EVIDENCING THE COST OF THE UK GOVERNMENT'S PROPOSED REGULATORY INTERVENTIONS FOR CONSUMER IOT

Main report: 2020

ACKNOWLEDGEMENTS

This study was carried out for DCMS by RSM UK Consulting LLP, with YouGov and the European Centre for International Political Economy.

The RSM project team comprised Jenny Irwin (Partner), Matt Rooke (Project Manager), Anna Clarke (Associate Director), Glenn Donnelly, Marianna Lemus Boskovitch, and Polly Jackson (Senior Consultants), Tubo Adeaga, Ciara Barry, Amy Hau, Emma Liddell, and Aidan Thornbury (Consultants).

The consumer survey was managed by Russell Feldman of YouGov. The international trade modelling was carried out by Dr Matthias Bauer and Dr Philipp Lamprecht of the European Centre for International Political Economy. Our other academic project advisors were Dr Razvan Nicolescu, Dr Jason R. C. Nurse, Professor Martin Sadler and Dr Leonie Tanczer.

The research team is grateful to the DCMS Secure by Design Team for their support in conducting the research, as well as all participants in the stakeholder consultations and business and consumer surveys.

EXECUTIVE SUMMARY

Introduction

RSM UK Consulting LLP was appointed by the Department for Digital, Culture, Media and Sport (DCMS) to conduct research evidencing the cost of the UK Government's proposed regulatory interventions to improve the cyber security of Consumer Internet of Things (IoT) devices.

Background and policy context

Consumer IoT is defined in this research as network-connected (and network-connectable) devices and their associated services that are usually available for consumers to purchase both online and in stores. The product's purpose is typically for use within the home or as a personal mobile device (e.g. wearable or smartphone).

For the purpose of this research, consumer IoT is split into three groups:

Big ticket items	Connecting the home	Consumer lifestyle
Smart TVs, smart white goods, smart kitchen appliances etc.	Smart thermostats, home assistants, smart speakers, smart security cameras, smart doorbells etc.	Smart tablets, smartphones, smart toys, smart watches etc.

The number of IoT devices in the UK and globally is increasing significantly; it is estimated that there will be approximately 75 billion connected devices by 2025.[1] The most prevalent consumer IoT devices include smartphones, smart TVs, wearable devices, and smart speakers. The lack of transparent information available about the security of these devices means that consumer security, privacy, and safety is vulnerable and liable to be compromised.

The UK Code of Practice (CoP) for Consumer IoT Security was developed in 2018 by DCMS, in conjunction with the National Cyber Security Centre (NCSC) and follows engagement with industry, consumer associations and academia. The CoP brought together 13 guidelines widely considered to be good practice in IoT security. The top three guidelines from the CoP are:

1. **All device passwords must be unique and not resettable to a factory default;**
2. **Device manufacturers must provide a public point of contact as part of a vulnerability disclosure policy to report vulnerabilities and act on these in a timely manner; and**
3. **Manufacturers must explicitly state the minimum length of time for which the device will receive security updates.**

In May 2019, the UK Government launched a consultation on regulatory proposals to improve the security of consumer IoT devices.[2] Respondents showed a preference for the government taking powers to regulate the security of consumer IoT devices and felt the top three aspects of the CoP were an appropriate minimum standard for device security, especially the requirement to remove default passwords.[3] The proposed regulatory options are therefore based around compliance with aspects of the top three guidelines.[4]

[1] Statista: Internet of Things (IoT) Connected Devices Installed Base Worldwide from 2015 to 2025 https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
[2] DCMS (2019) 'Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security'
[3] DCMS, 2020 'Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation'
4 DCMS 2020 'Government to strengthen security of internet connected products'

Market Study

A consumer IoT market study was conducted as part of this research to understand the key products on the market, within the three product category groups of ‘big ticket items’, ‘connecting the home’, and ‘consumer lifestyle’. This focused on the security information provided to consumers by manufacturers and retailers, both online and in stores. In total the market study included 345 different products from 164 unique manufacturers. These products were found and analysed across 15 different retailers’ websites and in seven different stores.

Very little information relating to the top three security guidelines is visible on online product listings, packaging, or downloads of product manuals available at the point of sale (see Table 1 below).

Table 1: Information at the point of sale on top three CoP guidelines by product group

Group	Security updates	Vulnerability disclosure policy	Default passwords
Group 1: Big Ticket Items	3%	0%	0%
Group 2: Connecting the Home	0%	7%	0%
Group 3: Consumer Lifestyle	6%	8%	0%

Source: Market Study of Consumer IoT Products (n=345)

It is notable that many of the security features that are identified by retailers or manufacturers relate to encryption and safeguarding of user data; this is likely due to the high visibility of the General Data Protection Regulation (GDPR) and public awareness of online privacy breaches.

Consumer survey

A survey of 5,421 consumers, representative of the UK population of adults (18 and over), was also conducted to assess consumer IoT device ownership and behaviours, analysed by the three product groups and subcategories within these. Respondents were asked about their interaction with smart devices, their device ownership and usage (including the use of internet connectivity functions), details of upgrading and replacing their devices, and use of smart devices by their employers. Full details of the questions can be found in Chapter 6 of the accompanying technical report.

It was found that the most commonly owned smart device is a smartphone, with 83% of survey respondents owning at least one.[5] The next most commonly owned devices were tablets (65%) and smart TVs (54%).[6] By contrast, the least commonly owned devices were smart or connected children’s toys and baby monitors, with these products only owned by 2% of the sample.[7]

The average number of devices owned are as follows:

- Group 1: Big ticket items: 0.88 per household (1.59 per household that owns at least 1)
- Group 2: Connecting the home: 1.06 per household (2.94 per household that owns at least 1)
- Group 3: Consumer lifestyle: 1.82 devices per household (2.01 per household that owns at least 1)

The most commonly disconnected smart device product group is “big ticket items”, with 25% of owners having disconnected their device from the internet at some point, or having simply never connected. This is closely followed by consumer lifestyle devices, at 24%. The lowest disconnection rate is for connecting the home devices, with only 15% of owners within this product group having disconnected at any point, or never connecting their device.

[5] Base: 5421 respondents
[6] Base: 5421 respondents
[7] Base: 5421 respondents

Survey respondents were also asked about their employers' use of consumer IoT devices in the workplace. Overall, 50% of respondents answered that smart devices were used by their organisations.[8] Of these, the most popular smart devices were smartphones, with 35 % of respondents indicating that their organisation uses these. This was followed by tablets, which were used by 21% of respondents' employers.

Concerns about the security of smart devices do appear to be a significant barrier to growth of the sector: among consumers who said that they did not plan to purchase smart devices in the next 12 months, 28% said that they were concerned about the security of smart devices, and 30% were concerned about their privacy. Those with security, privacy or quality concerns (n=690) were asked what factors would encourage them to purchase such a device. The most common answers were:

1. Independent certification / assurance of minimum security standards (28%);
2. Transparency on length of time that security updates would be provided (22%);
3. Assurance that each device has a unique password (20%);
4. Assurances from manufacturers on adherence to minimum security standards (19%)
5. Security information at point of sale (19%)
6. Assurance that vulnerabilities can be reported to the manufacturer (17%)

It is notable that for consumers, independent assurance of standards was more commonly cited as a factor to encourage purchasing of smart devices than assurances from manufacturers.

Manufacturer and retailer surveys

Surveys were completed by 22 consumer IoT manufacturers and 12 retailers. Survey fieldwork was partially conducted during the COVID-19 pandemic, which made it more difficult to contact businesses to encourage them to respond to the survey. The response count is lower than ideal and findings should therefore be treated with caution. In the case of IoT manufacturers, however, the overall number of companies in the UK is relatively low, and the survey population represents around 13% of all consumer IoT producers active in the UK market that our study was able to locate[9]. The manufacturer survey also represents a share of total UK IoT sales substantially higher than 13%, as the survey included some of the largest companies in the market (as identified in the market study exercise).

The top three consumer IoT security guidelines

Default passwords: The market study and accompanying review of literature found very few products explicitly supplied with default passwords in the UK market, although in many cases the information on products did not confirm this either way. The manufacturer survey findings suggested that such products are now rare in the UK market: out of 17 respondents, only one (6%) indicated that any of their devices were produced with a default password, and this was the case for only 1-10% of their products.

The firm in question stated that no costs of removing default passwords would be passed on to the consumer, and that no products would be discontinued, if this security requirement were to be mandated, suggesting that they would be absorbed as a normal cost of business and would not be significant. This was corroborated in telephone discussion with a small number of firms at the pilot stage of the research, who were already compliant with this Code guideline, but were asked to confirm what the costs of these changes *had been* when they undertook them; they were typically absorbed as normal costs of doing business and necessary to providing a secure product that would earn consumer trust. Given this, **the average cost of implementation can be assumed to be not significant**.

[8] Base: 5421 respondents
[9] 170 companies were located through a combination of market research, online searches, and liaison with sector representative bodies.

Vulnerability disclosure policies: Out of 16 respondents to the manufacturer survey, 12 (75%) stated that they already had a vulnerability disclosure policy. The remainder said that they would introduce such a policy for their consumer IoT products if mandated, with just one saying that they would stop selling some of their products to the UK market.

These results show that the overall impact of mandating this Code guideline would be low or zero in many cases, although even companies with a policy would bear some familiarisation costs to ensure that it was fully compliant with any legislation. These costs could include legal advice.

On average, the estimated amount of staff time required to implement any changes as a result of legislation and provide a point of contact for reporting vulnerabilities for manufacturers where a change was required was 28.0 person days. However, as many manufacturers believed that they were already compliant and would require no extra resources, **the average staffing cost of implementation across all companies was just £1,938 per manufacturer.** The respondents were also asked to consider other external costs (e.g. from legal or technical specialists); they were typically unable to quantify these without seeing any final legislation.

Security updates: Few manufacturers in the survey sample currently publish a minimum length of time for which security updates would be provided. Out of 17 respondents to this question, only 4 (24%) provided this information to consumers for all their products, 1 (6%) said that only 11-20% of their products provided this, and the remaining 12 (71%) said that none had this information.

If aspects of this Code guideline became mandatory, all 12 companies answering the question said they would implement it in full and provide information for all their consumer IoT products for sale in the UK. In addition, two (17%) said they also would stop selling some products in the UK, and one (8%) would stop producing some products in the UK.

Mandating aspects of this Code guideline potentially affects more of the market than the other two (many companies had already adopted the first two), and it is also viewed as more time-consuming to implement. Findings from this survey indicated that the average amount of staff time required for compliance would be 91.4 person-days, mostly within IT professional/technical roles, and sales and marketing roles[10]. **The average annual cost of the staff time is estimated at £17,631.**

Cost of physical IoT security label

Manufacturers estimated that significant effort would be required to implement mandatory physical labelling on their products, with cost estimates ranging from just £3,000 to £500,000 per company for the largest manufacturers. **The average one-off cost of implementing a physical label across all manufacturers is estimated at £100,630.** This is the highest manufacturer cost among all of the legislative options studied; however, the sample for this particular question includes more information from the largest manufacturers than any other in the sample. The response of £500,000 was 0.79% of the respondent's IoT turnover, a similar relative cost to those reported by other manufacturers (one small manufacturer reported a cost estimate of 1.63% of IoT turnover).

On average, manufacturers redesign their product packaging every 30.3 months; therefore, with sufficient lead-in time, labelling could be built in to regular redesign, thus reducing the costs.

Retailers believed that the cost of a labelling scheme to them would be minimal, at up to a person-day each for occupations including managers, legal professionals, sales advisors, customer service, and admin staff. **The estimated total was 8.1 person-days, costing £1,676.**

[10] Further information: page 111

Cost to retailers of presenting compliance information at the point of sale

Retailers had a low level of awareness of whether there would be any cost to them in obtaining, requesting, or storing information from producers about the compliance of their products if aspects of the top three guidelines of the Code were mandated in law. They suggested a wide range of methods for presenting product security information at the point of sale, including online, in technical specifications, in-store labels, brochures, and price tickets.

Staff time spent on familiarisation with the legislation would be an average of 30.4 person-days spread across their organisations; typically corporate manager or director time did not exceed four or five days, whereas the costs in administrative, sales advisor and customer services representative days was estimated to be five to ten person-weeks for some organisations. **The average one-off cost was estimated to be £4,781**. Two-thirds (67%) of respondents felt that they would not need to use external advice or consultancy.

Estimated familiarisation costs for manufacturers

Manufacturers estimated that familiarisation with the legislation based on mandating aspects of the top three guidelines of the Code would require an average of 15.2 person-days, or cost an equivalent of £2,465. This varied from "a few hours for the chief product officer" to "over three months to ensure the entire business was aware of the legislation". The variation appeared to be a function both of the size of the businesses and their present level of readiness.

For the product labelling option, **manufacturers** estimated that 11.8 person days would be required on average for familiarisation, costing an average of £1,585.

Costs to manufacturers of product self-assessment

Manufacturers estimated that an average of 30.1 person days per year would be required to undertake a self-assessment as part of their self-declaration to retailers. More than half of this time would be for IT professionals or technical staff, with time also spent by IT/technical directors or specialist IT managers. **The cash equivalent of this time is estimated at £6,575.**

Further research

Three of the research objectives were carried out by or in association with specialists from our academic advisory panel.

Impact on the ability of IoT security researchers and cyber security professionals to effectively report vulnerabilities

Recent survey evidence[11] suggests that researchers are already proactive about reporting vulnerabilities; some companies offer 'bug bounties' to encourage this but researchers report that companies are becoming more open to receiving vulnerability information and working with them. The majority of companies in our survey sample had some form of public route for vulnerabilities to be disclosed. They do not, therefore, anticipate that introducing legislation on vulnerability disclosure policies will lead to a great increase in their use. The typical length of time to respond to vulnerabilities varies greatly between companies, but also from report to report depending upon the nature of the vulnerability.

As the number of IoT devices continues to increase, and reported vulnerabilities are seen to be addressed, vulnerability disclosures are likely to increase, and the challenge then becomes whether companies can keep up with reports.

[11] HackerOne (2018) 'The 2019 Hacker Report'

Costs of disposal of non-compliant stock

Currently, only 17% of consumers dispose of IoT products by throwing them away; the rest are either retained, passed onto someone else or charity, or resold. Estimates of the cost of disposal of non-compliant stock ranged between 0.5% and 1.6% of turnover for three manufacturers who provided estimates; two more said that the cost would be “negligible”.

The retailers in our survey were not able to provide total costs of disposal without information on any implementation period, as this would determine the amount of stock they would need to dispose of; unit costs for disposal ranged from £10-£50 per unit, or free of charge if this was provided for in their relationship with their supplier. The most common retailer strategies for disposal were returning to the manufacturer, disposing in refuse, or destruction.

Wider environmental costs (including changes in fuel usage and release of carbon dioxide) were sought in the literature but an adequate evidence base could not be derived as the relevant information was not presented in the studies accessed.

Impacts on UK trade and investment

The costs to businesses identified in the survey research, and corroborating research from the academic and trade literature, was used to create an economic model of the potential impact to the UK economy if imports were banned for non-compliant products. Two policy options were considered: mandating aspects of the top three CoP guidelines, and a mandatory security label.

Under both policy options overall economic activity in the UK will remain largely unaffected by the proposed measures. UK trade volumes will only marginally decrease in response to the implementation of the policy measures, with UK production rising marginally to compensate.

Generally, SMEs would be more affected than large companies as they face higher compliance costs per unit, which may decrease their domestic and international competitiveness.

The highest relative impacts would likely result from costs related to the disposal of non-compliant products. These costs are, however, temporary. Foreign suppliers to the UK are expected to amend their products and make sure they comply with UK regulations.

It is not expected that investment in the UK will decrease as a result of the proposed regulations, nor is it expected that there will be a deterioration of the UK’s investment climate.

The effects on UK trade and investment will be even smaller if more countries proceed with the implementation of similar sets of regulations. International cooperation aiming for harmonised standards would contribute to maintaining high trade volumes in the medium- and long-term, while the proliferation of diverse unilateral measures would increase distortions in international trade.

CONTENTS

1. INTRODUCTION

RSM UK Consulting LLP was appointed by the Department for Digital, Culture, Media and Sport (DCMS) to conduct research evidencing the cost of the UK Government's proposed regulatory interventions to improve the security of the Consumer Internet of Things (IoT).

This research includes a two-stage evidence review, consisting of (a) framing the baseline of the consumer IoT landscape and (b) quantifying the costs of proposed regulatory options by the UK government. This builds upon the existing evidence base as set out in the 2019 regulatory consultation impact assessment.[12]

For the purposes of this piece of work, DCMS separated 'consumer IoT' into the following three product category groups:

- Group 1 ('**Big ticket items**'): For example, smart TVs, smart white goods, smart kitchen appliances etc.
- Group 2 ('**Connecting the home**'): For example, smart thermostats, home assistants, smart speakers, smart security cameras, smart doorbell etc.
- Group 3 ('**Consumer lifestyle'**): For example, smart handheld devices, smart watches, smartphones, smart toys etc.

Background and Context

Secure by Design

The UK Code of Practice (CoP) for Consumer IoT Security[13] was published in 2018 by the Department for Digital, Culture, Media and Sport (DCMS). The CoP brought together 13 guidelines widely considered to be good practice in IoT security and was developed with technical experts, the National Cyber Security Centre (NCSC) and a range of other stakeholders in industry, consumer associations, and academia. DCMS also published a mapping document[14] linking the CoP guidelines to existing standards, recommendations and guidance on IoT security and privacy from around the world. The top three guidelines of the Code are:

1. **All device passwords must be unique and not resettable to a factory default;**
2. **Device manufacturers must provide a public point of contact as part of a vulnerability disclosure policy to report vulnerabilities and act on these in a timely manner; and**
3. **Manufacturers must explicitly state the minimum length of time for which the device will receive security updates.**

In February 2019, the European Standards Organisation (ETSI) published the first globally applicable cyber security standard for consumer IoT devices, which established a security baseline for internet connected consumer devices and could provide a basis for future certification schemes. The ETSI Technical Specification (TS) 103 645 builds on the Code of Practice for Consumer IoT Security and has been developed with wider European and global objectives in mind. The Technical Specification is in the process of being transposed into

[12] https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security

[13] DCMS (2018) 'Code of Practice for Consumer IoT Security'

[14] DCMS (2018) 'Mapping of IoT security recommendations, guidance and standards'

European Standard, EN 303 645. As of April 2020, the Final Draft of the EN is subject to voting by European National Standards Organisations.

The CoP is a voluntary set of guidelines; however many consumer IoT devices are sold without critical minimum security features, and securing them is an afterthought due to the lack of economic incentives for device manufacturers.[15] For example, 87% of IoT manufacturers have no form of public vulnerability disclosure policy[16] as per CoP guideline 2. There is evidence that consumers are concerned about the security of devices,[17] but are not always aware that security features exist or know how to configure these features.[18]

Cyber security and IoT

Consumers face an increasing threat of cyber-attacks through exploitation of insecure consumer IoT devices. There is a need to create transparency within the market, particularly between manufacturers and consumers by ensuring that information about the security built into products is more clearly communicated, to help consumers understand how they can reduce their risk of attack.

