Internet Outage. Wired.

Case study 5: Architectural Firm

It is not only the producers of smart devices and their customers that are exposed to the risks brought by hackable devices. Indeed, the risks of hacking and other cyber security threats exist for different organisations along the value chain, such as the businesses using smart connected devices in their business models. Every firm which possess devices that are connected to the Internet can suffer the consequences of a cyber attack, including service firms such as the architectural firm presented in this case study.

The Attack: Vulnerability, Exploitation and Mitigation

A smart drawing pad is a device that can be used to draw and present designs for different purposes. It can be used by firms in the creative industry to present examples of their work to clients. However, as is true for many devices used in the modern workplace, these can connect to the Internet. As such, the smart drawing pads used by these companies can become the medium through which a cyber-criminal can attack the integrity of a business' activity. These attacks are made more likely when companies use devices with default credentials.

The designers at an architectural firm in Italy[289] were using smart drawing pads to send schematics and drawings to clients and staff members. These devices had not had their software default credentials updated, and because they were connected to the office Wi-Fi, they were vulnerable to potential attackers scanning the Internet for weak targets.[290] As such, it was possible for the attackers to use the default credentials that came with the pad software to hack the devices and use them to send distributed denial of service attacks. As a consequence of this, a series of anomalous behaviours occurred within the firm, such as spikes in its external communications, which led to vast volumes of data being sent to entertainment, government and design websites.[291] The hacked devices were responding to a type of request used to disable the targets' systems by flooding the victim organisations with superfluous requests for information.

The implementation of unique passwords, which are not resettable to any universal factory default value, would have prevented the attack to this firm's smart drawing pads, which affected theirs and other companies' networks, disabling critical business infrastructure.

Impacts

IoT attacks such as those discussed in this case study can have several impacts to the affected parties. As drawing pads were crucial to the firm's business model, their hacking could have led to the loss of device performance and the disruption of the firm's business, which could have led to economic losses. These effects would have also had the potential to bring additional reputational damage and even bring legal liabilities had the attack damaged the networks of other companies.

Attacks of this type can have an impact on other businesses, by flooding their websites with data in a denial of service attack, which in return can affect their ability to function or shut their services to online users. Moreover, this case study illustrated that attacks can damage the network of other organisations, which can lead them to underperform, lose information or lose money. To prevent attacks of this type, firms will have to prevent the purchase and set-up of smart devices without the oversight of an IT or security team.

[289] InfoSecurity. (2017). Global Threat Report 2017. Info Security North America.
[290] Draktrace. (2018). Global Threat Report 2017.
[291] Cimpanu, C. (2017). Smart Drawing Pads Used for DDoS Attacks, IoT Fish Tank Used in Casino Hack.

Case study 6: Router vulnerabilities

Wi-Fi access via a router is nearly ubiquitous across the UK; in 2019, the ONS found that 93% of all households had access to the internet, 98% of which connected via a fixed internet connection (i.e. through a Wi-Fi router).[292] However, cyber security vulnerabilities are commonly found in home Wi-Fi routers. For instance, ENISA specifically noted multiple examples of malware authors targeting home and small office routers in its 2018 Cyber Threat Landscape Report.[293] This case study illustrates a real-life example of the exploitation of vulnerabilities in routers and the subsequent impacts.

The Attack: Vulnerability, Exploitation and Mitigation

In 2013, the Polish Computer Emergency Response Team (CERT) received reports of modifications to internet banking websites, which meant that consumers were receiving messages about account number changes that required mobile Transaction Authentication Numbers (TANs) for confirmation. TANs are a form of single use one-time password used by banks to authorise financial transactions. For example, a bank may generate an mTAN when a user initiates a transaction and send it to the mobile phone of the user via SMS for confirmation.