Of particular concern is the risk of cybercriminals exploiting vulnerabilities, such as default passwords, in consumer IoT to take control of devices and use them to mount large Distributed Denial of Service (DDoS) attacks on public services, infrastructure and businesses. DDoS attacks are malicious attempts to disrupt the normal traffic of a targeted server, service or network by overwhelming the target with a flood of internet traffic. Successful DDoS attacks use multiple compromised systems, including IoT devices, as sources of attack traffic.[19]

The Mirai botnet attack of October 2016 was the one of the largest DDoS attacks in history[20], using an estimated 100,000 devices to disrupt popular websites like Twitter, Amazon, PayPal and Netflix for almost an entire day. As well as the potential to blackmail organisations and cause disruption to services, costs to consumers of DDoS attacks are mostly from the increased internet bandwidth and energy use per device while it is being used as part of an attack.[21]

While DDoS attacks are currently the main threat,[22] there is interest among some cybercriminal communities in using similar malware to hijack devices[23] to 'mine' crypto-currency, such as Bitcoin, for financial gain.[24] Bitcoin mining requires considerable computing power and, although the wider impacts are less serious, would be likely to incur higher costs (internet and electricity usage) to consumers per device than DDoS attacks.[25]

[15] Blythe JM, Sombatruang N, & Johnson S (2019) 'What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?'
[16] IOTSF (2020) 'Consumer IoT: Understanding the Contemporary Use of Vulnerability Disclosure 2020 Progress Report'
[17] Zubiaga A, Procter R & Maple C (2018) 'A longitudinal analysis of the public perception of the opportunities and challenges of the Internet of Things' PLoS ONE 13(12): e0209472.
[18] McKinsey & Company (2017) 'Security in the Internet of Things – How semiconductor companies can address the major obstacle to IoT growth, and benefit in the process'
[19] https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack/
[20] Payne BR & Abegaz TT (2018) 'Securing the Internet of Things: Best Practice for Deploying IoT devices' in Daimi K (ed.), Computer and Network Security Essentials pp 493-506
[21] Fong K, Helper K, Raghavan R & Rowland P 'rIoT: Quantifying Costs of Insecure Internet of Things Devices' University of California Berkeley School of Information
[22] Hilt S, Kropotov V, Merces F, Rosario M & Sancho D (2019) 'The Internet of Things in the Cybercrime Underground' Trend Micro Research
[23] Hilt S, Kropotov V, Merces F, Rosario M & Sancho D (2019) 'https://documents.trendmicro.com/assets/white_papers/wp-the-internet-of-things-in-the-cybercrime-underground.pdf' Trend Micro Research
[24] McMillen D & Alvarez M (2017) 'Mirai IoT Botnet: Mining for Bitcoins?' Security Intelligence
[25] Lee T (2017) 'Bitcoin's insane energy consumption, explained'. Ars Technica.

Cyber-attacks against consumer IoT may also be damaging to the privacy and security of individual device owners. For example, an attacker may hack into a smart door lock and enter an individual's property without permission, or a smart toy might be hacked into to listen in on and communicate with a child.

Consumers currently lack information about security features included in smart devices. As they are not able to assess important security information, they are not able to reward those manufacturers making secure products by purchasing devices with greater security over less secure ones.[26] A recent study[27] reviewed security information in manuals and online support pages for consumer IoT devices. In this study, 270 products were reviewed and overall 170 had some security information discussed in the user manual or on the website.

As a greater number and variety of devices enter the market, the possibilities for attackers are multiplying, which is likely to lead to the development of more advanced threats, such as firmware infections.[28]

2019 Consultation on the Security of Consumer Internet of Things

In May 2019, the UK Government launched a consultation on regulatory proposals to improve the security of consumer IoT devices.[29] The three options proposed were:

- **Option A:** Mandate retailers to only sell consumer IoT products that have a 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 aspects of the top three guidelines of the CoP, with manufacturers to self-assess that their consumer IoT products adhere to the relevant aspects of the top three guidelines of the CoP 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 which evidences compliance with all thirteen guidelines of the CoP 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.

DCMS published a response to this consultation in February 2020, with the consultation receiving 60 formal written responses. Respondents showed a preference for the government taking powers to regulate the security of consumer IoT devices and felt the top three aspects of the CoP were an appropriate minimum standard for device security, especially the requirement to remove default passwords.[30] The proposed regulatory options are therefore based around compliance with aspects of the top three guidelines.[31] For more information, the consultation response can be found at: www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/outcome/government-response-to-the-regulatory-proposals-for-consumer-internet-of-things-iot-security-consultation.

[26] Morgner P, Freiling F & Benenson Z (2018). 'Opinion: Security Lifetime Labels -- Overcoming Information Asymmetry in Security of IoT Consumer Products.' 11th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'18)
[27] Blythe JM, Sombatruang N, & Johnson S (2019) 'What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?'
[28] Hilt S, Kropotov V, Merces F, Rosario M & Sancho D (2019) 'The Internet of Things in the Cybercrime Underground' Trend Micro Research
[29] DCMS (2019) 'Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security'
[30] DCMS, 2020 'Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation'
[31] DCMS 2020 'Government to strengthen security of internet connected products'

Methodology

A mixed-methods approach has been used, including primary and secondary research, comprising:

- desk research on the consumer IoT sector in the UK and the literature on vulnerabilities;
- stakeholder consultations with experts in industry and academia;
- a market study to gain information on the products available to UK consumers;
- a consumer survey, conducted by YouGov, on ownership of IoT devices; and
- surveys of manufacturers and retailers for evidence on the specific costs of regulation.

Literature review

We reviewed literature focusing on: existing cyber security policy and guidelines; existing research into IoT cyber security and vulnerabilities; case studies of relevant cyber-attacks; the current levels of security information provided by manufacturers and retailers of consumer IoT devices. Sources included the following.

- Government policy literature including the UK National Cyber Security Strategy 2016-2021[32], the UK Code of Practice (CoP) for Consumer IoT Security[33], and The Internet of Things: making the most of the Second Digital Revolution[34];
- Research and policy papers from the PETRAS IoT research hub, the IoT Security Foundation, ENISA, and AIOTI; and
- Articles from a wide range of academic journals looking at IoT, cyber security and vulnerabilities, and the effects of regulation.

Consultation with stakeholders

We conducted telephone interviews for expert advice and sector consultation to confirm the design of the research and seek information on wider benefits to consumers, businesses and society which could be realised as a result of a mandatory security baseline for consumer IoT devices. These discussions were used to confirm the potential vulnerabilities by product type that the regulation of consumer IoT security is being designed to address. They also established additional contacts for further consultation later in the research programme and helped identify published data and reports for desk research.

Market study

The market study involved a review of the consumer IoT marketplace through a variety of methods. We have completed rigorous online investigations into the three product category groups and their subcategories, as well as visiting high street retailers of consumer IoT products to examine product packaging in person. We have also undertaken a brief review of relevant research in this area and have found one highly relevant paper[35] which analyses the communication of security features of consumer IoT products in manuals and support pages.

Our research included online searches of popular retailers, such as Amazon, Currys PC World, John Lewis, Argos, Very, B&Q, and Electrical Showroom, for smart devices within each of the product category groups. In total, we found products from 15 different online retailers, which were selected by searching for devices online and finding the most common/popular retailers within search results. We used these searches to find a range of products within each subcategory,

[32] HM Government (2016) 'National Cyber Security Strategy 2016 to 2021'
[33] DCMS (2018) 'Code of Practice for Consumer IoT Security'
[34] Walport (2014) 'The Internet of Things: making the most of the Second Digital Revolution' Government Office for Science
[35] Blythe JM, Sombatruang N, & Johnson S (2019) 'What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?'

collecting data on the product name, model number, price, manufacturer, product size (where relevant), and security information available on the retailers' websites.

A total of 345 different products were identified online and recorded any security information that was available directly on retailers' websites. For 21 products (or 6% of the sample) the retailers' website also provided the user manual for the product, which were analysed for details of security information. In all 21 cases where the user manuals were provided, these were provided on Amazon.

We then also researched the security information available to consumers online via manufacturer websites. A total of 164 different global manufacturers were identified and reviewed as part of this market study. This analysis consisted of checking for any details of the top three CoP guidelines, as well as any other relevant security information such as security notices and privacy policies. Product descriptions can be found in Chapter 2 of the accompanying technical report.

As well as online research, we also investigated the security information available to consumers in physical high street retailers. We were able to investigate seven different retail stores and the packaging of 25 different consumer IoT products, however relevant security details were rare.

Consumer survey

A large-scale, representative[36] survey of consumers was the only way to provide robust quantitative answers to the research questions on IoT ownership by product category.

YouGov conducted a survey of 5,421 UK consumers. The primary aim of the survey was to provide reliable quantitative data on the number of consumer IoT devices per household by brand and product group. The survey also included questions to allow us to estimate the average rate at which UK-based consumers upgrade or replace their consumer IoT devices, broken down by the above three categories of device, and explored the extent to which the decision to replace IoT products is driven by price or other factors. The survey was also used to explore user perceptions of IoT security, and to estimate the average number of consumers in the UK who, after purchasing a consumer IoT device opt out or switch off the internet connection function of the device, and the reasons for doing so.

The full consumer survey can be found in chapter 6 of the accompanying technical report.

Surveys of manufacturers and retailers

Participants for the manufacturer survey were identified through the market study (drawing from the 164 companies identified at that stage of the research), use of general business databases (Fame/ORBIS), internet research (including the IoT Nation database) and consultation with

[36] All figures are from YouGov Plc. Total sample size was 5,421 adults. Fieldwork was undertaken between 12th - 14th February 2020. The survey was carried out online. The figures have been weighted and are representative of all UK adults (aged 18+). The national representative quotas are derived from a range of sources and are all based on data from 2017 onwards. Sources include: ONS data (age, gender, region), annual population survey (to provide details of education level), national readership survey (to provide detail of social grade), census data (education level and social grade are both cross referenced with this). This survey has been conducted using an online interview administered to members of the YouGov Plc UK panel of 1,000,000+ individuals who have agreed to take part in surveys. Emails are sent to panellists selected at random from the base sample. The e-mail invites them to take part in a survey and provides a generic survey link. Once a panel member clicks on the link they are sent to the survey that they are most required for, according to the sample definition and quotas. The responding sample was weighted to provide a representative reporting sample of the UK population aged 18+. The profile for this is derived from census data. All results are based on a sample and are therefore subject to statistical errors normally associated with sample-based information.

manufacturers associations and DCMS. In total, 170 manufacturers were found that had a UK presence and were producing consumer IoT products available in the UK, of which 147 (86%) had publicly-available contact details and were therefore available to take part in our research.

Manufacturers were contacted by phone and email wherever possible prior to commencement of the survey in order that they could locate the most appropriate respondent(s) and the relevant information. Respondents could carry out the survey online, or could arrange to be taken through the questionnaire by phone. Following the initial contact and piloting, fieldwork ran for two weeks from 16-30 March 2020. In total, 22 responses were achieved. The full questionnaire can be found in chapter 8 of the accompanying technical report.

Potential retailers of consumer IoT goods were identified through two methods. A shortlist of 100 retailers was identified from information in the market study and from internet searches for each of the product groups. Subsequently, the business database Fame was used to identify a much longer list of retailers that had been identified as potentially selling at least one consumer IoT product in the UK by their Standard Industrial Classification code (such as electronics retail, audio-visual retail etc). In total, 1,886 retailers were directly invited to take part in this survey. In addition, two retailer umbrella bodies were contacted and asked to share the survey with their members, as well as publicising the survey through our social media channels. Fieldwork ran for 2 weeks from 17-30 March 2020. The survey received 12 valid responses. This is likely due to COVID-19 and many businesses focusing on their response to the situation, as well as several retail stores closing operations. The full questionnaire can be found in chapter 10 of the accompanying technical report.

Standalone research: security research, environmental impacts, international trade impacts

Additional research was conducted investigating whether a manufacturer publishing a point of contact to report vulnerabilities would impact on the ability of IoT security professionals to effectively report vulnerabilities; estimating costs associated with disposing of non-compliant stock; and evidencing the short, medium, and long-term impacts of regulatory proposals on UK trade and investment.

Investigations into these requirements involved building on questions asked in the manufacturer, retailer, and consumer surveys, and augmenting this with additional reviews of literature and industry publications, led by our academic advisory team. Estimations of costs of disposing of non-compliant stock also involved input from RSM's Green Book cost appraisal team. Evidencing the impacts on trade and investment required specialist analysis of the consumer and business survey data on current market activity and expected responses to any change in regulations, leading to a model-based simulation of the impacts of higher costs of production brought about by the regulations, and a proposed import ban for non-compliant products. This section was developed by an international trade economics team from the European Centre for International Political Economy.

Limitations

Limitations of this research chiefly concern the availability of primary data from businesses. Fieldwork took place during the COVID-19 novel coronavirus pandemic and its associated lockdown, during which companies were focused on core business activities and less willing to respond. This is particularly the case for the retailer survey, as these companies were more likely to have been explicitly closed down during the government's pandemic response, and fieldwork started slightly later for these businesses.

The population of consumer IoT manufacturers active in the UK is not well-known - there was no reliable external database that could have been used to recruit participants for the fieldwork. We are confident that the research has identified the majority of the population, and certainly the largest companies in the market, because of the combined approach of using the market research to identify products available in the market, and their manufacturers, and also publicising the survey online and through industrial associations and stakeholder groups.

The 22 responses from manufacturers are skewed towards the larger companies in our contact database; they are probably more likely already to be compliant than the population of manufacturers at large, and can bear the costs of necessary changes more efficiently. However, this skewness does mean that the results are representative of a large fraction of UK consumer IoT purchases by turnover; much larger than the 15% suggested by the response rate of 22 companies from a contact list of 147.

2. MARKET STUDY

This section of the research involved a review of the consumer IoT marketplace through online searches of popular retailers and visits to high street stores. This fieldwork was undertaken throughout January 2020 and completed on January 31.

As background research for this market study, we reviewed relevant research[37] which has been recently conducted, investigating the communication of security features of consumer IoT products in manuals and support pages. This research paper was published in the Journal of Cybersecurity and was written by three members of the UCL Department of Security and Crime Science, one of whom is also a member of a computer security service, CybSafe. The paper was written in light of the creation of the UK Code of Practice for Consumer IoT Security.

The study was slightly more specific than our research, with analysis of only the user manuals and support pages of consumer IoT devices, rather than including retailer websites. This involved the analysis of 270 consumer IoT devices produced by 220 different manufacturers, to provide an overview of a consumer's view of security features and the challenges they may face when making purchases. The identified security features were mapped to the CoP to examine the extent to which devices currently on the market conform to it.

The research found that manufacturers do not provide enough publicly available information about the security features of their devices, with information found in total on only five of the 13 UK CoP guidelines. Overall, it is suggested that this lack of information means that consumers often have very limited detail on the security of devices prior to purchase. The products that provided the most security details were produced by large manufacturers, suggesting that perhaps larger manufacturers disclose greater detail of security features (perhaps to service the requirements of international markets as well as the UK). While updates were the most commonly referenced feature, only 10% of devices that gave information on updates mentioned security explicitly as an aspect of those updates.

Moreover, across all of the products sampled, there was no indication of the minimum length of time that security updates would be provided for. The report also suggests that 'the burden for protecting devices is currently on consumers and manufacturers need to reduce this through greater "security by design"'.[38] Finally, the study highlighted that there is a lack of standardisation in the communication of security information for IoT devices.

The conclusions of this research support the findings of our own market study, with the key theme being that there is currently limited security information easily available to consumers at the point of purchase. The rest of this section looks at a range of products by device type, and provides information on price, the main manufacturers and retailers, and the security information provided to consumers.

[37] Blythe JM, Sombatruang N, & Johnson S (2019) 'What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?'
[38] Ibid.

Table 2: Summary of security information provided for devices in the three product groups

Group	Security updates	Vulnerability disclosure policy	Default passwords
Group 1: Big Ticket Items	3%	0%	0%
Group 2: Connecting the Home	0%	7%	0%
Group 3: Consumer Lifestyle	6%	8%	0%

Source: Market Study of Consumer IoT Products (n=345)

The market study for this research found that the most commonly discussed of the top three CoP guidelines was vulnerability disclosure policies (VDP), followed by security updates. There were no examples in our sample that discussed default passwords.[39]

It is also worth noting that there were no cases where information relating to more than one of the top three CoP guidelines was highlighted to consumers in any single product.

The table below shows the breakdown of these product groups into individual devices and the security information available for these.

[39] There may be smart products which do not have or require passwords; therefore, they would rightly have no information on passwords mentioned.

Table 3: Information provided on top three CoP guidelines summary

Group	Subgroup	Percentage of products that included any form of security information	Percentage of products that discussed any of the top three CoP guidelines	Which of the top three CoP guidelines were mentioned
Group 1: Big Ticket Items	Smart TVs	10%	7%	Security updates[40]
	Smart White Goods	10%	0%	n/a
	Smart Kitchen Appliances	33%	0%	n/a
Group 2: Connecting the Home	Smart Home Thermostats	50%	8%	VDP
	Home Assistants	71%	0%	n/a
	Smart Speakers	30%	15%	VDP
	Smart Security Cameras	47%	0%	n/a
	Smart Doorbells	27%	27%	VDP
	Smart Door Locks	67%	0%	n/a
	Smart Alarms and Sensors	63%	11%	VDP
	Smart Baby Monitors	56%	0%	n/a
	Additional Household Appliances	28%	0%	n/a
Group 3: Consumer Lifestyle	Smartphones	80%	15%	Security updates
	Smart Handheld Devices	68%	5%	Security updates
	Smart Watches and Health Monitoring	59%	5%	Security updates
	Smart Toys	35%	35%	VDP

Source: Market Study of Consumer IoT Products (n=345)

Group 1 (big ticket items) was less likely than groups 2 and 3 to include any form of security information. Smartphones (group 3) were most likely to include any form of security information, whilst smart toys (group 3) and smart doorbells (group 2) were the most likely to provide any information on the top three UK CoP guidelines.

Big Ticket Items

This product group includes larger consumer purchases such as smart TVs, smart white goods, and smart kitchen appliances. The total mean price for this product group is £735.96, with a large price range of £67.99[41] (smart kettle) to £6,999.00 (smart fridge freezer). This is on average the most expensive product group.

Relevant consumer IoT security information is uncommon with these devices. The only top three UK CoP guideline to be detailed was security updates, and even this did not include information about how long these would be provided. The general information on security was provided in the smart TV device category, and only covered 7% of the smart TVs sampled, and 3% of the total

[40] Where security updates were highlighted as an important security feature, the length of time for which these would be provided was never included.

[41] Smart thermometers costing as little as £32.99 are also included in this group as a subset of "smart kitchen appliances" but are not a typical "big ticket item".

big ticket item sample. Both smart white goods and smart kitchen appliances sampled did not include any details of any of the top three UK CoP guidelines.

Smart TVs

Ofcom estimate around 53% of TV owning households in the UK have an internet connection[42] to their TV and most TVs sold in the UK are now smart TVs. While broadcast TV is still the most popular way to watch, the amount of time spent on this is declining across all age groups, particularly younger ones, while other ways of watching (e.g. subscription services such as Netflix) are increasing.

Price and Size

It is difficult to provide an overall average cost for a smart TV due to differences in size and consumer choice, however the table below shows the median price and price range for different sizes. This data is based on a sample of 60 smart TVs.

Table 4: Smart TV price data

Size	Median Price	Price Range
24”	£179.00	£149.00 - £189.00
32”	£199.00	£156.40 - £253.00
40”	£249.00	£229.99 - £499.00
43”	£380.00	£289.00 - £899.00
49”/50”	£463.50	£298.00 - £1,099.00
55”	£724.00	£369.00 - £1,699.00
65”	£1,099.00	£549.00 - £2,499.00

Source: Market Study of Consumer IoT Products (n=60)

The overall median price for smart TVs was £373.97. The most common television size in Amazon’s Top 50 bestselling TVs was 32”.[43]

Manufacturers and Retailers

The smart TV market is dominated by a few manufacturers, such as LG, Samsung, Toshiba, Hisense, Sony, Panasonic, Sharp and JVC. There are also smaller manufacturers in this market, such as Blaupunkt, Westinghouse and Cello. The major brands in smart TVs generally do not manufacture in the UK, but some of the smaller examples, such as Cello electronics, do still manufacture in the UK. Smart TVs can be purchased at all major retailers of electronic devices, including Amazon, Currys PC World, Argos, John Lewis and Tesco.

Security Information

- Six (10%) of the 60 smart TVs that we sampled provided some form of security information for the consumer.
- None of these gave details of **default passwords**.
- Four (7%) highlighted the importance of **security updates** in user manuals, but this did not include details of the length of time for which these would be available.
- None gave details of a **vulnerability disclosure policy**.
- Two provided details of data encryption on the retailers’ website.