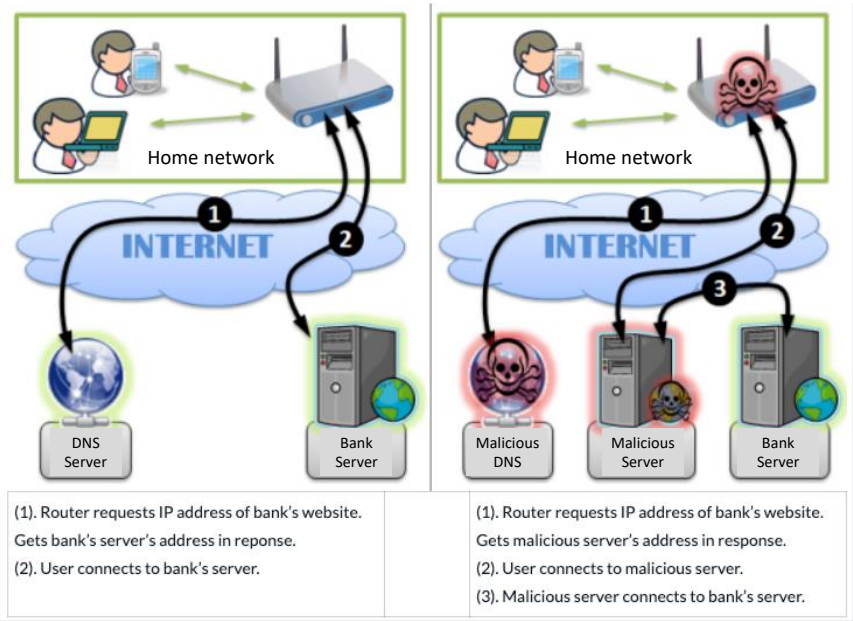
Following an investigation of these reports, the Polish CERT found that attackers had exploited a vulnerability in router firmware reportedly used in a number of commonly used router products.[294,295]

The vulnerability, known as ZyNOS, was used to conduct a range of attacks, including a man-in-the-middle attack to steal bank credentials from users of the routers. The ZyNOS vulnerability allowed the attackers to download the configuration file for the router without authentication. This file could then be unpacked and parsed to extract the router's 'admin' password.[296]

Once access to the router was gained, the attackers used a technique called DNS hijacking to take control of DNS servers, allowing them to redirect traffic to servers under their control. As illustrated in the below image, the attackers subverted the normal process for connection to the bank's server (shown on the left). The attackers achieved this by rerouting traffic intended for the banking website to their malicious server. As a result, the attackers tricked users into providing usernames, passwords and even TANs.

In addition, researchers at Team Cymru found that a separate campaign had used the ZyNOS vulnerability amongst other approaches to launch attacks against more than 300,000 wireless routers across Europe, Asia and the Americas. Team Cymru noted that "consumer unfamiliarity with configuring these devices, as well as frequently insecure default settings, backdoors in firmware, and commodity-level engineering standards make SOHO-type (small office / home office) wireless routers a very attractive target for cyber criminals".[297]

[292] Office for National Statistics. (2019). Internet access – households and individuals, Great Britain: 2019, Release date: 12 August 2019.
[293] ENISA. (2019). ENISA Threat Landscape Report 2018.
[294] CERT.PI. (2014). Large-scale DNS redirection on home routers for financial theft.
[295] Constantin, L. (2014). Cybercriminals compromise home routers to attack online banking users. PCWorld News.
[296] Root@Nasro. (2014). Information Security Blog: How I saved you're A** from the ZyNOS Attack.
[297] Team Cymru Threat Intelligence Group. (2014). SOHO Pharming, A Team Cymru EIS Report: Growing Exploitation of Small Office Routers Creating Serious Risks.



Source: Translated from CERT.Pl, (2014), Large-scale DNS redirection on home routers for financial theft.