[42] Ofcom (2019) ‘Media Nations: UK 2019’

[43] https://www.amazon.co.uk/Best-Sellers-Electronics-TVs/zgbs/electronics/560864 [Date Accessed: 15/01/20]

Very little security information is available for smart TVs online, with only 10% of the products reviewed providing any security information. The user manuals for products were available online in six cases (10%), and four of these did contain details of security updates but they did not state for how long updates are available. These manuals gave no information on default passwords or setting passwords, and similarly no information regarding vulnerability disclosure policies. Aside from the six (10%) cases where the retailer website did provide some form of security information in the user manual, none of the other products had any security information available online.

Smart White Goods

Price

Smart white goods can have a large price range, as reflected in the table and graph below. These items can cost thousands of pounds, depending on the manufacturer, type of product, and features. The table below shows the median price and price ranges for examples of smart white goods. These medians and ranges are based on 17 examples of washing machines/ dryers, eight examples of smart fridges, seven examples of dishwashers, and eight examples of smart ovens.

Table 5: Smart white goods price data

Product	Median Price	Price Range
Washing Machine/Dryer	£514.00	£299.00 - £1,259.00
Fridge Freezer	£2,299.00[44]	£1,199.00 - £6,999.00
Dishwasher	£709.00	£398.00 - £1,349.00
Oven	£1,099.00	£869.00 - £1,149.00

Source: Market Study of Consumer IoT Products (n=40)

It is worth noting that the price range for fridge freezers is large, with one example of such a smart device costing £6,999. However, the majority of smart fridges found in our market study cost between £1,000 and £3,000 to purchase.

Manufacturers and Retailers

The main manufacturers of smart white goods are Hotpoint, LG, Samsung, Beko, Bosch and Hoover. Smart white goods are available to purchase at major retailers, such as Currys PC World, Argos, John Lewis and B&Q.

Security Information

- Four (10%) of the 40 smart white goods that we sampled provided security information.
- None gave any details of **default passwords**.
- None of these provided details of **security updates**.
- None gave details of a **vulnerability disclosure policy**.
- Two (5%) provided details of data encryption in the user manuals for the products.
- Two (5%) gave details of unique appliance identification in the user manuals.
- One (2.5%) also referred to the importance of deleting personal information when disposing of or selling a device.

Only 10% of the smart white goods sampled had security information available online. One of those that did highlighted that the network configuration should be reset whenever a washing machine is being disposed of or sold, or when purchasing a used washing machine. The product manual for this smart washing machine also mentioned that the user is responsible for deleting any personal data stored on the device before it is disposed of.

[44] The median price, excluding the outlier was £2,099.00.

One manufacturer's smart dishwasher uses the HomeWhiz app, developed by HomeWhiz who won the inaugural IoT Security Champion Award in 2018. HomeWhiz complies with guidance documentation provided by the IoT Security Foundation (IoTSF), which includes the requirement for unique passwords, and following of IoTSF 'Vulnerability Disclosure Guidelines' to deal with vulnerabilities when they occur.[45] The information regarding the use of HomeWhiz was provided by manufacturers in user manuals that were available online, rather than directly by the retailers. Further information about the specific requirements of the IoTSF Compliance Framework are not directly provided to the consumer and would have to be independently researched.

Smart Kitchen Appliances

Price

Smart kitchen appliances can cost considerably more than regular kitchen appliances. The table below highlights the median price and price range for various types of smart kitchen appliances. Our market study included six examples of smart coffee machines, three examples of smart kettles, five examples of precision cookers, and four examples of smart thermometers.

Table 6: Smart kitchen appliances price data

Product	Median Price	Price Range
Coffee Machine	£1,457.98	£179 - £2,147
Kettle	£99.00	£67.99 - £129.99
Precision Cooker	£99.00	£69.99 - £600
Thermometer	£64.00	£32.99 - £99

Source: Market Study of Consumer IoT Products (n=18)

The price range for some of these products is relatively broad, reflecting that the devices can come with a variety of features which can significantly influence the price.

Manufacturers and Retailers

The manufacturers for smart kitchen appliances are often highly specialised. For instance, MEATER is a company that solely manufactures smart meat thermometers, and Anova Culinary only produces smart precision cookers. These are the two key manufacturers for these specific subcategories. Smart kettles and coffee machines have a wider variety of manufacturers, including large companies such as Bosch and Siemens, as well as more specialised producers, including Smarter, Melitta, and Appkettle. Smart kitchen appliances are most commonly available at major retailers such as Amazon, Currys PC World, and John Lewis.

Security Information

- Six (33%) of the 18 smart kitchen appliances that we sampled provided security information.
- None of our sample provided any details of **default passwords**.
- None provided any details of **security updates**.
- None gave details of a **vulnerability disclosure policy**.
- Five (28%) highlighted that encryption technology is used to protect users' data. Four of these cases were found on the manufacturers' website and one was found via the online retailer.
- Four (22%) of the products highlighted the users' ability to control or manage their data.

For example, one manufacturer website highlights the importance of security features and discusses the use of encryption to prevent unwanted access and control, as well as protection of

[45] https://www.homewhiz.com/security/ - This uses industry-standard authentication protocols to prevent unauthorised users from accessing connected home data.

login and user information. Larger companies provide slightly more detail about their Home Connect functions. Two larger manufacturers highlight that they perform regular checks of their systems for hackers, use the latest encryption technology, and use independent experts to regularly test their systems. They also both highlight that they have been awarded the TÜV TRUST IT “Trusted App”, which includes guarantee of encryption and data security in line with the US Federal Data Protection Act. One of these companies additionally assures that only essential data is saved on their Home Connect server, and that a firewall on the server and password protection for the Home Connect App ensures users’ security.

The information online also highlights that it is possible to reset appliances to factory settings so that network settings and accounts are separated from the appliance, however it is not clear whether resetting in this way will result in the device returning to a default password.

Of the 18 products that were sampled, no security information was found on the retailers’ websites. None of the sample highlighted any details of default password settings, security update details, or vulnerability disclosure policies.

Connecting the Home

This product group includes devices that can be found around the house to provide monitoring, connectivity, and automation, including smart thermostats, smart home assistants and speakers, smart security cameras, smart doorbells, smart door locks, smart alarms and sensors, smart baby monitors, and additional household appliances. The total average price for this product group is £113.74, with a price range of £14.95 (mini smart speaker) to £449.99 (smart security camera). This is the lowest price range of the three product groups.

Overall, the only top three UK CoP guideline to be included within this product group sample was vulnerability disclosure policy, for which 7% of the connecting the home sample provided this information. Details of vulnerability disclosure policies were found within four of the nine device categories of this product group. There were no mentions of security updates or default passwords found within this sample.

Smart Thermostats

Price

The prices for these devices can vary depending on the features and level of control provided by the product. The table below is based on data from 12 examples of smart thermostats.

Table 7: Smart thermostat price data

	Price
Price range	£20.29 - £175.99
Median	£113.49
Mean	£108.22

Source: Market Study of Consumer IoT Products (n=12)

Manufacturers and Retailers

Many of the manufacturers of smart thermostat technology are highly specialised. Examples include Drayton Controls, tado°, MOES, and SALUS Controls, which only produce heating control technology. Companies such as Hive and Google produce smart thermostats alongside other smart technology products. Online retailers for these products include Amazon, Currys PC World, B&Q, and ScrewFix, and in some cases they are also available for purchase directly from the manufacturers.

Security Information

- Six (50%) of the 12 smart thermostats that we sampled provided some form of security information.
- None of our sample provided any details of **default passwords**.
- None provided any details of **security updates**, or for how long these would be available.
- One (8%) of the manufacturers gave details of a **vulnerability disclosure policy** on their website.
- Two (16%) highlighted the use of encryption technology, one via the manufacturers' website and one in a user manual.
- Three (25%) manufacturers highlighted their commitment to keeping personal data secure but did not specifically cite encryption technology as a method for ensuring this.

On their websites, six of the manufacturers included in this sample recognise the importance of security and highlight steps taken to keep their customers safe. These often include encryption of data and the ability to factory reset devices to remove personal data when required by users. In five cases this information was provided via the manufacturers' website, and in one case in the user manual for the product. Only one manufacturer provided details of a vulnerability disclosure policy and none reference default passwords or security updates for the products.

Online retailers provide limited information regarding security of smart thermostat technologies, with most not including any information at all. In only one case (8% of the sample) was the user provided with any security information and this was via a user manual rather than directly. This example detailed the use of encryption technology to protect users' data but did not include any of the top three CoP security features. This situation is similar when consumers go to physically purchase these products in store, with devices in our sample including no details of security on their packaging, despite providing information online.

Smart Home Assistants

Price

The price of smart home assistants ranges substantially depending on the specific model, functions, and quality of the audio included. The table below reflects the extent of this price range from the eight smart home assistants sampled.

Table 8: Smart home assistant price data

	Price
Price range	£24.99 - £299.00
Median	£114.50
Mean	£139.50

Source: Market Study of Consumer IoT Products (n=8)

Manufacturers and Retailers

Key manufacturers for smart home assistants include Amazon, Google, and Apple. These are available to purchase directly from the manufacturers, but also from large retailers such as Currys PC World, Argos, Maplin, B&Q, and John Lewis.

Security Information

- Five (63%) of the eight smart home assistants that we sampled provided some form of security information.
- None of our sample provided any details of **default passwords**.
- None provided any details of **security updates**, or for how long these would be available.
- None of the manufacturers gave any details of a **vulnerability disclosure policy**.

- All of the details provided were in relation to data collection and storage and did not address any of the top three CoP guidelines. In two cases this was found via the retailers' website and in three cases via the manufacturer website.

When searching for security information online, one manufacturer provides extensive detail relating to privacy and data collection. This particularly focuses on the storing and sharing of video footage and audio which is collected by home assistants. This is only available to consumers via the manufacturers' websites and was not included on the retailers' websites sampled. Another manufacturer similarly provides privacy details relating to managing audio and video settings of their products, and this is included when consumers purchase directly from the manufacturer. It seems, however, that neither of these manufacturers provide details of default passwords, or for how long their product will receive security updates. While the first manufacturer has a company vulnerability disclosure policy, there are no details of this available via their 'home assistance' device webpages, meaning that consumers are not currently provided with this information at the point of sale.

Our physical market study similarly highlights that there is limited security information available to consumers on product packaging. For instance, two smart home assistants reviewed highlight that the camera and microphone of the smart home assistant can be easily switched off, but the possibility remains that an attacker could simply switch these functions back on. Moreover, there are no details of security updates, default passwords for the device, or vulnerability disclosure. Another product that was reviewed did not include any security information on its physical packaging at all.

Smart Speakers

Price

The price of smart speakers can vary considerably depending on the functions included and the quality of audio provided. The table below reflects examples from a sample of 20 smart speakers.

Table 9: Smart speaker price data

	Price
Price range	£14.95 - £409.00
Median	£149.00
Mean	£192.67

Source: Market Study of Consumer IoT Products (n=20)

Manufacturers and Retailers

Most manufacturers of smart speakers specialise in sound technology, with examples including Sonos, Bose, Majority, Zolo, KitSound Audio, AZATOM, Roberts Radio, and JBL. Manufacturers who also produce other products include Samsung, LG, Yamaha, and Apple. The key retailers of these products include Amazon, Currys PC World, and John Lewis.

Security Information

- Six (30%) of the 20 smart speakers that we sampled provided some form of security information.
- None of our sample provided any details of **default passwords**.
- None provided any details of **security updates**.
- One manufacturer gave details of a **vulnerability disclosure policy**, covering 15% of the sampled products.
- Three (15%) of the examples where security information was provided consisted of details of secure storage of data and users' ability to manage information collection.

- One example (5% of the sample) gave details of how to remove personal data from the device.

Six of our sample (30%) of devices had manufacturers which provided security information online, with Bose, for example, outlining a vulnerability disclosure policy. As noted above, 15% of the sample simply highlighted information about the collection of data in a privacy policy statement, but did not outline any of the top three CoP security measures.

Very little security information is available online via retailers for smart speakers. Of the 20 products and three online retailers sampled, no security information was provided at the point of sale via retailer websites. When shopping for these products in stores, consumers will similarly find limited security information, with no mention of the above details found in our sample of four devices in stores.

Smart Security Cameras

Price

Due to the many additional features, varying camera quality, and use both inside and outside the home, the prices of smart security cameras can vary significantly. The table below reflects this, highlighting prices of low, medium, and high range products. These examples were taken from a sample of 19 smart security cameras.

Table 10: Smart security camera price data

	Price
Price range	£24.99 - £449.99
Median	£39.99
Mean	£103.31

Source: Market Study of Consumer IoT Products (n=19)

The majority of smart security cameras found as part of our market study were in the lowest price range of £25 to £125.

Manufacturers and Retailers

There are several different manufacturers of smart security cameras, with many specialising in this subcategory of smart technology. Manufacturers that are dedicated to smart home security products include Blink and Ring, both owned by Amazon, Neos, Wansview, Arlo, and blurams. Other manufacturers of these devices include Google, Victure, and TP-Link. Retailers of these products include Amazon, John Lewis, Currys PC World, Maplin, ScrewFix, and B&Q.

Security Information

- Nine (47%) of the 19 smart speakers that we sampled provided consumers with some form of security information.
- None of our sample provided any details of **default passwords**.
- None provided any details of **security updates**.
- None gave any details of a **vulnerability disclosure policy**.
- In seven cases (37%), the only security information provided to consumers on retailers' websites was the use of encryption.
- Two manufacturers provided details of users' privacy, highlighting secure storage of information and consumers' access to their data.

Two of the manufacturer's websites (covering 16% of the products sampled) highlight security details such as encryption technology and cloud storage, as well as their privacy policies relating to accessing videos by users and third parties. So, while manufacturers do provide some security information for these products, this did not include any details of the top three CoP guidelines, including default password settings, security updates, or vulnerability disclosure policies.

Some online retailers do highlight product security details such as the length of time that videos are stored, and how these are stored securely. Details such as these were included for 37% of the products reviewed, on retailers' websites. The FAQ document available for one manufacturer's products via the retailer's website also highlights that each camera has its own secret key and certificate to ensure that its identity can be securely validated.

Our market study of stores suggests that there is limited information relating to security when consumers purchase these devices in person. Plaques detailing the product information highlight the many features but do not mention any security information. This was the case for the three smart security cameras that we reviewed in stores.

Smart Doorbells

Price

Compared to some types of smart product, smart doorbells have a relatively narrow price range. This is reflected in the table below. These figures have been calculated from 11 examples of different smart doorbells.

Table 11: Smart doorbell price data

	Price
Price range	£52.99 - £229.00
Median	£79.99
Mean	£99.89

Source: Market Study of Consumer IoT Products (n=11)

The majority of smart doorbells on the market cost less than £100.00 to purchase.

Manufacturers and Retailers

One of the earliest smart doorbells on the market was manufactured by Ring, and this is still one of the key producers in this subsection of smart technology. While Ring does still dominate the manufacturing of smart doorbells, there are several smaller producers, including Accfly, YINXN, YIROKA, Innotic, and Victure. There are a range of retailers that sell smart doorbells, including Amazon, B&Q, Maplin, John Lewis, Argos, ScrewFix, The Electrical Showroom, Very, and Littlewoods.

Security Information

- Three (27%) of the 11 smart doorbells that we sampled provided consumers with some form of security information.
- None of our sample provided any details of **default passwords**.
- None provided any details of **security updates**.
- One manufacturer did give details of a **vulnerability disclosure policy**, covering 27% of the products sampled.
- One (9%) of the products included in the study provided details of a tamper alarm which would be set off if the device was illegally disassembled. This was included on the retailers' website.

There was limited security information for smart doorbells both on manufacturers' websites, retailers' websites, and in stores. One manufacturer provides information online relating to the storage and security of the videos recorded by their devices, highlighting measures such as rigorous security reviews, secure software development requirements, and encryption of communication between their devices and cloud servers.

It is noted that users can access and delete stored recordings if they subscribe to a Protect Plan. There is also a vulnerability disclosure policy in place, with a page on their website that provides an email address to contact if any security issues are discovered. This information was available via the manufacturers' website. No other manufacturers provided any details relating to the top three CoP points.

The key smart doorbell online retailers such as Amazon, B&Q, Maplin, and John Lewis provide little to no security information, depending on the specific product being reviewed. In one case the retailer gave details of a tamper alarm included in the product to prevent illegal disassembling. None of the online retailers for any of the 11 products reviewed give any details of default passwords, for how long security updates will be available, or vulnerability disclosure policies.

Of the devices in our sample reviewed in stores, there was no security information on the products' physical packaging, despite information being available online.

Smart Door Locks

Price

As with smart doorbells, the price range for smart door locks is relatively narrow. These figures have been calculated from data collected for nine different examples of smart door locks.

Table 12: Smart door lock price data

	Price
Price range	£75.00 - £259.00
Median	£198.99
Mean	£198.99

Source: Market Study of Consumer IoT Products (n=9)

Most of the smart door locks on the consumer market are between £100.00 and £200.00 to purchase.

Manufacturers and Retailers

Some manufacturers of smart door locks have created these products as extensions of their business as traditional lock manufacturers. Examples of these include Yale and Kwikset, which both still produce traditional locks alongside smart door locks. Many other smart lock manufacturers are specialised manufacturers, and examples of these include NUKI, We.lock, ZKTeco, and Ultion. Retailers of smart door locks include B&Q, The Electrical Showroom, Amazon, ScrewFix, Wickes, Argos, and John Lewis.

Security Information

- Six (67%) of the nine smart door locks that were sampled did provide consumers with some form of cyber-security information.
- None of our sample provided any details of **default passwords**.
- None provided any details of **security updates**.
- None gave any details of a **vulnerability disclosure policy**.
- Two (22%) highlighted the use of encryption as a security feature, through the retailers' website.
- Two (22%) manufacturers also gave consumers details about the security features used in sharing and storing their data.

In two cases (22%) we found manufacturers emphasising the importance of data encryption, as well as user authentication processes and master codes, which restrict users from adding or changing existing codes. However, there do not seem to be any details relating to how long the product will receive security updates for, default passwords, or any mention of vulnerability disclosure policies.

When purchasing these products online, consumers are provided with varying levels of security information depending on the product and retailer. Most retailers provide details of encryption to ensure security, as well as tamper alarms included in the product settings. Some highlight the ability to reset the device to factory default settings if necessary.

Smart Alarms and Sensors

Price

The table below shows the median price and price range for the three main types of smart alarms and sensors. The price range for these types of smart products is relatively narrow when compared to some other categories of smart goods.

Table 13: Smart alarm price data

Product	Median Price	Price Range
Motion Detector/ Burglar Alarm	£28.58	£21.00 - £39.99
Smoke Alarm	£89.99	£23.89 - £109.95
Water Leak Detector	£33.44	£23.99 - £59.04

Source: Market Study of Consumer IoT Products (n=19)

These prices are based on nine examples of smart motion detectors, five examples of smoke alarms, and five examples of smart water leak detectors. The majority of smart alarms and sensors cost less than £100.00 on the consumer market.

Manufacturers and Retailers

The key manufacturers of smart alarms and sensors are similar to manufacturers of other smart security products, such as smart doorbells, smart security cameras, and smart door locks. These include Ring, Hive, Yale, Nest, Panasonic, Samsung, and Bosch. The retailers of these products are also similar, with Amazon, B&Q, Screwfix, Argos, Currys PC World, and John Lewis all stocking various smart alarms and sensors.

Security Information

- In 12 (63%) of the 19 smart alarms and sensors that were sampled, consumers were provided with some form of security information.
- None of our sample provided any details of **default passwords**.
- None provided any details of **security updates**.
- In two cases (11%) manufacturers gave any details of a **vulnerability disclosure policy** on their website.
- Two (11%) of the products had details of encryption as a security measure included on the retailers' website.
- Eight (42%) of the sample simply saw manufacturers providing details of data collection and the security of this data storage. This was in seven cases included on manufacturers' websites and in one case in a user manual.

In 53% of the smart alarms sampled, manufacturers provided some security information on their websites. In 42% of cases this simply consists of generic information about the collection of personal information and data, including how this is collected and who it is shared with. Some manufacturers such as Nest and Ring, covering 11% of products sampled, go into detail about the specific measures for protection of data.

Online retailers of smart alarms and motion sensors do not tend to provide security information for these products. Security information was provided on retailers' websites in three cases (16%). However, there is no information available to consumers via online retailers about default passwords, for how long the product will receive security updates, or about vulnerability disclosure policies.

It appears that when purchasing these goods in person, consumers are also provided with limited security information. The products reviewed in store as part of our sample did not include any details of security on the packaging, despite information being available online.

Smart Baby Monitors

Price
The table below reflects the range of prices for smart baby monitors. These examples have been taken from a sample of 16 different smart baby monitors. The differences in price are determined by the varying features, including the picture quality of products.

Table 14: Smart baby monitor price data

	Price
Price range	£17.99 - £145.00
Median	£29.79
Mean	£49.14

Source: Market Study of Consumer IoT Products (n=16)

While some smart baby monitors cost more than £100.00 to purchase, the majority are priced below this threshold.

Manufacturers and Retailers
Many manufacturers of smart baby monitors are also smart security camera manufacturers, with examples including Victure, Wansview, Netvue, CACAGOO, HeimVision, and Nooie. Other less specialised manufacturers include BT and Motorola. Smart baby monitors are available to purchase at many retailers, including Amazon, John Lewis, Currys PC World, Maplin, and Argos.

Security Information

- Nine (56%) of the 16 smart baby monitors that were sampled, provided some form of security information.
- None of our sample provided any details of **default passwords**.
- None provided any details of **security updates**.
- No details of **vulnerability disclosure policies** were found in our sample.
- All nine examples (56%) of security information were related to encryption to ensure users' data is secure. In seven of these cases the details were provided directly on retailers' websites, and in two cases these were mentioned on manufacturers' websites.

Most manufacturers appear to provide no security information on their websites. HeimVision and Nooie, accounting for 13% of the sample products, highlight security measures such as encryption to ensure the safety of consumers' data. However, there were no examples of manufacturers providing any detail of default passwords, security updates for their products, or vulnerability disclosure policies.

Some online retailers do provide security information for some of their smart baby monitors. This was the case for seven (44%) of the sample and usually includes details of encryption technology to ensure data protection, cloud storage, and the fact that access to video files is limited to the user's account.

Additional Household Appliances

Price

The table below shows the median price and price range for each type of product within the subcategory of additional household appliances, from a sample of 29 products.

Table 15: Smart household appliances price data

Product	Median Price	Price Range
Vacuum Cleaners	£249.00	£199.99 - £352.23
Projectors	£129.98	£69.99 - £369.95
Printers	£147.91	£44.00 - £162.27
Lamps and Lighting	£43.98	£18.99 - £75.00
Essential Oil Diffusers	£51.49	£29.99 - £219.98
Clocks	£79.99	£36.99 - £147.60

Source: Market Study of Consumer IoT Products (n=29)

These medians and ranges are based on data collected for five examples of smart vacuum cleaners, five smart projectors, five printers, seven examples of lamps/ lighting, four different essential oil diffusers, and three different smart clocks.

Manufacturers and Retailers

The major retailers for these smart household appliances include many of the typical retailers of smart products, such as Amazon, Argos, Currys PC World, and Maplin. The key manufacturers of these products vary by category. Manufacturers of smart vacuum cleaners are generally specialised and include iRobot, Bagotte, Eufy, and Neato Robotics. Manufacturers of projectors include Jinhoo, Nebula, and VicTsing. The key manufacturers of smart printers include HP, Canon, and Epson, all companies that also manufacture regular printers. The manufacturers of lamps and lighting, essential oil diffusers, and clocks, are all smaller companies that are generally specialised in their specific area of smart technology.

Security Information

- Eight (28%) of the 29 additional household appliances that were sampled provided some form of security information.
- None of this sample provided any details of **default passwords**.
- None of these products gave details of **security updates**.
- No details of **vulnerability disclosure policies** were found in this sample.
- One (3%) of the sample gave details of how to delete personal information when disposing of or reselling the device. This information was included in the user manual.
- Two (7%) of the 29 appliances mentioned password protection for the wireless connection in the user manuals.
- Three (10%) highlighted the use of encryption technology to protect customers' data.
- In two cases (7%) manufacturers' websites gave details of data collection and protection through secure storage and limited access.

The most comprehensive security information in this category is given by the manufacturers of smart printers. One smart printer user guide, which is accessible online, emphasises the importance of deleting personal information when the printer is given away or disposed of and directs users on how to do this. Another manufacturer's smart printer manual, found via an online retailer, addresses the issue of password protection. It highlights that the default setting for the Wi-Fi Direct connection security is 'Manual' rather than 'Automatic', meaning that the password is changed by the user when the printer is set up. However, the ‘Automatic’ option for Wi-Fi Direct does involve the use of a default password, which cannot be changed.

Of this sample of 29 smart household appliances, 72% did not have any security information available via the online retailers. No information was available for the smart vacuums and projectors in the sample. No online retailers gave any details about default passwords, how long the product will receive security updates for, or vulnerability disclosure policies.

The physical market study also suggests that information relating to device security is scarce when purchasing these products in person rather than online. We were able to sample smart printers and smart lighting in physical stores. The two examples of smart lighting products that were analysed did not include any security information on their packaging, and this was also the case for the smart printer.

Consumer Lifestyle devices

This product group includes ‘lifestyle’ devices such as smartphones, tablets, smart watches and health trackers, and smart toys. The average overall price for this product group is £206.30 and the price range is £13.40 (smart health thermometer) up to £1,199.00 (smartphone). This is the lowest average of the three product groups, as the inclusion of products such as smart health tracking products and smart toys has reduced the mean. The price range is higher than connecting the home due to the inclusion of higher priced products such as smartphones.

This was the product group with the most security information provided to consumers, with information on both security updates and vulnerability disclosure polices found within the sample. However, the details on security updates covered just 6% of the consumer lifestyle sample, and vulnerability disclosure policies covered 8% of this product group. Details of at least one of the top three UK CoP guidelines was found within each of the device categories, being security updates for smartphones, smart tablets, and smart watches and health monitoring, and vulnerability disclosure policies for smart toys.

Smartphones

Price

The price of smartphones can vary significantly depending on factors such as brand popularity, amount of data storage space, camera quality, and screen size and quality. The graph and table below reflect this range in prices, based on 20 examples of different smartphones. A YouGov survey of the most popular mobile phone models in the UK showed that there are over 100 different smartphone models on the market.[46] The sample of 20 used for this market study therefore represent only some of the products available, but includes products from a range of producers and price bands.

Table 16: Smartphone price data

	Price
Price range	£59.98 - £1,199.00
Median	£209.99
Mean	£364.94

Source: Market Study of Consumer IoT Products (n=20)

[46] https://yougov.co.uk/ratings/technology/popularity/phone-models/all

Overall, 12 of the 20 examples analysed for this market study can be purchased for less than £310. However, these tend to be older models, and many newly released phones, and those with more storage, can be priced at a far higher value.

Manufacturers and Retailers

Research into the UK mobile phone market reflects that there are nine key smartphone producers in the market, including Apple, Samsung, RIM, HTC, Nokia, Sony Ericsson, Motorola, Google, and LG.[47] Apple has the majority share of the mobile device market, with a 49.24% share in 2019. Smartphones are available to purchase at many online retailers, including Currys PC World, Amazon, Argos, John Lewis, Carphone Warehouse, Very, and Littlewoods.

Security Information

- 16 (80%) of the 20 smartphones that were sampled provided some form of security information.
- None of this sample provided any details of **default passwords**.
- Three (15%) of these products highlighted the importance of **security updates**, but none gave any details about for how long the product would receive them. These details were provided in the user manuals for the products, all of which were Samsung devices.
- No details of **vulnerability disclosure policies** were found in this sample.
- Seven (35%) highlighted the use of password protection, fingerprint sensor, or face recognition technology, as a key form of security for users. In four cases this information was included in the user manual, and in three examples these details were included on the retailers' website.
- Six (30%) of the sample highlighted security in terms of the storage of users' personal information, and the measures used to keep this data secure.

Manufacturers that covered 80% of the products included for this sample had some security details included online. This largely included an outline of what information is collected by the company, as well as the users' control over data sharing through application permissions and limiting the sharing of personal data with the manufacturer.

In eight examples (40% of the sample), the online retailer provided some security information, whether this was directly on the website or by providing a user manual. Some online retailers provide more security information than others. For instance, one user manual included on a retailer's website included details of security updates. It highlighted the importance of these updates to users and suggested that they regularly check for updates, as well as informing users that emergency security updates will be installed automatically. However, it did not include information about how long the device would receive these security updates for. Most retailers do not include any details of security updates for the products they are selling, with only three examples where this was provided. There were no cases where the retailers' website discussed default passwords or vulnerability disclosure policies.

Security information for smartphones is often limited in stores, particularly as there is usually no access to the physical phone boxes on display. Consumers typically interact with a sample model phone with information plaques rather than the phone box itself. These plaques often provide details of the phone's features but no security information. When mentioned, security details are usually limited to features such as touch ID and face ID. This was the case in four stores that were included in our physical market study.

[47] https://www.statista.com/statistics/487780/market-share-of-mobile-device-vendors-uk/

Smart Tablets

Price

As with smartphones, the prices of tablets can vary depending on factors such as screen size and quality, data storage, and camera quality. The graph and table below reflect this range of prices and are based on 22 different tablets.

Table 17: Smart tablet price data

	Price
Price range	£49.99 - £1,079.00
Median	£154.98
Mean	£308.60

Source: Market Study of Consumer IoT Products (n=22)

As is the case with smartphones, tablets are most commonly within a relatively lower price range. However, there are much higher priced examples, these often being newer releases and devices with more storage space.

Manufacturers and Retailers

The key manufacturers of smart tablets are similar to the smartphone manufacturers highlighted above. These include Samsung, Apple, and Huawei, with tablets also manufactured by Amazon, Microsoft, Linx, and Lenovo. The main retailers of these products are also similar to those for smartphones, and include Amazon, Currys PC World, Argos, Carphone Warehouse, and John Lewis.

Security Information

- 15 (68%) of the 22 tablets that were sampled had some form of security information available to consumers.
- None of this sample provided any details of **default passwords**.
- One (5%) of these products highlighted the importance of **security updates** in the user manual, but this did not include any details of for how long these would be provided.
- No details of **vulnerability disclosure policies** were found in this sample.
- Two (9%) of the sample highlighted the use of encryption to protect users' data. This information was included on the retailers' website.
- Three (14%) highlighted the use of password protection, fingerprint sensor, or face recognition technology, as a key form of security for users. In one case this information was included in the user manual, and in two examples these details were included on the retailers' website.
- Five manufacturers (23%) provided details of security on their websites, covering 15 (68%) products within the sample. These highlight what data is collected from users' and measures used to protect this through secure storage and limited access.

As with smartphones, the manufacturers of tablets often do provide security and privacy information online. This typically involves an outline of what personal information is collected, as well as privacy policies detailing data sharing policy, which can be found on manufacturers' websites. However, there appears to be no reference to default passwords, for how long products will receive security updates, or details of vulnerability disclosure policies.

User manuals are not consistently provided by online retailers, meaning that some products do not have any details of security information. In one instance the online retailer included the user manual of a product, which provided some information, including that performance and security updates are installed automatically for the product. However, it does not give any details about how long the product will receive these security updates for. In four instances (or 18%) the online retailer directly provided some security details, and these included encryption technology and password protection/ face identification. None of the online retailers gave any details of default passwords or vulnerability disclosure policies.

Security information in stores was limited in a similar way to smartphones, as consumers typically interact with a sample model rather than the product box itself. The information plaques often provide details of the features but no security information. When mentioned, security details were limited to features such as touch ID and face ID. This was also the case for smart tablets in the four stores that were included in our physical market study.

Smart Watches and Health Monitoring

Price
The price of health monitoring devices usually depends on the type, complexity, and various functions of the device.

Table 18: Smart watches and health monitoring price data

Product	Median Price	Price Range
Smart watch/wristbands	£104.00	£39.99 - £379.00
Smart scales	£89.98	£49.99 - £116.85
Other smart health trackers	£32.86	£13.40 - £47.28

Source: Market Study of Consumer IoT Products (n=22)

This data is based on 11 examples of smart watches/ wristbands, six examples of smart scales, and five other smart health trackers, including thermometers and otoscopes.

Manufacturers and Retailers
These smart watches and health monitoring devices are typically manufactured by large and well-known brands such as Fitbit, Apple, Samsung, and Huawei. They are sold by major retailers such as Amazon, Curry's, Argos, John Lewis, Decathlon, Withings (Nokia), and Qardio. Outside of these well-known brands, there are many other manufacturers ranging from mid-sized manufacturers to smaller companies that sell mainly through online marketplaces such as Amazon.

Security Information

- Seven (59%) of the 22 smart watches and health trackers that were sampled had some form of security information available to consumers.
- None of these provided any details of **default passwords**.
- One (5%) of the sample highlighted the importance of **security updates** in the user manual, but this did not include any details of for how long these would be provided.
- No details of **vulnerability disclosure policies** were found in this sample.
- Two (9%) of the sample products highlighted the use of encryption to protect users' data. This information was included in one case on the retailers' website and in one instance in the user manual for the product.
- One (5%) of the devices gave details of how users can delete their personal data in the user manual.
- Four manufacturers (covering 36% of the products sampled) provided details of data security on their websites, where they highlight what data is collected, the measures used to protect this, and the level of control consumers have over their data.

Manufacturers of smart watches and health monitors in 36% of our sample provided security information through their websites. Security information ranges from: details of secure data communication; securely stored data in encrypted form; making it easy for consumers to delete their personal data; and keeping software updated through automatic installations. Details of software updates did not include information about the length of time that security updates would be available for, and there was no mention of default passwords or vulnerability disclosure policies.

In four cases (18%) there was some form of security information provided by online retailers. This includes three instances (or 14% of the sample) where details of security updates, data encryption, and deleting personal information were provided through online user manuals. Our market study of physical purchases similarly suggests that there is limited security information available to consumers in stores.

Smart Toys

Price
The price of these products can vary significantly, with robots/action figures being the most expensive subcategory. This data is based on six examples of drones, eight examples of robot/action figures, and five examples of kids' smart digital photography cameras.

Table 19: Smart toys price data

	Price
Price range	£16.99 - £145.99
Median	£41.99
Mean	£58.45

Source: Market Study of Consumer IoT Products (n=20)

It is worth noting that high-quality photography drones can become far more expensive than this price range indicates. Our research into drones was limited to those products specifically aimed at children, which is reflected in the relatively low price range above.

Manufacturers and Retailers
Manufacturers of smart toys consist largely of businesses with no online presence other than on online marketplaces, such as Amazon. Some smart toys are available to purchase at other retailers including Maplin, Argos, and John Lewis.

Security Information

- Seven (35%) of the 20 smart toys that were sampled included some form of security information available to consumers.
- None of these provided any details of **default passwords**.
- None of the sample gave any information about **security updates**.
- Two manufacturers gave details of **vulnerability disclosure policies**, which were found on the manufacturers' websites. These vulnerability disclosure policies covered seven (or 35%) of the products reviewed.
- These manufacturers also detailed the use of encryption technology to protect users' data.

Despite the large number of manufacturers of smart toys, few had any security information available. Many of these manufacturers had no online presence other than Amazon, meaning that for 65% of the products sampled, there was no security information available. The largest toy robot manufacturer did provide some information. While the details it provided did not fully meet the consumer IoT CoP, it did mention a vulnerability disclosure policy, secure communication through encryption, the ability for consumers to delete personal data, GDPR compliance, and securely storing sensitive data. None of the security information detailed by smart toy manufacturers included any details of default passwords or security updates.

None of the smart toys sampled had any security information included on the retailers' websites.

Meeting the three Codes of Practice

The market study explored whether the devices sold met the top three Code of Practice guidelines of:

1. **All device passwords must be unique and not resettable to a factory default;**
2. **Device manufacturers must provide a public point of contact as part of a vulnerability disclosure policy to report vulnerabilities and act on these in a timely manner; and**
3. **Manufacturers must explicitly state the minimum length of time for which the device will receive security updates.**

Devices sold in the UK with default passwords

Our market study suggests that there is very little information that is easily available to consumers regarding default passwords when purchasing consumer IoT products. There were no cases found within the market study sample that explicitly highlighted that a device used default passwords. However, there were also no examples where the avoidance of default passwords was highlighted specifically to consumers as a security feature.

Research[48] investigating the communication of security features of consumer IoT products in user manuals and support pages highlights how many of the 270 devices reviewed included information on the prevalence of default passwords. Among the 170 that provided any information on security features (in manuals or online), only 5% were sold stating that they had a default password, and 78% gave details requiring users to create login credentials or a pin instead of using a default password. There was no information available for 100 of the devices, meaning that consumers would not know whether these have a default password or not. This research therefore suggests that a minimum of 3% of devices are sold with a default password, but this could potentially be higher as many devices do not provide any information to consumers. Moreover, with those that gave information about setting up an account, it was not necessarily clear whether this was required in order to operate the device, or whether consumers could still use the device with a default password by opting out of creating a login.

It is worth noting the differing methodology used for this study, where the process included a specific search for a ‘manual’ or ‘guide’ for each device. In contrast, our study included analysis of user manuals only where these were provided for consumers by retailers or directly on manufacturers’ websites. It can therefore be seen that while this information may be available to consumers when they choose to search for it, it is often not provided at the point of purchase.

As this issue is one that is often not directly addressed by manufacturers or retailers, it is currently very difficult to provide an estimate of the numbers of devices in the UK market that are sold with default passwords. Where this is addressed, it is not in a way that is easily accessible to consumers, and therefore cannot be consistently used to inform decision making when purchasing devices.

[48] Blythe JM, Sombatruang N, & Johnson S (2019) ‘What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?’

Case study – Mirai

One of the most notorious and well-known IoT security threats is Mirai malware.[49] The original Mirai code exploited a vulnerability in devices such as digital video recorders (DVRs), which were used to mount Distributed Denial of Service (DDoS) attacks against the Domain Name Service provider Dyn in 2016. Mirai Botnets or variations of Mirai were also used to attack the KrebsonSecurity website and phone company Deutsche Telekom.

How was the vulnerability exploited?

Mirai accesses devices to create a Botnet through exploiting factory default or generic credentials, i.e. the code for Mirai contains a list of usernames and password combinations to access devices. The first item of the CoP is that all IoT device passwords shall be unique and not resettable to any universal factory default, which would have prevented access to devices from easily guessable default usernames and passwords. Most of the devices used in the Dyn attack were DVRs. It is estimated that around 100,000 devices were used in the 2016 Dyn attack which led to many high-profile services such as Twitter and Netflix being unavailable for nearly a day.

Who was affected and possible future attacks?

Project rIoT at UC Berkeley has a cost estimator for this type of attack. It puts the overall total consumer resource cost of the Dyn attack at US$115,308 (around £87,819), and the cost per device as US$1.08 (£0.82).[50] This is based on the cost of electricity and internet bandwidth, and does not take into account other costs.

A recent review of security information and manuals for 270 devices available in the UK suggests 4.7% of products are supplied with default passwords[51] which may make them vulnerable to this type of attack in the future, unless better password security is built into new devices.

Most of the owners of IoT devices that have been compromised in this way will most likely never know, as the vulnerability is exploited to attack a third party. However, they may be subject to 'attack to defend' attacks, such as 'BrickerBot', which was released following Dyn. This 'bricked' Mirai infected devices, rendering them useless to the attacker, but also the owner, by wiping device drives and Flash storage as an aggressive response to Mirai. The infected IoT device owners may also be inconvenienced by DDoS attacks if they are unable to access websites.