It is noted that router manufacturers have released firmware patches for affected devices, but that users rarely update routers and other networking devices.[298] Beyond patching, the Polish CERT advises that default usernames and passwords should not be used and should be changed, and consumers should pay close attention to the browser's address bar to ensure HTTPS is in use.[299]

In this respect, preventing the use of default usernames and passwords by routers as detailed in the CoP Guidelines would act to mitigate similar attacks from occurring in the future.

Impacts

In this, and attacks using similar vulnerabilities, the primary objective was financial theft from targeted individuals. Although there is no insight into the extent of the theft via this attack, the Team Cymru finding at least 300,000 targeted routers indicates the potential scale of the theft.

In addition to financial theft, the access achieved through the ZyNOS vulnerability provides opportunities for other personal and wider impacts. For instance, in the same way as it can be used to redirect users attempting to access their online banking, DNS hijacking can also have significant privacy consequences. Malicious actors can profile users on the basis of the DNS queries they make, as well as conduct man-in-the-middle attacks, as described above, to redirect and gather not only card details but usernames and passwords across a whole variety of webpages. This could allow such malicious actors to access a range of private and potentially sensitive documents, messages, images, videos, for example through user accounts with cloud storage services and social media platforms, or steal access to services and subscriptions paid for by the user (e.g. online video streaming services).

Furthermore, the significant number of routers potentially compromised could also be used to conduct Distributed Denial of Services (DDoS) attacks.

[298] Constantin, L. (2014). Attack campaign compromises 300,000 home routers, alters DNS settings. PCWorld News.
[299] CERT.Pl. (2014). Large-scale DNS redirection on home routers for financial theft.

Case study 7: Attacking the power grid

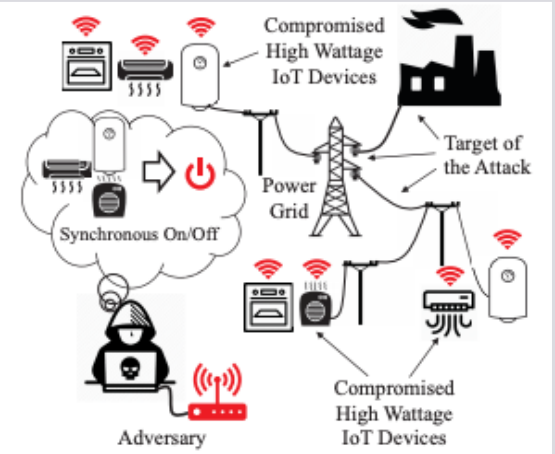
In its most recent Connected Home report, techUK reported that, although the appeal of smart appliances is lower than many other product categories (for example, smart entertainment and connectivity products or smart energy and lighting products), consumer appeal has increased in 2019.[300] Furthermore, increases in appeal were found across specific products within the smart appliance category, particularly considering larger products such as smart refrigerators and smart washing machines. In addition, this study has found that manufacturers of smart appliances add connectivity to existing appliances but may have little experience in security engineering.[301]

This case study details the findings of research from Princeton University that demonstrates how risks to the power grid can occur as a result of exploiting vulnerabilities in high-wattage smart home appliances.[302]

The Attack: Vulnerability, Exploitation and Mitigation

The research does not highlight specific vulnerabilities, but presumes the existence of a botnet that, like the Mirai botnet, could compromise significant numbers of smart devices (in this case, high-wattage home appliances like air conditioners and heaters). To give an idea of the scale, the Mirai botnet compromised 600,000 devices at its peak and used default usernames and passwords as a key mechanism to infect consumer IoT devices.[303]

Through the use of a botnet of high-wattage smart appliances, the researchers detail a new class of potential cyber attacks called the Manipulation of demand via IoT (MadIoT). These attacks target the power grid by manipulating power demand. Five variations of the MadIoT attacks are illustrated:



Source: Soltan, S., Mittal, P. and Poor, H.V. (2018). BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid, Princeton University, Paper for the 27th USENIX Security Symposium.