The impact on third party targets of attacks could be very costly and serious. In 2015, two Ukrainian power plants were attacked by hackers, leading to power cuts affecting more than 80,000 people for between one and six hours, additionally mounting DDoS attacks on call centres to prevent consumers from accessing information on the blackout.[52]

A 2016 report[53] looked at the costs of a well-resourced and carefully developed attack on the electricity distribution network in the south and east of England and impacts on UK Critical National Infrastructure. The economic losses to sectors are in the range of £11.6 billion to £85.5 billion in the different variants of the scenario. The overall GDP impact of such an attack was estimated between £49 billion to £442 billion across the entire UK economy in the five years following the outage, when compared against baseline estimates for economic growth. The scenarios tested range from three to twelve weeks leaving between 8.9 million and 13.1 million people without power, and would include socio-economic impacts such as panic buying and a decrease in productivity as workplaces close and people are unable to get to work.

[49] See for example https://securityintelligence.com/news/leaked-mirai-malware-boosts-iot-insecurity-threat-level/

[50] UCB IoT DDoS Consumer Cost Calculator https://groups.ischool.berkeley.edu/riot/

[51] Blythe J, Sombatruang N & Johnson SD (2019) 'What security features and crime prevention advice is communication in IoT manuals and support pages?' Journal of Cyber Security

[52] Zetter K (2016) 'Everything we know about Ukraine's Power Plant Hack' Wired

[53] Kelly S, Leverett E, Oughton EJ, Copic J, Thacker S, Pant R, Pryor L, Kassara G, Evans T, Ruffle SJ, Tuveson M, Coburn AW, Ralph D & Hall JW (2016) 'Integrated Infrastructure: Cyber Resiliency in Society, Mapping the Consequences of an Interconnected Digital Economy' Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge.

Devices sold in the UK with vulnerability disclosure policies

Details of vulnerability disclosure policies were found to be the most commonly provided of the top three CoP guidelines in our market study. Nonetheless, these were still relatively rare. Details were provided in no cases within the product group 'big ticket items', in only 7% of the 'connecting the home' sample, and in 8% of 'consumer lifestyle' products. The subcategory where vulnerability disclosure policies were most commonly provided was smart toys, with 35% of the products in our sample being covered by a disclosure policy. This was followed by smart doorbells, with 27% of the sample being covered, and smart speakers at 15%.

Where found, details of vulnerability disclosure policies were provided exclusively on manufacturers' websites. It is worth noting that details of these policies were never provided directly to consumers by retailers, and they would therefore have to be researched independently by the consumer.

Other research[54] suggests a slightly higher level of information on vulnerability disclosure policies, with materials for 32% of the products reviewed detailing a vulnerability disclosure policy. However, it was similarly noted that this information was usually provided on the manufacturers' website.

Devices sold in the UK with security update information

Security update information was found to be the second most common of the top three Code of Practice guidelines to be highlighted to consumers in our market study, after vulnerability disclosure policies. Security update information was provided in four of the 16 device subcategories, and overall for 3% of the big ticket item sample, in no cases within connecting the home, and for 6% of the consumer lifestyle sample. In total, only 2% of the market study sample gave any details of security updates.

These figures reflect that very few consumer IoT devices are sold with any information on security updates. In none of these cases were the consumers given any detail of how long these updates would be available. It is also important to note that all instances of security update information were found in user manuals included on retailers' websites, and it is unclear how many consumers would take time to read these, or how thoroughly they would do so.

As above, the Blythe et al research[55] highlights how many of the devices reviewed included information on software or firmware updates within manuals and support pages. This was found to be discussed in 62% of the sample, however, security updates specifically were only mentioned in 10% of cases. Moreover, as in our market study, there were no cases where it was detailed for how long these security updates would be provided.

[54] Blythe JM, Sombatruang N, & Johnson S (2019) 'What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?'

[55] Blythe JM, Sombatruang N, & Johnson S (2019) 'What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?'

Case study – VxWorks

How did the vulnerability occur?

In July 2019 security researchers found 11 vulnerabilities, subsequently named URGENT/11, in the VxWorks OS that runs on more than 2 billion devices worldwide, mostly including medical and industrial devices, but also on some consumer IoT devices, such as smart doorbells. VxWorks is the most widely used real-time operating system in the world.[56]

A few weeks after the initial discovery, similar vulnerabilities were found affecting a hospital infusion pump that did not run on VxWorks. It was subsequently found that the vulnerability is in the original IPnet code developed in the early 2000s, which was licensed to an array of customers. In 2006 the developer of VxWorks acquired the developer of the original IPnet code and dissolved the company, meaning that there was no longer any software support for IPnet licences.[57] This meant that the existing bugs remained, with IPnet users unaware of them.

How could the vulnerability be exploited?

Six of the vulnerabilities were classified as critical and enable Remote Code Execution, meaning that an attacker could gain control over a device remotely. The remaining vulnerabilities were classified as denial of service, information leaks, or logical flaws.[58] The severity of URGENT/11 centres around the fact that it allows hackers to take over devices with no user interaction required, and even bypass perimeter security devices such as firewalls.[59]

Three possible scenarios have been described for URGENT/11.[60] The first affects VxWorks devices at the perimeter of the network, such as firewalls. Using the vulnerabilities, the attacker could launch a direct attack, taking control of them, and subsequently the networks they guard. Secondly, an attack could affect a VxWorks device which has an external network connection. The vulnerabilities would allow attackers to take over such devices, regardless of any firewall implemented. The low-level nature of the vulnerabilities allows the attacker to remain invisible to security measures, as they would be viewed as benign network connections. Finally, an attacker already within the network as a result of a previous attack, such as the two previous scenarios, can take full control over the device, with no user interaction required.

Prevention going forward

The developer of VxWorks and other affected manufacturers have developed and distributed patches; however, the difficulties in dealing with vulnerabilities such as these have been highlighted. As software components that can be separately licenced, or are open source, get adapted and incorporated into various software products, they evolve over time. The lack of standardisation makes it difficult to develop a single security patch that will cover all models.[61] It therefore could be impossible in some instances to update every device potentially affected.[62]

The FDA highlighted that although they were not aware of any adverse events related to these vulnerabilities to date, software to exploit them is already publicly available.[63] It recommends risk assessments and development of risk mitigation plans by both manufacturers and health care providers. Armis has also released an URGENT/11 Detector, a free, downloadable tool designed to detect devices vulnerable to URGENT/11 regardless of the operating system.[64]

[56] Armis (2019) 'UPDATE: URGENT/11 affects additional RTOS – Highlights Risks on Medical Devices'
[57] Lily Hay Newman (2019) 'Decades-Old Code Is Putting Millions of Critical Devices at Risk'
[58] Armis (2019) 'UPDATE: URGENT/11 affects additional RTOS – Highlights Risks on Medical Devices'
[59] Ibid
[60] Ibid
[61] Lily Hay Newman (2019) 'Decades-Old Code Is Putting Millions of Critical Devices at Risk'
[62] Ibid
[63] U.S Food and Drug Administration (2019) 'URGENT/11 Cybersecurity Vulnerabilities in a Widely-Used Third Party Software Component May Introduce Risks During Use of Certain Medical Devices: FDA Safety Communication'
[64] Ben Seri (2019) 'URGENT/11 Affects Additional RTOS – Highlights Risks on Medical Devices'

IoT Manufacturers in the UK

This study has involved analysis of the organisations that manufacture consumer IoT devices for the UK market. This included any organisations that manufacture and sell at least one consumer IoT product for the UK market. The total number of relevant companies we believe to exist in the UK consumer IoT market is approximately 170; this includes foreign-owned companies and multinationals with a UK presence. The names of the companies included in our market study can be found in chapter 4 of the accompanying technical report.

A sector profile prepared by RSM in 2019 included an analysis of 100 consumer IoT manufacturers found in business databases such as Companies House or ORBIS. Information on turnover was available for 60 of these companies (as not all companies have published accounts or business records that allow an estimate of size to be made). This analysis is included in the technical report. A summary table of the size distribution is shown in Table 20 below.

Table 20: Distribution of known UK consumer IoT companies by size, 2019

Organisation size	Percentage of companies
Small (under £10.2m)	65%
Medium (£10.2m to £49.9m)	8%
Large (£50m and over)	27%
Base	60

Source: RSM/ORBIS (information on size available for 60 out of 100 companies found in 2019)

Number of IoT products

Our market study included analysis of 345 different products from 164 different manufacturers. The table included in chapter 4 of the Technical Report reflects the number of products included in the study for each manufacturer. The manufacturer with the greatest number of products was Samsung, with 40 products included in the study, across seven of the 16 subcategories. The rest of the top five manufacturers included LG (14 products), Apple (12 products), Panasonic (10 products), and Bosch (9 products).

Further research was conducted into the most prolific producers in order to assess the upper bound for consumer IoT production. Samsung was found to be one of the largest sellers in the UK, as was suggested by our initial market study research. They produce 140 consumer IoT devices which can be purchased by UK consumers. These include devices from all three product groups: smart TVs, smart fridge freezers, smart washer/dryers, smart vacuum cleaners, smart motion sensors, smart plugs, smart speakers, smartphones, smart tablets, and smart watches/health trackers.

However, while several manufacturers produced multiple products, the majority only produced one or two products that could be found in our market study. In total, only 28 of the 164 manufacturers in the study produced more than two of the products included in our analysis. There were 20 manufacturers that produced two products, and 116 that only produced one. These figures reflect that while there are some prolific manufacturers that dominate certain subcategories, there are also many specialised manufacturers who focus on one area of smart technology and produce on a much smaller scale.

3. CONSUMERS OF IOT PRODUCTS

A survey of 5,421 consumers, representative of the UK population of adults (18 and over) was conducted in February 2020, in order to assess consumer IoT device ownership and behaviours, analysed by the three product groups. Full details of the questionnaire can be found in chapter 6 of the accompanying technical report.

Device ownership: The average number of devices owned per product group are as follows:

- Group 1: Big ticket items: 0.88 per household (1.59 per household that owns at least 1)
- Group 2: Connecting the home: 1.06 per household (2.94 per household that owns at least 1)
- Group 3: Consumer lifestyle: 1.82 devices per household (2.01 per household that owns at least 1)

Disconnecting IoT devices: The most commonly disconnected smart product group is “big ticket items”, with 25% of owners having disconnected their device from the internet at some point, or having simply never connected. This is closely followed by consumer lifestyle devices, at 24%. Only 15% of owners of “connecting the home devices” have disconnected them at any point, or never connected them.

Use of consumer IoT devices in business: Overall, 50% of employed respondents answered that smart devices were used by their employers in the workplace. Of these, the most popular smart devices were smartphones, with 35 % of respondents indicating that their organisation uses these. This was followed by tablets, which were used by 21% of respondents’ employers.

Security as a barrier to growth: Among consumers who said that they did not plan to purchase smart devices in the next 12 months, 28% said that they were concerned about the security of smart devices, and 30% were concerned about their privacy. Those consumers with security concerns (n=690) were asked what factors would encourage them to purchase such a device. The answers in order of frequency were:

1. independent certification / assurance of minimum security standards (28%);
2. transparency on length of time that security updates would be provided (22%);
3. assurance that each device has a unique password (20%);
4. assurances from manufacturers on adherence to minimum security standards (19%)
5. security information at point of sale (19%)
6. assurance that vulnerabilities can be reported to the manufacturer (17%)

It is notable that independent assurance of standards was more commonly cited as a factor that would encourage purchasing of smart devices than manufacturer self-assessment.

Context

In the UK, there were an estimated 13 million connected devices in 2016, forecast to increase to 156 million by 2024, including around 40 million consumer electronics and fast-moving consumer goods (FMCG).[65]

The TechUK State of the Connected Home Survey for 2019[66] shows:

- 19% of consumers have a fitness or activity tracker;
- 22% have a smart speaker (e.g. Amazon Echo or Google Home);
- 46% have smart TVs.

[65] Cambridge Consultants (2017) ‘Review of latest developments in the Internet of Things’ for OFCOM

[66] TechUK (2019) ‘The State of the Connected Home: Edition Three June 2019’

Among consumers who own only one smart device, it is likely to be a smart TV. It is worth noting that this TechUK report does not include smartphones, tablets or PCs as connected devices; however, smartphones were found to be the most common item used for IoT device control.

Ofcom estimates 79% of UK adults have an internet enabled smartphone, mostly with a 4G service. Their research shows 52% consider this their most important device for going online. Again, this is especially prevalent for younger age groups (16 to 34 year olds).[67] Smart speakers and fitness trackers are also prevalent among consumers who only have one or two devices.[68]

Evidence from Wrap (a waste reduction / resource efficiency organisation) estimated that ownership of consumer IoT devices could rise from 10 to 15 devices in each UK household in 2020.[69] A more recent review conducted by DBS Asian Insights showed increasing global adoption of IoT devices and predicted that the IoT installation base would grow from 6.3 million units in 2016 to 1.25 billion in 2030.[70]

The consumer survey

Our consumer survey asked a range of questions to further investigate the average consumer ownership of IoT devices per UK household. This survey was answered by 5,421 UK consumers.

Table 21: Devices owned by respondents by product group

Product Group	Percentage of people who own at least one device in this product group
Group 1: Big ticket items	56%
Group 2: Connecting the home	38%
Group 3: Consumer lifestyle	92%

Source: Consumer Survey Q1: Which, if any, of the following devices do you currently have in your household? (n=5421 – all respondents)

The most common product group is consumer lifestyle, with 92% of all respondents owning at least one product included in this category, this being likely supported by the inclusion of common items such as smartphones and tablets. Big ticket items were the next most popular product group, this supporting the TechUK research above, which finds that smart TVs are one of the most commonly owned smart devices.

The table below reflects the breakdown of these product groups into device types.

[67] OfCOM (2019) ‘Media Nations: UK 2019’
[68] TechUK (2019) ‘The State of the Connected Home: Edition Three June 2019’
[69] Wrap: Smart Devices & Secure Data Eradication: The Evidence http://www.wrap.org.uk/sites/files/wrap/Data%20Eradication%20report%20Defra.pdf
[70] Forbes (2018) ‘2018 Roundup of Internet of Things Forecasts and Market Estimates’

Table 22: Devices owned by respondents

Product Group	Device	Percentage
Group 1: Big ticket items	Smart TVs	54%
	Connected domestic appliances (e.g. washing machines, fridges)	13%
Group 2: Connecting the home	Smart home thermostats	10%
	Smart home assistants/ speakers	31%
	Smart security system (smart video doorbells, smart video cameras etc.)	8%
	Smart lighting	10%
Group 3: Consumer lifestyle	Smartphones	83%
	Tablet	65%
	Smartwatch	15%
	Wearable health trackers	22%
	Smart or connected children’s toys and baby monitors	2%
	Other	6%
	None of these	5%
	Base	5421

Source: Consumer Survey Q1: Which, if any, of the following devices do you currently have in your household? (n=5421 – all respondents)

This table reflects that the most common consumer IoT device is the smartphone (83%), followed by tablets (65%) and then smart TVs (54%). The top two most common IoT devices are both from Group 3 (consumer lifestyle), further reflecting that this is the most popular product group. The least commonly owned device type was smart or connected children’s toys and baby monitors, with only 127 people (or 2% of the sample) owning devices in this category.

Table 23 below includes the mean number of devices owned among those that own them, and also (in brackets) the overall amount. For example, among those that have smart lighting, there is an average of just over 4 light bulbs per respondent, but the overall average among all respondents (including those with no smart lighting devices) is just 0.36.

The highest mean device ownership was found to be for connecting the home, with users of devices in this product group on average owning 2.94 connecting the home devices. This high average is supported by the high mean number of smart lighting devices (4.02). This is a logical category to have the highest average number of devices owned, as these products can be connected and controlled simultaneously throughout the home. This was followed by an average of 2.09 consumer lifestyle devices, and 1.59 big ticket items.

Table 23: Mean number of devices owned by respondents

Product Group	Device	Mean number of devices[71]	Weighted[72] mean number of devices	Base
Group 1: Big ticket items	Smart TVs	1.43 (0.76)	1.59 (0.88)	2885
	Connected domestic appliances (e.g. washing machines, fridges)	1.87 (0.12)		385
Group 2: Connecting the home	Smart home thermostats	1.19 (0.12)	2.94 (1.06)	533
	Smart home assistants/ speakers	1.97 (0.57)		1579
	Smart security system (smart video doorbells, smart video cameras etc.)	1.70 (0.12)		392
	Smart lighting	4.02 (0.36)		494
Group 3: Consumer lifestyle	Smartphones	1.54 (1.26)	2.01 (1.82)	4449
	Tablet	1.42 (0.85)		3243
	Smartwatch	1.25 (0.17)		724
	Wearable health trackers	1.24 (0.23)		1000
	Smart or connected children's toys and baby monitors	2.36 (0.05)		113

Source: Consumer Survey Q3: (For those owned and used) How many of each of the following devices do you currently own and use? (Base for each row=owners of this device type)

In all categories, excluding smart lighting and domestic appliances, a mean ownership of less than two devices for each type was the most common. This was the most significant for smart home thermostats, where 91% of ownership was of only one device. The second most common category where only one device is owned and used is smart watches, with this being the case for 84% of smart watch owners.

Type of smart domestic appliance

Survey respondents were asked in more detail about their ownership of smart domestic appliances, with this category broken down into nine product types.

[71] Figures shown are the mean number of devices among just the households that own them, and then in brackets the mean number of devices among **all** households.
[72] Weighted mean: calculated based on the mean number of devices (calculated by YouGov using a weighted base) and scaled using the base size.

Table 24: Smart domestic appliance ownership

Device	Percentage of respondents who own and use these devices
Smart oven	1%
Smart fridge/freezer	2%
Smart microwave	1%
Smart cooker	1%
Smart dishwasher	1%
Smart washer/dryer	4%
Smart toaster	1%
Smart coffee machine	1%
Smart kettle	1%
Other smart appliance	1%
Don't know	1%
Not applicable, I don't own a smart domestic appliance	92%
Base	5421

Source: Consumer Survey Q4: Which, if any, of the following smart domestic appliances do you own and use? (n=5421 – all respondents)

The survey results reflect that the average ownership of smart domestic appliances is low, with 92% of all survey respondents indicating that they do not own any internet connected domestic appliances. This is noteworthy in terms of ownership within Group 1 (big ticket items), as smart white goods and smart kitchen appliances make up two of the three subcategories within this group. In contrast, smart TVs are also included in this group and, as noted above, are one of the most commonly owned smart consumer devices.

Of those that do own smart domestic appliances, the most common is a smart washer/ dryer, with 4% of the sample indicating ownership of this device. By contrast, the least common was a smart toaster, with less than 1% of respondents indicating ownership of this device.

Those smart devices that were added by respondents as 'other' within this category are all devices that are not included in the smart domestic appliance category, but are included in the 'consumer lifestyle' and 'connecting the home' categories.

Popular brands and channels for purchase

This section looks in more detail at the brands of devices, channels for purchase, and expenditure on smart domestic appliances, smart thermostats, smart home assistants/speakers, smart security systems, and smart lighting.

The respondents who were asked for details on each type of device they had previously indicated ownership in that category.

Brand: Smart Domestic Appliances

Table 25: Smart domestic appliances most common brand

Device	Most common brand	Percentage of owners	Base
Smart oven	LG	15%	59
Smart fridge/freezer	Samsung	28%	86
Smart microwave	LG	18%	58
Smart cooker	Samsung	18%	47
Smart dishwasher	Bosch/Miele	14% each	52
Smart washer/dryer	Samsung	23%	192
Smart toaster	Hotpoint	23%	40
Smart coffee machine	Bosch	19%	60
Smart kettle	LG	13%	58

Source: Consumer Survey Q47 Thinking of each smart appliance that you own, which brands are they? (Base for each row=owners of this device type)

The most popular brand for each type of appliance varies by device type but Samsung and LG are the two most popular brands for smart domestic appliances overall, being the most common brand for six of the nine subcategories.

Brand: Smart Thermostats

The most popular brand was Hive, with this being the case for 55% of smart home thermostat owners.[73] The second most popular brand was Nest, with 17% ownership, and the third most popular brand was Honeywell, with 5% of ownership.

Brand: Smart Home Assistants/Speakers

Amazon was by far the most commonly owned brand of smart home assistant/speaker, with 77% of respondents who said that they own a smart home assistant/speaker owning this brand.[74] Google products were the second most popular with 22% of respondents owning this brand. Finally, the third most popular brand was Sonos, with 6% of ownership. Amazon Echo was released around 2015, while Google Home was released in the UK in 2016. Many of the other brands listed in this question are more recent entrants to this market.

Respondents who indicated that they own more than one brand of smart home assistant/speaker were asked which of these they use most often, with 72% choosing Amazon as their most popular brand, and 17% choosing Google.

Brand: Smart Security Systems

Ring is the most common home security system among respondents (32%), followed by Nest (6%) and Hive (6%). There were 75 respondents who indicated that they use ‘other’ brands for home security systems. These include a wide range of different manufacturers represented by only one or two respondents, however, some popular brands included: Arlo (9), Canary (5), Yi (4), Annke, Hik, Neos, Netatmo and Wansview (3 each)

Brand: Smart Lighting

The most popular brand for smart lighting was Phillips, with 41% of respondents that own smart lighting choosing this brand. The second most popular brand was found to be Hive, with 18% of

[73] Base: 546 respondents

[74] Base: 1,685

ownership. Finally, the third most popular brand is TP-Link, where 8% of smart lighting owners indicated that this is their brand of choice.

Expenditure on Smart Devices

The following table reflects consumers' estimated total spend on **all** smart devices in the last year and in total.

Table 26: Total spending on all smart devices in the last year and in total

Cost	Spending on smart devices in the last year	Total spending on smart devices
Nothing	27%	11%
Under £100	20%	10%
£100 to £199	12%	8%
£200 to £299	7%	5%
£300 to £399	5%	6%
£400 to £499	3%	5%
£500 to £599	2%	5%
£600 to £699	1%	3%
£700 to £999	3%	6%
£1,000 to £1,999	4%	10%
£2,000 to £2,999	1%	5%
£3,000 to £3,999	0%	2%
£4,000 to £4,999	0%	1%
£5,000 or more	1%	2%
Don't know	15%	20%
Base	2,224	2,224

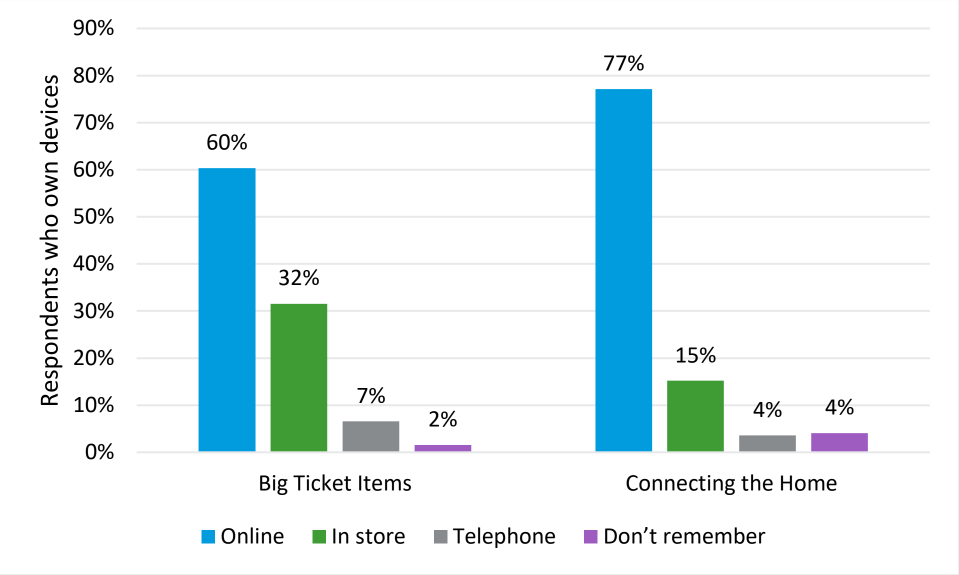
Source: Consumer Survey Q68 Thinking about the last 12 months… how much do you think you have spent on all smart devices that you own & use? Please think of all your smart home devices. And Q69 How much have you spent in total on all your smart devices that you own & use? Please think of all your smart home devices. (n= 2,224 – all smart device owners)

In terms of spending in the last year, the most common answer was that respondents have spent nothing on smart devices, with this being the case for 27% of the sample. Overall, this table reflects that consumers have spent relatively little on smart devices in the last year, with over half (54%) of respondents indicating that they have spent less than £150 in the last 12 months. It is worth noting that 15% of respondents did not know how much they have spent on smart devices within the last year.

When asked about spending on smart devices in total, 11% of respondents had spent nothing on smart devices, however these answers were more evenly distributed across the price range than the responses relating to expenditure within the last year. Just over half (51%) of respondents have spent less than £600 in total on smart devices. It is also worth noting that 20% of respondents did not know how much they have spent in total on smart devices.

Sources of purchase

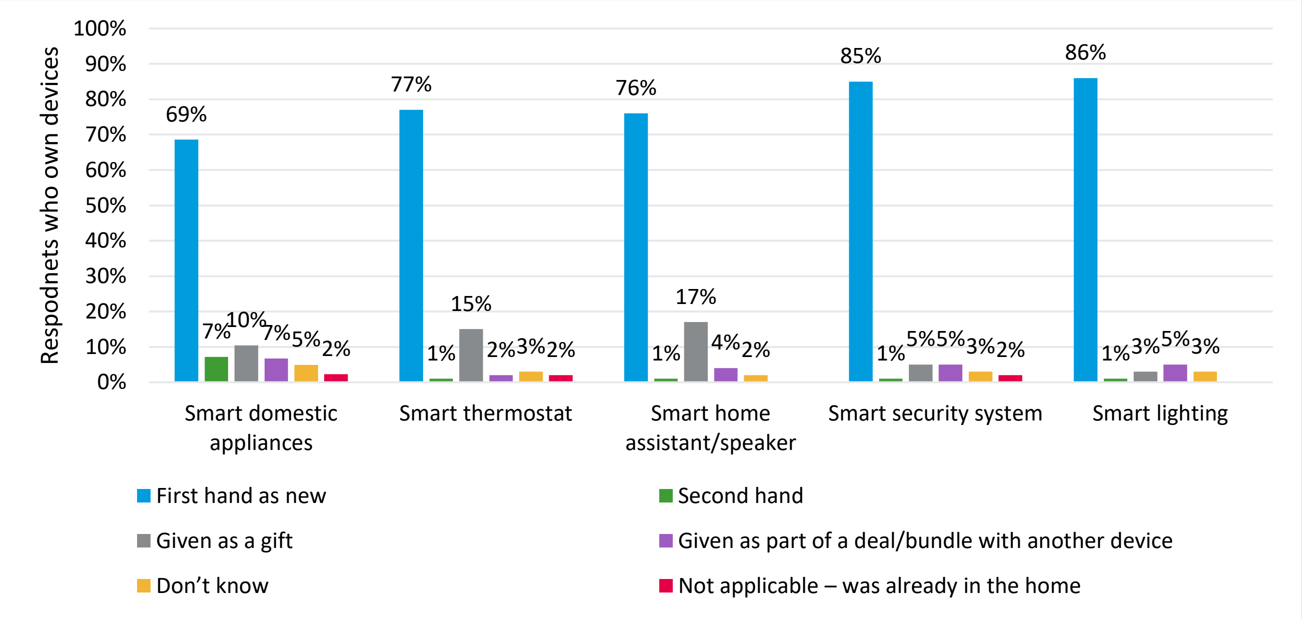
Figure 1: How smart devices were purchased



Source: Consumer Survey Q31/Q36/Q40/Q44/Q48/Q50/Q52/Q54/Q56/Q58/Q60/Q62/Q64 How did you purchase your [smart device]? (n= 1254; 400; 436; 342; 51; 80; 49; 42; 42; 170; 38; 55; 50 – all who purchased each device type)

For both big ticket items and connecting the home, it was most common for consumers to purchase these online, followed by in store purchases. It was, however, far more common for connecting the home purchases to be online, at 77% compared to 60% for big ticket items. This reflects that for more expensive big ticket purchases, consumers are more likely to want to make these purchases in person. In total across all device types, on average 74% of purchases are made by consumers online, with 18% made in store.

Figure 2: How smart devices were acquired by owners



Source: Consumer Survey Q32/Q37/Q41/Q45/Q49/Q51/Q53/Q55/Q57/Q59/Q61/Q63/Q65 Was your smart device purchased… (n= 1685; 546; 522; 407; 59; 86; 58; 47; 52; 192; 40; 60; 58 – all who own each device type)

Smart devices were most commonly purchased first-hand as new by the owners. This was most likely to be the case for smart washer/dryers, where 87% of owners had purchased these first-hand as new. This was least likely to be the case for smart toasters and smart microwaves, where in both cases only 54% of owners had purchased their device first-hand as new. The purchase of smart devices second hand was uncommon, being most popular for smart ovens (15%) and smart microwaves (14%). Smart toasters were most likely to be given as a gift, at 22%, followed by smart cookers and home assistant/speakers both at 17%.

The table below reflects the most popular retailer for each device type.

Table 27: Most common retailer used by device type

Device	Most common retailer	Percentage of owners	Base
Smart oven	Amazon	15%	59
Smart fridge/freezer	Currys PC World	19%	86
Smart microwave	Amazon	14%	58
Smart cooker	AO.com	12%	47
Smart dishwasher	Argos/Amazon/Currys PC World	11% each	52
Smart washer/dryer	Currys PC World	28%	192
Smart toaster	Amazon	24%	40
Smart coffee machine	Amazon	16%	60
Smart kettle	Amazon	22%	58
Smart thermostat	Directly from the manufacturer/brand	23%	546
Smart home assistant/speaker	Amazon	48%	1685
Smart security system	Amazon	35%	407
Smart lighting	Amazon	49%	522

Source: Consumer Survey Q31/Q36/Q40/Q44/Q48/Q50/Q52/Q54/Q56/Q58/Q60/Q62/Q64 Where did you purchase your smart device? (Base for each row=owners of this device type)

While level of popularity varies, Amazon is often the most popular retailer reported by respondents, being the most common response for nine of the 13 subcategories analysed. The second most common retailer was Currys PC World, with this being the most popular answer for three of the 13 subcategories.

Average expenditure by consumer group

On average the survey respondents had spent £124.21 on smart devices in the last 12 months. This includes all respondents, including those who have never bought a smart device - those who already own a smart IoT device and spent money on consumer IoT devices in the last 12 months reported spending an average of £302.76. This figure represents the average across all age groups, genders, social grades, and regions. The table below highlights the average expenditure broken down across these groups.

Table 28: Average annual expenditure on consumer IoT devices

Group	Subgroup	Mean expenditure (if already own a device)	Mean expenditure (whole population)
Overall	-	£302.76	£124.21
Gender	Male	£330.24	£142.35
	Female	£271.65	£106.14
Age	18 – 24	£282.28	£125.30
	25 – 34	£362.45	£174.20
	35 – 44	£344.11	£163.21
	45 – 54	£358.37	£159.17
	55 – 64	£288.24	£104.65
	65+	£157.13	£48.04
Social grade	ABC1	£325.12	£143.06
	C2DE	£264.31	£97.81
Region	North	£262.26	£109.46
	Midlands	£233.21	£108.61
	East	£312.90	£132.89
	London	£490.45	£178.98
	South	£319.37	£128.43
	Wales	£219.13	£90.97
	Scotland	£298.89	£115.05
	Northern Ireland	£266.76	£88.23

Source: Consumer Survey Q68 Thinking about the last 12 months, how much do you think you have spent on all smart devices that you own and use? (Base= 2,224 – all who own a smart device; or Base=5,421 - all respondents)

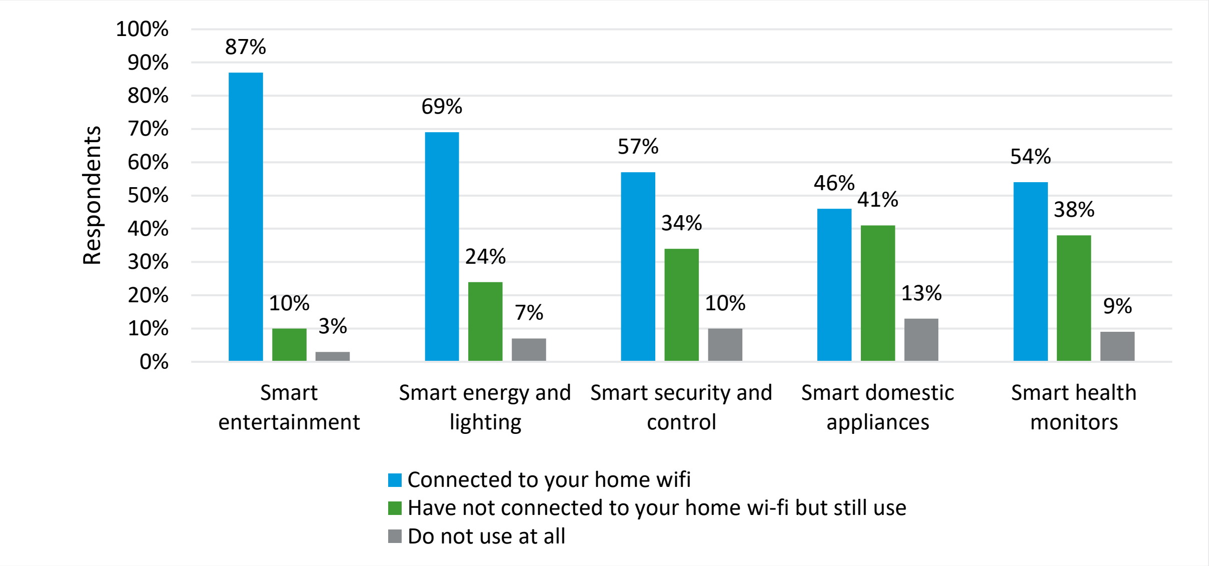
The average expenditure has been used to calculate an estimated total UK expenditure on consumer IoT products. With the mean expenditure per adult (18+) across the UK population estimated at £124.21, and the adult population[75] estimated to be 52.7 million, the total estimated annual UK expenditure on consumer IoT (by the adult population) is £6.5bn. Of this total expenditure, it is estimated that £3.7bn was spent by male consumers, and £2.9bn by female consumers.

Consumers who opt out of internet functionality

Not all consumers that purchase IoT devices connect them to the internet. TechUK's State of the Connected Home 2019[76] report found that smart entertainment devices such as smart speakers were the most likely to be connected. Smart domestic appliances, including smart kettles and coffee makers; smart refrigerators; smart washing machines and smart ovens/hobs, were the least likely to be connected.

[75] Population statistics for this calculation come from Office for National Statistics detailed population statistics for 2019 (published May 2020) by age, sex, and local authority.
[76] TechUK (2019) 'The State of the Connected Home: Edition Three June 2019'

Figure 3: Device connectivity by device type



Source: TechUK (2019)

An industry association interviewed by RSM as part of this study suggested that people who purchased connected white goods were more likely to be buying because of the connectivity of the devices, as these tend to be more expensive than non-connected devices, so it is surprising that this group is the most likely to not be connected to the home wi-fi.

Our survey also investigated the use of the internet connectivity functions of smart devices. Smartphones were the devices most likely to be used and connected to the internet, with 98% of all responses reporting that the consumers' device was connected. In fact, most devices are reported by consumers as connected devices, with nine of the 12 categories having over 80% of respondents own and use their device with the internet connected.

The category with the highest level of use without internet connection was smart or connected baby toys and monitors at 29%. This was significantly higher than any other category, with the next highest being smart security systems at 9%.

The table below summarises this data by product group.

Table 29: Device ownership and usage by product group

Product Group	Device owned and used currently	Device owned and used, but not connected to the internet	Device owned but no longer used	Base
Group 1: Big ticket items	94%	4%	1%	3,449
Group 2: Connecting the home	90%	5%	4%	2,584
Group 3: Consumer lifestyle	91%	3%	5%	10,055
Total average	92%	4%	3%	16,088

Source: Consumer Survey Q2: Of these smart devices that you have in your household, which are: owned and used currently; owned and used, but not connected to the Internet; owned but no longer used? (NB The individual products have been amalgamated into product groups, so a respondent owning 2 kinds of "big ticket" item counts twice in this group. The base for each row is therefore greater than the number of respondents overall.)

Group 3 ‘consumer lifestyle’ is the product group where consumers are least likely to own and use a device but not have it connected to the internet. However, all three product groups have very low levels of device use without connectivity.

These survey findings correlate with the TechUK report[77] to a certain extent. In that report, ‘smart entertainment’ devices also had the lowest levels of use without connecting to the internet, including smartphones at 1%, smart tablets at 2%, and smart TVs at 4%.

Despite generally high usage with internet-connection, this data does reflect that estimates of the average number of connected consumer IoT devices owned by UK households may be slightly misleading, as in some cases these owners do not actually use the connection function of their device, or may not even use the device anymore at all.

Respondents were asked to further detail their connectivity habits, highlighting whether devices are always connected to the internet; disconnected from the internet; intermittently disconnected; or have never been connected to the internet.

Consistent internet connectivity was found within popular categories such as smartphones (83%), smart TVs (81%), smart home assistants/ speakers (82%), smart home thermostats (86%), and smart security systems (82%). These top five categories all show over 80% of respondents indicating that their devices are always connected to the internet. This again corresponds with TechUK’s research, which reflects that connectivity is highest in smart entertainment devices.

The survey responses for connected domestic appliances show that relatively fewer consumers have these devices constantly connected to the internet. All categories within smart domestic appliances showed that less than 40% of owners had these devices always connected to the internet. Again, this is interesting in light of the idea that connected white goods tend to be more expensive than non-connected devices and as such it might be expected that these are purchased by consumers specifically for these functions. This also corresponds with TechUK research reflecting that smart domestic appliances have relatively low connectivity and high use without internet.

Using this data, the number of respondents who had indicated any form of opting out of the internet function of their smart device (including: disconnected from the internet; intermittently disconnected/ connected to the internet; and never connected them to the internet) were totalled to show the number of users who had opted out at any point in their ownership.

Table 30: Devices disconnected from the internet or never connected

Product Group	Average percentage of device owners who had disconnected from the internet at some point, or had never connected the device	Base
Group 1: Big ticket items	25%	3,576
Group 2: Connecting the home	15%	3,160
Group 3: Consumer lifestyle	24%	10,153

Q70: Of the smart devices that you own and use, have you decided to disconnect them from the internet, opt out of or disable their internet connectivity, or did you never connect them to the internet? (Base for each row = total respondents for each product group)

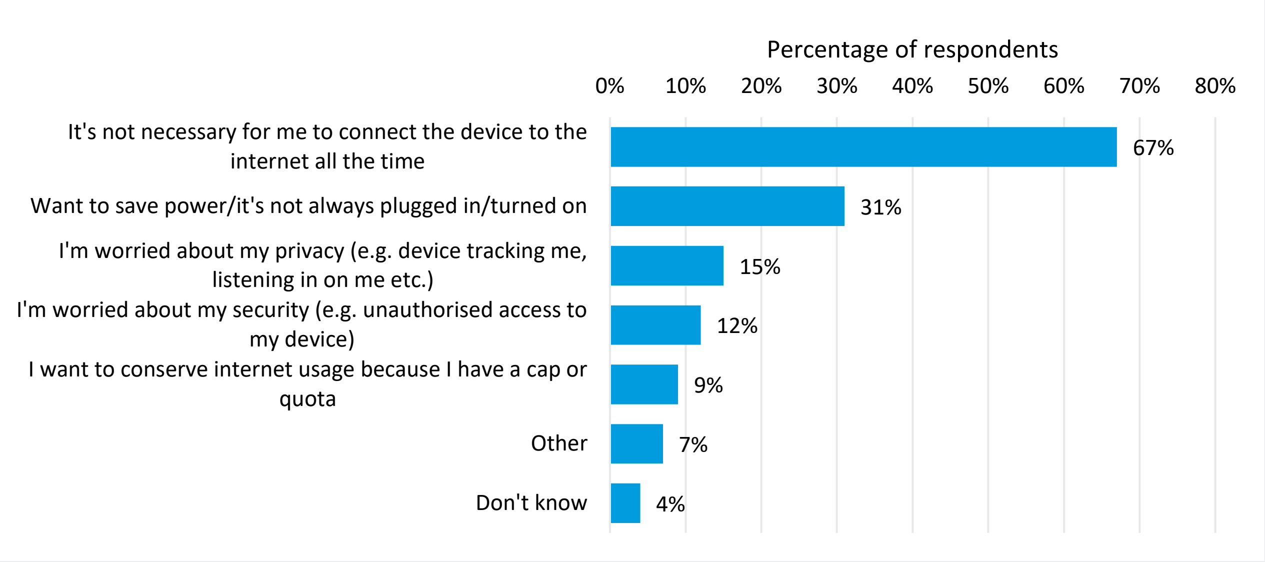
All connected domestic appliances had a total opt out rate of at least 50%.