- **Significant increases or decreases in power demand** by synchronously switching all bots in the botnet on or off;
- **Disrupting power grid restart** by synchronously switching all bots on when the power restarts following a blackout, when inertia across the system is low and the system is particularly vulnerable to demand changes;
- **Line failures and cascades** by targeting specific power lines by synchronously switching on all bots in those locations. Furthermore, increasing demand in some locations while decreasing demand in others, thereby keeping total demand constant, could have similar affects to the first attack variation, with greater ability to hide the attack;
- **Failures in the tie-lines** that connect neighbouring independent power systems, for example between neighbouring countries and the Independent System Operators (ISOs). The actual

[300] techUK. (2019). The State of the Connected Home: Edition Three.
[301] ENISA. (2014). Threat Landscape and Good Practice Guide for Smart Home and Converged Media; and IoT.
[302] Soltan, S., Mittal, P. & Poor, H.V. (2018). BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid, Princeton University, Paper for the 27th USENIX Security Symposium.
[303] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., et al. (2017). Understanding the Mirai botnet. In Proc. USENIX Security Sympsion'17.

power flows between ISOs can be monitored online. As such, this represents another type of specifically targeted attack, which can focus on tie-lines that are carrying close to capacity;

- **Increasing the operating cost** by slowly switching on the bots during peak hours of power demand, requiring ISOs to purchase additional electrical power from reserve generators at a higher price.

From a mitigation perspective, the MadIoT attacks have a range of unique properties that limit the ability to protect against them. As the researchers summarise, "the MadIoT attacks' sources are hard to detect and disconnect by the grid operator due to their distributed nature. These attacks can be easily repeated until being effective and are black-box since the attacker does not need to know the operational details of the power grid [to implement the attack]."[304]

Here, the implementation of aspects of the top three CoP guidelines are unlikely to contribute significantly to mitigation. However, at the root of the attacks is the existence of a botnet, which could be built on infecting consumer IoT devices using default username and password credentials, as well as other vulnerabilities. The implementation of the first CoP guideline should improve the situation with regard to the use of default credentials, while the second and third guidelines should improve the overall vulnerability environment by ensuring known vulnerabilities are patched effectively.

Impacts

The cyber attacks described above could have significant impacts on the power grid of a country, as well as power exchange between countries. Although such attacks have not been implemented, the researchers detail three categories of impact that build on the five variations:

- Cause frequency instability by forcing a sudden increase or decrease in power demands causing generators to trip and potentially instigate a large-scale blackout.
- Cause line failures and result in cascading failures in specific locations.
- Increase operating costs for grid operators. Beyond increasing operating costs for operators, this could also be used to manipulate the electricity market to the benefit of a particular utility, for example by slowly increasing demand at a particular time of day or in a certain location.

In addition, the researchers highlight examples of real-life large-scale blackouts, the impacts of which could equally have been caused by a MadIot attack and thus illustrate the potential impact of such an attack:

2003 Blackout in Italy: Italy was importing more power from Switzerland and France than initially agreed. As this was happening, a tie-line between Switzerland and Italy tripped due to an overload caused by touching a tree. This series of events caused a further overload on and tripping of a separate tie-line between Italy and Switzerland. Subsequently, further lines between Italy and France, Slovenia and Austria also tripped resulting in the disconnection of the Italian grid from the continental European grid. As a result, Italy suffered a significant imbalance between supply and demand that it could not correct leading to a power outage across the vast majority of the country. Over the next 18 hours, an estimated 177 gigawatt hours (GwH) of electrical power were not supplied;[305] according to Ofgem, one GwH can power one million UK homes for an hour.[306]

[304] Soltan, S., Mittal, P. and Poor, H.V. (2018). BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid, Princeton University, Paper for the 27th USENIX Security Symposium.
[305] Union for the Coordination of the Transmission of Energy (UCTE). (2004). Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy, UCTE Report, April 2004.
[306] Ofgem. (n.d.). Electricity generation: facts and figures.