The product groups ‘connecting the home’ had the lowest percentage of consumers who at any point had opted out of internet connectivity, at 15%; 2.7% had never connected them to the

[77] TechUK (2019) ‘The State of the Connected Home: Edition Three June 2019’

internet. ‘Big ticket items’ and ‘consumer lifestyle’ have slightly higher average opt out rates, at 25% and 24% respectively; however, big ticket items were more than twice as likely to have never been connected to the internet at all (6.3%) than consumer lifestyle items (3.0%).

Figure 4: Reasons for not connecting devices to the internet



Source: Consumer Survey Q71 You said that some of the smart devices that you own and use are not always connected to the internet. Which of the following are reasons for this? (n=2284 – all who own smart devices which aren’t connected to the internet (always or sometimes))

42% of all survey respondents had indicated that at some point they have disconnected at least one of their smart devices from its internet connectivity function. The most popular reason for users not always having smart devices connected to the internet was that the internet connectivity is not always necessary, with 67% of respondents indicating this as one of their reasons. The least popular reason given was that users want to conserve their internet usage, with only 9% of respondents indicating this as one of their reasons.

Consumer replacement of devices

Survey respondents were asked several questions to investigate the average rate at which consumers upgrade or replace their smart devices. As this survey was conducted in February (2020), it is worth noting that the months immediately preceding this included Christmas and January sales, which may have influenced consumers’ purchasing habits.

Current ownership

Consumers were asked when they first purchased a smart device in each category:

Table 31: When the first smart device was purchased

	Big Ticket Items	Connecting the Home	Consumer Lifestyle
Before 2015	19%	3%	10%
Since 2015	11%	3%	5%
Since 2016	12%	7%	9%
Since 2017	15%	14%	13%
Since 2018	17%	29%	24%
Since 2019	15%	34%	26%
Since 2020	3%	4%	3%
Don't know	9%	5%	9%
Average age	3.12	1.73	2.29
Base	3309	3160	127

Source: Consumer Survey Q9 How long have you had your devices in your household for? Please think about the first one of each type of device you may have had, rather than the existing device. (Base = total respondents for each product group)

Note: Weighted averages computed using midpoint of ranges; "Before 2015" assumed to be Jan 2014.

Overall, the date of first purchase for big ticket items is relatively evenly spread between 2015 and 2019, reflecting the findings that while smart TVs were most commonly purchased before 2015 (20% of smart TV owners), smart domestic appliances were often owned only since 2019 (28% of smart domestic appliance owners). Connecting the home items were most commonly owned since 2019 (34%), reflecting that many of the items included in this category are relatively new to the consumer IoT market. Overall, other than smart TVs, all categories reflected that the highest percentage of consumers' smart devices have been owned since 2018 or 2019.

Table 32: Reason for most recent device purchase

Device	Replaced this device with a newer one (upgraded)	Bought additional devices from this category	Bought connected version of device for the first time	Don't know	Base
Big Ticket Items	30%	9%	56%	5%	3,309
Connecting the Home	7%	14%	74%	5%	3,160
Consumer Lifestyle toys and baby monitors	13%	11%	69%	7%	127

Source: Consumer Survey Q10 What was the reason for your most recent purchase in each category? (NB The individual products have been amalgamated into product groups, so a respondent owning 2 kinds of "big ticket" item counts twice in this group. The base for each row is therefore greater than the number of respondents overall.)

The most common answer for all individual device categories was that consumers had purchased their most recent smart devices for the first time, rather than to replace older smart devices or buy additional devices in that category. This answer was most prominent for smart home thermostats, where 80% of respondents answered that this had been their first purchase in this category. Big ticket items had the highest average rate of upgrade, at 30% overall, with 31% replacing their smart TVs and 24% their smart domestic appliances. The category with the highest rate of consumers purchasing additional devices was smart lighting, with 21% of smart lighting owners indicating that their most recent smart lighting purchase was in addition to other devices already owned in this category.

Table 33: Length of time since devices have been replaced and upgraded

Product Group	Group 1: Big ticket items	Group 2: Connecting the home	Group 3: Consumer lifestyle
Within the last 3 years or longer*	22%	9%	0%
Within the last 2 to 3 years	19%	14%	10%
Within the last 1 to 2 years	21%	16%	23%
Within the last 6 to 12 months	12%	15%	25%
Within the last 3 to 6 months	8%	9%	9%
Within the last 3 months	7%	18%	7%
Within the last month	5%	10%	23%
Don't know	6%	9%	4%
Weighted average (years)	1.92	1.23	0.86
Base	993	210	16

Source: Consumer Survey Q11 When was the last time you replaced/ upgraded each of the following devices? (Base = total devices being replaced in each product group)

**Note: Weighted averages computed using midpoint of ranges; "3 years or longer" assumed to be 4 years*

It appears that 'big ticket items' have been upgraded least recently, with 22% having been replaced only within the last 3 years or longer. Big ticket items are the group that tend to be the most expensive, with an overall mean price found in our market study of £735.97. This would perhaps explain why these items are replaced less often by consumers.

In total, 64% of smart TV owners have not upgraded their device within the last year. Other categories, by contrast, appear to be much more evenly distributed in terms of most recent replacement and upgrade of smart devices.

Smart home speakers have most commonly been upgraded in the last three months, with 24% of users indicating this answer. It is worth noting that this trend may have been influenced by the Christmas and January sales that preceded this survey. However, the majority of users (55%) indicated that they had upgraded this device longer than three months ago.

The most common answer for smart domestic appliances was that these had been upgraded within the last one to two years, given by 20% of those owners that had upgraded, with the second most common being within the last six to 12 months (16% of owners of smart DAs that had upgraded).

Where relevant, survey respondents were also asked about what they did with old devices when they replaced and upgraded them.

Table 34: How consumers dispose of old devices

	Big Ticket Items	Connecting the Home	Consumer Lifestyle
Traded it in as part of a deal for the new one	4%	3%	6%
Passed it on to somebody I know	25%	10%	18%
Kept it as a spare	15%	15%	29%
Continue to use it	12%	16%	0%
Threw it away	17%	18%	12%
Sold it via an online third party (e.g. eBay, Gumtree, Amazon, Depop, Facebook Marketplace etc.)	9%	9%	12%
Sold it via a high street store (e.g. CEX, Cash Converters etc.)	3%	7%	18%
Gave to charity	5%	3%	0%
Other	5%	6%	0%
Don’t know	4%	12%	6%
Base	1,030	208	17

Source: Consumer Survey Q12-Q17 Which of the following did you do with your older device? (Base = total devices being replaced in each product group)

Overall, methods for disposal of old devices varies by device type. For big ticket items the most common option was passing old devices on, with this being the case for 28% of smart TV owners. For connecting the home, the most common disposal method was simply throwing the item away (18%), and for consumer lifestyle this was to keep the device as a spare (33%). It is worth noting that the base sizes vary here as this question was dependent on consumers indicating that they have previously replaced and upgraded a device within the product group.

Within the product groups, the most common response varied depending on the type of device. For smart security systems (22%) and smart children’s toys and baby monitors (33%), keeping the old device as a spare was the most common answer in both cases for those who had replaced or upgraded the device. For both smart thermostats and smart lighting, the most common answer was to throw old devices away, with 32% for smart thermostats and 20% for smart lighting. For smart home assistants/ speakers the most common answer was to continue to use older devices (28%), and for smart domestic appliances the most common response was to sell them via an online third party (20%).

Case study- Smart lighting

What was the vulnerability?

An independent investigation was carried out by a security researcher, to test the security hardware of the a smart lightbulb.[78] The researcher found three vulnerabilities in the product, which were disclosed to the manufacturer and later confirmed by the company.[79] These included Wi-Fi credentials stored in plain text within the flash memory of the device allowing for access to the network. There was an overall lack of security measures in place to protect the bulb's hardware, meaning that devices that can be physically accessed are at risk.

The researcher was able to saw through the light bulb to expose the inner electronics. They found the main component of the bulb and were able to connect the device hardware to their computer with a customised physical connector that they soldered onto the bulb's circuit board. Once this link was established, the researcher was able to find the vulnerabilities they discovered.

Purpose/possible future attacks

These vulnerabilities required physical access in order to be exploited, as opposed to being accessed remotely. This highlights the potential for old devices that are disposed of incorrectly to expose the previous owner's network to cyber-attacks. Many smart light bulbs connect directly to a home's wireless network, without needing a smart home hub. Smart home hubs are hardware or software designed with the aim of overseeing communication between devices in your smart home, so would ensure greater security. Smart light bulbs are also equipped with infra-red technology so that they work with home security cameras. The infra-red technology can also be exploited to extract information from devices connected to the same network, through the creation of a 'covert channel' between the light bulb and the infrared-sensing device, ie. the camera.[80]

This also applies to devices other than smart light bulbs. Small and inexpensive products can be bought by attackers relatively easily and taken apart to see what is inside them, how they work, the general weaknesses of the product and how they could exploit the device over a network.[81]

Once a device is released and becomes popular, cheaper alternatives are likely to follow. Since effective cyber security design and implementation adds additional cost, naturally these cheaper alternatives will not have the same level of security as their more expensive counterparts.[82] Moreover, because these devices are typically part of a 'smart home'[83], the potential for other smart home devices and, therefore, for sensitive information to be exposed are vast[84].

Prevention

The lightbulb manufacturer has addressed the vulnerabilities through automatic firmware updates.[85] The company has now encrypted all sensitive information stored in the firmware, and has introduced further security settings in the hardware. Customers are now able to update their firmware through the app, where they will be prompted to do so.

Consumers are encouraged to only purchase products that they can update with security patches in the instance of vulnerabilities being exposed.[86] While this is not a proactive solution, it prevents further vulnerabilities once an issue is found. The CoP guideline 3 ('Keep software updated') recommends making devices securely updateable; for each update to be easy to implement and its purpose made clear to consumers; and to publish a minimum support period for each device stating the minimum length of time for which it will receive software updates.

[78] https://limitedresults.com/2019/01/pwn-the-lifx-mini-white/

[79] https://www.lifx.com/pages/privacy-security-responsible-disclosure-of-security-vulnerabilities

[80] Williams R (2019) 'Why your smart lightbulb could leave your home vulnerable to hacking'

[81] Mutscsler, AS. (2019) *'Iot Device Security Makes Slow Progress'* in Semiconductor Engineering.

[82] Denko, W. (2017) *A Privacy Vulnerability in Smart Home IoT Devices.* University of Michigan-Dearborn.

[83] https://www.smarthome.com/automating-your-home.html

[84] Williams R (2019) 'Why your smart lightbulb could leave your home vulnerable to hacking'

[85] https://www.lifx.com/pages/privacy-security-responsible-disclosure-of-security-vulnerabilities

[86] Mutscsler, AS. (2019) *'Iot Device Security Makes Slow Progress'* in Semiconductor Engineering.

Expected replacement of devices

The consumer survey gives information on when households first purchased a smart device, the reason for purchase, whether smart devices have been replaced and upgraded, and if so, how recently this happened. However, this does not tell the whole story, as many of the devices are so new onto the market that it is too early to tell this from the data.

Survey responses have been used to calculate the average lifespan for each device type in months, where respondents already owned a device, reported when this was purchased and indicated that they intended to replace it within 12 months. It is important to note however, that the base size for these calculated lifespans is small (under 20 responses), and the population is likely to be biased. Few respondents indicated that they are planning to replace devices within the next year, and those that already own smart devices and intend to replace them within 12 months are not representative of the population as a whole. Therefore, these results are indicative and should be interpreted with caution.

Table 35 below presents summary statistical information on the average reported ages of devices (based on date of purchase), the average lifespan where all the data necessary to calculate this was provided, and indicative lifespans for these devices (or similar, non-smart equivalents) from literature.[87]

Table 35: Evidence on device lifetimes by type

Device	Age of first device (still in use)	Lifespan (if to be replaced within 12m)	Lifespan (literature)
Smart oven	38 months	26 months	156 months
Smart fridge freezer	24 months*	25 months	156 months
Smart microwave	24 months*	26 months	108 months
Smart cooker	24 months*	31 months	156 months
Smart dishwasher	24 months*	42 months	108 months
Smart washer/ dryer	24 months*	32 months	120 months
Smart toaster	24 months*	28 months	122 months
Smart coffee machine	24 months*	37 months	122 months
Smart kettle	24 months*	24 months	122 months
Smart home thermostat	26 months	33 months	120 months
Smart home assistant/ speaker	20 months	27 months	Not found
Smart security system	18 months	32 months	Not found
Smart lighting	16 months	36 months	180 months
Smart toys + baby monitors	27 months	n/a	Not found

** Domestic appliances grouped together in consumer survey responses.*

Source: Consumer Survey Q77 You mentioned that you are likely to buy the following device(s). Approximately when do you expect to buy each of the following device(s)? and Q78/ Q81/ Q83/ Q86/ Q89/ Q92/ Q95/ Q98/ Q101/ Q104/ Q107/ Q110/ Q113 You said that you already own a

[87] Data from Consumer Electronics Association (2015, electronics), National Association of Home Builders (2010, appliances); https://housetechlab.com/how-long-does-a-home-thermostat-last/; https://homeaudioforge.com/2018/08/03/how-long-do-smart-bulbs-last/; http://www.smartwatch.me/t/do-smartwatches-turn-obsolete-in-just-two-years/1769/2

[smart device type] in your household and that you intend to purchase another. Will this new smart device: be purchased in addition to your existing device; be to replace the older device; don't know? And Q79/ Q81/ Q84/ Q87/ Q90/ Q93/ Q96/ Q99/ Q102/ Q105/ Q108/ Q111/ Q114 How long have you had your existing [smart device] that you are replacing? (n=17; 10; 13; 11; 9; 11; 7; 6; 5; 11; 9; 11; 3 – number who plan to purchase devices in the next 12 month and provided details on when this would be)

Purchasing patterns

Table 36: Purchase of smart devices in relation to non-connected devices

Device	Purchased in addition to a non-internet connected version of this device	Replace an older non-internet connected version of this device	Purchased instead of a non-internet connected version of this device	Don't know	Base
Smart domestic appliances	13%	36%	22%	29%	1558
Smart home thermostat	16%	34%	27%	22%	337
Smart home assistant/ speaker	22%	18%	29%	31%	276
Smart security system	20%	18%	41%	21%	475
Smart lighting	24%	24%	30%	22%	388

Source: Consumer Survey Q80/ Q82/ Q85/ Q88/ Q91/ Q94/ Q97/ Q100/ Q103/ Q106/ Q109/ Q112/ Q115 You said that you will get a [smart device]. Will this: be in addition to a non-internet connected version of the device; be to replace an older non-internet connected version of the device; be purchased instead of a non-internet connected version of the device; don't know? (Base = total of those who don't own each device type but plan to purchase one)

Consumers that reported that they were likely to get a new smart device within the next 12 months were asked the purpose of this: to use in addition to existing devices, to replace them, or as a new purchase in preference to a non-internet connected version. There were some differences in responses between categories; domestic appliances and thermostats were more likely to be purchased as replacements for existing non-connected devices, while other devices were more likely to be purchased instead of a non-internet connected version. It is worth noting that smart domestic appliances have a lower rate of respondents indicating that devices will be purchased in addition to non-internet connected versions of the device (13%). All nine connected domestic appliance subcategories show that this will be the case for less than 20% of respondents.

This may be because consumers reported that they are more likely to purchase smart domestic appliances as a replacement to existing non-smart versions of these products (36%). The categories with the highest rate of consumers purchasing devices to replace older non-internet connected versions of the device are smart microwaves and smart ovens. In both cases, 41% of respondents indicated that their purchases would be to replace an old, non-connected device.

This is in contrast to the four non-domestic appliance categories, for which only one subcategory (smart home thermostats) shows that devices will be purchased in addition to non-internet connected versions in less than 20% of cases.

The categories with the highest rate of respondents indicating that they would be purchasing the device instead of a non-internet connected one were smart washer/driers and smart coffee machines (both 27%), followed closely by smart kettles and smart dishwashers (both 25%).

Respondents who had previously indicated that they are unlikely to purchase a smart speaker, smart thermostat, smart lighting, smart security systems, or smart domestic appliances in the next 12 months, were asked to give their reasons for this.

Table 37: Reasons for not purchasing smart devices in the next 12 months

Reason for not purchasing smart devices	Percentage of respondents agreeing
I am not interested in the smart home	62%
There are not enough reasons for me to get any smart devices	49%
I am concerned about privacy of smart devices (e.g. device tracking me, listening in on me etc.)	30%
I am concerned about the security of smart devices (e.g. unauthorised access to my device)	28%
Smart devices are too expensive	25%
I don't know enough about smart devices	12%
I think smart devices are still in their infancy and would rather wait until they are more developed	12%
I am concerned about how smart devices work (e.g. access the internet, what they do etc.)	12%
I've heard bad things about some smart devices	8%
I am concerned about the quality of smart devices	4%
I will get smart home devices but not in the next 12 months	3%
Smart devices are not stylish enough/ I don't like their designs	1%
Other	7%
Don't know	3%
Base	1901

Source: Consumer Survey Q117 You've said that you are unlikely to purchase any of the following smart devices in the next 12 months: smart speaker, smart home thermostat, smart lighting, smart security system, smart domestic appliances. Which, if any, of the following are reasons for this? (n=1901 – all who are unlikely to purchase smart devices in the next 12 months)

Privacy and security are the third and fourth most common reasons for not wanting to purchase smart devices within the next year. This suggests that improving the security measures of IoT devices and providing consumers with more information could potentially increase the number of consumer IoT devices in UK households, and therefore increase the benefits felt by these consumers from device ownership.

Price sensitivity

The above table reflects that concerns over price were not in the top three reasons for avoiding smart devices, suggesting that this is not one of the major issues for potential consumers of IoT devices. That being said, "expense" was highlighted by 25% of respondents as one of the reasons that they will not be purchasing a smart device in the next 12 months, and was the fifth most popular reason. This suggests that although smart devices being too expensive is not one of the top deterrents, it is still something that influences potential consumers.

The 25% of respondents that selected "expense" as one of the reasons for avoiding purchasing smart devices were asked to detail how much they would be willing to spend on each device.

It is interesting to note that for every device type the two most common answers were the lowest price bracket and the option for not knowing how much you would be willing to pay. This reflects that consumers are often unwilling to pay high amounts for smart devices, or alternatively are unsure about how much they would be willing to pay.

Table 38: Mean willingness to pay by device type and product group

Product Group	Device	Mean willingness to pay	Price range (market study)	Mean willingness to pay by product group
Group 1: Big ticket items	Smart oven	£165.48	£869 - £1,149	£111.09
	Smart fridge freezer	£174.21	£1,199 - £6,999	
	Smart microwave	£61.87	n/a	
	Smart cooker	£166.52	£69.99 - £600	
	Smart dishwasher	£149.83	£398 - £1,349	
	Smart washer/ dryer	£168.41	£299 - £1,259	
	Smart toaster	£31.52	n/a	
	Smart coffee machine	£49.22	£179 - £2,147	
	Smart kettle	£32.76	£67.99 - £129.99	
Group 2: Connecting the home	Smart home thermostat	£54.99	£20.29 - £175.99	£56.48
	Smart home assistant/ speaker	£44.14	£14.95 - £409.00	
	Smart lighting	£41.12	£18.99 - £75.00	
	Smart security system	£85.68	£21 - £449.99	
Group 3: Consumer lifestyle*	Smart or connected children's toys and baby monitors	£34.29	£17.99 - £145.00	£34.29

**Note: This group includes some more expensive items such as tablets and smartphones that this question was not asked for due to their high level of ownership (ie barriers to ownership have been largely surmounted by the population).*

Source: Consumer Survey Q118 What is the maximum you would be willing to pay for each of the following devices (Base = all unlikely to purchase smart devices as they're too expensive)

The mean willingness to pay is highest for the product group 'big ticket items'; these devices are intrinsically the most expensive. However, as these quantitative responses were only given by the 25% of the respondents that explicitly said that price was a factor, and as "don't know" was a commonly-selected option, these statistics are indicative only. The key finding from this section of the research is that cost is not the major factor influencing purchasing decisions and deterring consumers from accessing IoT technology. It is interesting that the “willingness to pay” amount fell within some of the price bands reported in the market study, suggesting that there could be other more important factors than cost as a barrier.

Devices used by businesses

Overall, 42% of the respondents worked full time and 15% worked part time. Of these 3,083 respondents who were employed, 60% work in the private sector, 30% in the public sector, and 7% in the third sector.

Table 39: Respondents' organisation size

Organisation size	Percentage of respondents
Micro enterprise	21%
Small enterprise	12%
Medium-sized enterprise	13%
Large enterprise	45%
Base	3,083

Source: Consumer Survey Q122 Including yourself, approximately how many full-time employees are employed by your organisation in total in the UK? (n=3,083 – all respondents who work full/part time)

These respondents were asked whether the organisation they work for uses any consumer IoT devices.

Table 40: Organisations that use any type of smart device by size

Organisation size	Percentage of people whose organisation uses any smart devices
Micro	47%
Small	54%
Medium	53%
Large	55%

Source: Consumer Survey Q123 Does the organisation you work for use any of these consumer Internet of Things devices? (n=3,083 - all respondents who work full/part time)

Table 40 reflects that larger organisations are only slightly more likely to use any smart devices than small and medium-sized organisations.

Table 41: Organisations that use any type of smart device by sector

Organisation type	Percentage of people whose organisation uses any smart devices
Private sector	52%
Public sector	48%
Third Sector	52%

Source: Consumer Survey Q121 What kind of organisation do you work for? (n=1,542 – all respondents who said that their organisation uses at least one smart device)

The percentage of people whose organisation uses at least one smart device is slightly lower for those who work in the public sector, at 48%, compared with a 52% usage rate for private and third sector employees.

Table 42: Types of smart devices used by businesses

Device	Percentage of respondents whose employers use this device
Smart TVs	12%
Smart domestic appliances	2%
Smart thermostats	4%
Smart speakers	5%
Smart security system	7%
Smart lighting	6%
Smartphones	35%
Smart tablet	21%
Smart printers	13%
Other	3%
None of these	50%

Source: Consumer Survey Q123 Does the organisation you work for use any of these consumer Internet of Things devices? (n=3083 - all respondents who work full/part time)

Half of the respondents reported that their organisations do not use any types of consumer IoT devices. The most commonly used device is the smartphone, with 35% of respondents indicating that their organisation uses these. The second most common device is the smart tablet (21%), followed by smart printers (13%). This data again indicates that smart domestic appliances are fairly uncommon, with only 49 respondents (2%) indicating that their organisation uses any connected domestic appliance.

Overall, half of respondents indicated that their organisation uses at least one consumer IoT device. This means that these organisations currently face the risk of insecure IoT devices that consumers also face when owning devices for personal use, if appropriate security measures are not in place. The costs associated with these risks would be far higher for organisations using IoT devices, rather than individuals, as they are exposed to potential breaches on a much larger scale.

4. MANUFACTURERS OF IOT DEVICES

Summary

Evidence in this section comes from a survey of 22 consumer IoT manufacturers supplying consumer IoT devices to the UK market. The key findings on impacts of the proposed regulatory options are as follows:

Default passwords: Out of 17 respondents, only one indicated that any of their devices were produced with a default password. This was only the case for 1-10% of their products, and any amendment costs would be absorbed as a normal cost of business and would not be significant.

Vulnerability disclosure policies: The majority of respondents stated that they already had a vulnerability disclosure policy. Only one reported that they would stop selling some products in the UK. The overall cost to manufacturers of implementing aspects of this CoP guideline would be low or zero in many cases. **The average annual staffing cost of implementation across all companies was just £1,938 per manufacturer.**

Security updates: In contrast to the first two guidelines of the Code, few manufacturers in the survey sample currently publish a minimum length of time for which security updates would be provided for their products. Mandating aspects of this third CoP guideline therefore potentially affects more of the market, and it is also viewed as more time-consuming to implement. The average amount of staff time required would be 91.4 person-days, and **the average annual cost of staff time is estimated at £17,631.**

Physical IoT security label:
Manufacturers estimated that an average of 20.7 person-days would be required to implement mandatory physical labelling on all of their products. Direct estimates of costs ranged from £3,000 to £500,000. Combining both methods of estimation, **the average one-off cost of implementation is estimated at £100,630, or a median of £18,434.**

Manufacturers reported redesigning their products every 30.3 months on average, with most redesigning every 2-3 years. This suggests that with sufficient lead-in time, labelling could be built in to regular redesign processes, thus reducing the cost.

Estimated familiarisation costs for businesses:
Manufacturers estimated that familiarisation with the legislation based on aspects of the **top three CoP guidelines** would **require an average of 15.2 person-days, or equivalent to a one-off cost of £2,465.**

For the **product labelling** option, manufacturers estimated that 11.8 person days would be required on average for familiarisation. Incorporating one response that estimated that zero additional time was required, **the overall estimate of this one-off cost is just £1,585.**

Costs to manufacturers of product self-assessment:
Manufacturers estimated that an average of 30.1 person days per year were required to undertake self-assessment of compliance of their consumer IoT products, as part of their self-declaration to retailers. **The cost equivalent of this time is estimated at £6,575 annually.**

Where possible, these costs have been related to company turnover arising from IoT sales and averages calculated. These are summarised below.

Table 43: Cost of implementation as a share of turnover related to the sale of IoT

Policy element	Cost (share of IoT turnover)
Implementation: default passwords	0.01%
Implementation: vulnerability disclosure policy	0.03%
Implementation: minimum security update period	0.21%
All 3 code guidelines: familiarisation	0.03%
Recurring: product self-assessment	0.06%
Physical label: implementation	0.20%
Physical label: familiarisation	0.02%
One-off: cost of disposal of non-compliant goods	1.32%

Source: Manufacturer survey, March 2020

Profile of survey respondents

A bespoke contact list of manufacturers was assembled during the market study phase of the research. In total, 147 manufacturers were identified as being eligible to take part in our research, meaning that they produce at least one consumer IoT product which is currently available to UK consumers and had contact details available (a further 23 were not contactable).

We also contacted 12 manufacturers' associations to ask them to circulate the survey to their members, and the survey was publicised by RSM and DCMS through a variety of social media channels, including Twitter and LinkedIn. The survey received 22 valid responses[88], including some of the very largest manufacturers; therefore, although this response count is relatively low for a survey of this kind, it accounts for the views of 13% of the 170 UK consumer IoT businesses known to us from our research, and likely more than this fraction of consumer IoT sales in the UK. The full questionnaire is shown in chapter 8 of the Technical Report.

Table 44: Types of organisation by size (employment in UK consumer IoT production)

	Small companies (1 to 49 employees)	Medium companies (50 to 249 employees)	Large companies (250+ employees)	Number of employees unknown	Total
UK only based organisation	3	1	0	0	4
Multinational organisation with UK head office	0	3	3	0	6
UK branch/facility of multinational organisation	4	3	3	2	12
Total	7	7	6	2	22

Source: Manufacturers Survey Q5 and Q70, March 2020 (n=22)

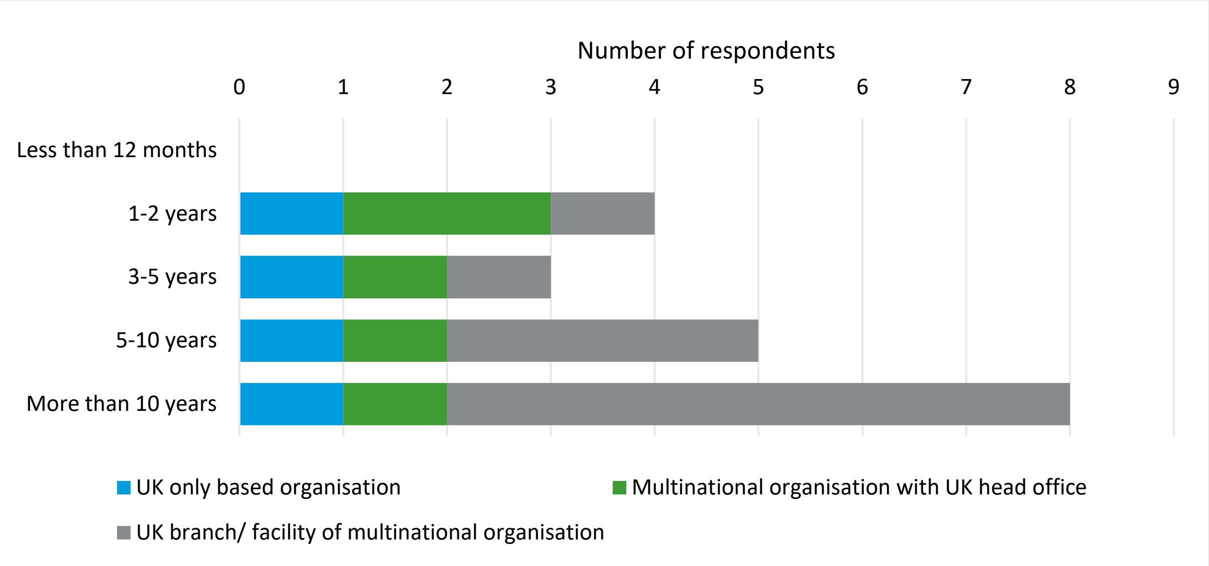
Where respondents did not submit information about their number of employees this information was identified from a search of published accounts and Companies House data (using RSM's proprietary "Tracker" tool which aggregates data from these sources, and Bureau van Dijk's 'Fame' database). This provides information about the overall size of the organisation, and it is not possible to separate out the number of employees involved in the manufacture of IoT from the total number of employees, or the turnover from IoT from the total turnover; however, where it

[88] 15 complete responses, 6 partially completed.

was clear that a company derived most or all of its sales from consumer IoT, we have used the published statistics. We received seven responses from small organisations with fewer than 50 employees, eight responses from medium-sized enterprises, and six from large companies.

The graph below shows the type of organisation by length of time in the IoT sector:

Figure 5: Type of organisation by length of time in sector



Source: Manufacturers Survey Q5 and Q12, March 2020 (n=20)

Nearly half of the respondents (40%) had been manufacturing consumer IoT products for the UK market for over ten years; this was the most common response, and was most frequently the case where the organisation is a UK branch of a multinational organisation. The next most common answer on the length of time in the industry is ‘five to ten years’, which was the case for five respondents distributed across UK based organisations, multinational organisations with a UK head office, and UK branches of multinational organisations.

Over half of respondents were UK branches of a multi-national organisation which produces consumer IoT devices for the UK market. Survey respondents were asked about their organisation’s main activities undertaken in relation to the production of consumer IoT.

As Table 45 shows, the most common activity was the design of consumer IoT products, which was undertaken by nearly all organisations of each type (81%). The second most common activity reported was the distribution or selling of consumer IoT products, which was cited by 15. The two least common activities selected were testing of consumer IoT products and manufacturing of components for consumer IoT products. Only two respondents indicated relevance for each of these two activities.

Table 45: Type of organisation and activity

	UK only based organisation	Multinational organisation with UK head office	UK branch/facility of multinational organisation	Total
Design consumer IoT products	4	5	8	17
Test consumer IoT products	0	2	0	2
Manufacture components for consumer IoT products	0	0	2	2
Manufacture finished consumer IoT products	1	4	6	11
Import components of consumer IoT products	0	2	1	3
Import finished of consumer IoT products	2	3	5	10
Distribute/sell consumer IoT products	2	4	9	15
Export consumer IoT products	0	2	1	3
Other	2	0	1	3
Total respondents:	4	6	12	22

Manufacturers Survey Q5 and Q6 (n=22)

Products sold by IoT manufacturers

The table below reflects the devices selected by respondents within the three product groups as produced by their organisation, broken down by organisation type.

Table 46: Type of device made by organisation type - total number of devices selected in each category

	UK only based organisation	Multinational organisation with UK head office	UK branch/ facility of multinational organisation	Total
Big ticket items (7 products)	0	0	6	6
Connecting the home (8 products)	7	10	18	35
Consumer lifestyle (7 products)	1	2	11	14

Manufacturers Survey Q5 and Q8-Q10 (n=21). Note that each manufacturer could select more than one device in each category.

The most common product group was ‘connecting the home’, with individual types of product in this group selected 35 times by respondents as produced by organisations. Overall, the most common device type manufactured was found to be smart home thermostats, with this being manufactured by eight respondents.

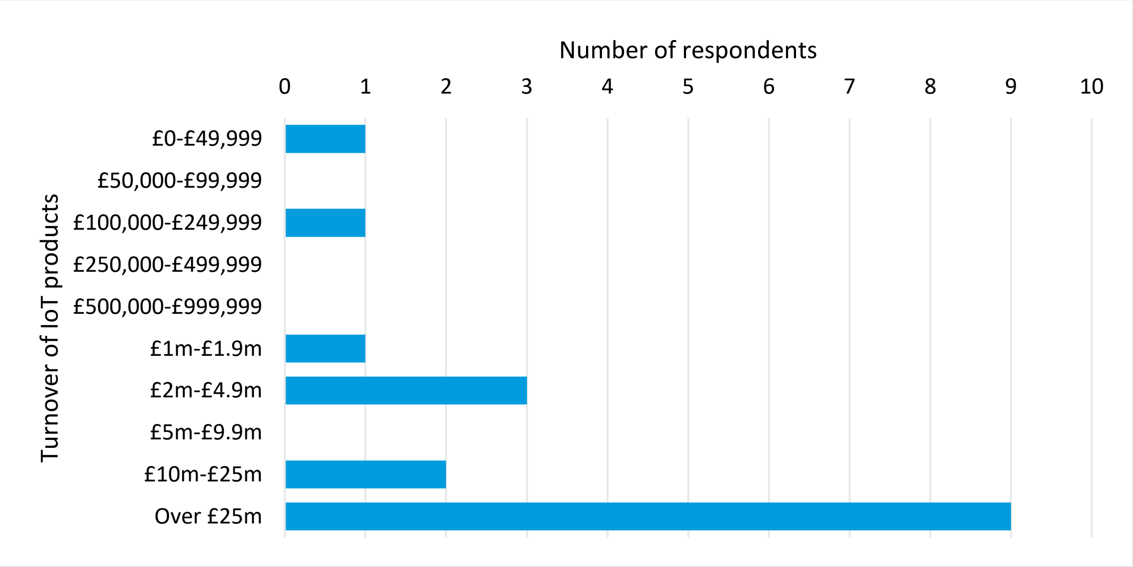
The category ‘other smart connecting the home device’ also had eight responses. These included smart energy/electricity monitors, smart water leak detectors, smart plugs and sockets, smart motion sensors, and smart printers. The third most common device produced by respondents was wearable health trackers, which are manufactured by five of the survey respondents.

Respondents were also asked about the number of product lines produced, including individual versions of the same product, produced for sale in the UK. Most manufacturers (61%) had between one and 15 product lines. Production of more than 15 product lines was less common, with this being the case for only seven respondents out of 18 responses.

The average number of devices produced was 21, and the median number of product lines was eight – reflecting the fact that the distribution is very skewed by a small number of manufacturers with very large numbers of product lines. For small businesses, the average number of product lines was 20. For medium sized businesses, it was 22, and for the large businesses 18. This suggests there is little relationship between the size of businesses and the number of product lines.

We asked manufacturers about their turnover from selling consumer IoT devices in the UK in the last 12 months.

Figure 6: Turnover from sales of IoT products in the last 12 months



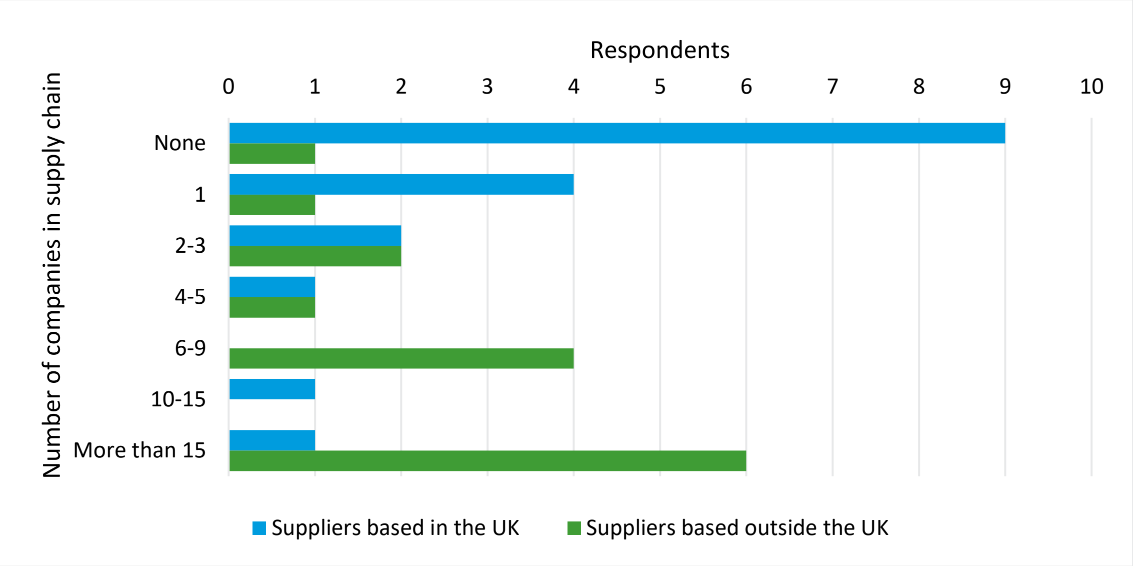
Manufacturers Survey Q13 (n=17)

There were eight survey responses to this question, and results were supplemented with overall turnover data from published accounts where available.

Supply chains

Respondents were asked about the number of companies in the manufacturers' IoT supply chains, both in the UK and outside the UK:

Figure 7: Number of companies in manufacturer supply chains, by supplier location



Manufacturers' Survey Q14 (n=18) and Q15 (n=15)

Overall, 18 respondents provided information about their number of UK based suppliers, and 15 provided information about the number of suppliers based outside the UK. Nine organisations reported having no UK-based suppliers in their supply chain. On average, respondents had 2.3 companies in their supply chain based in the UK and 9.1 suppliers based outside the UK. This is based on taking the midpoint of each band (where they contain more than one number), multiplying by the number of responses and dividing by the number of respondents.

Manufacturing is a global industry, with supply chains located across many different countries. Those respondents that indicated they had suppliers outside of the UK were asked which continent they were based in.

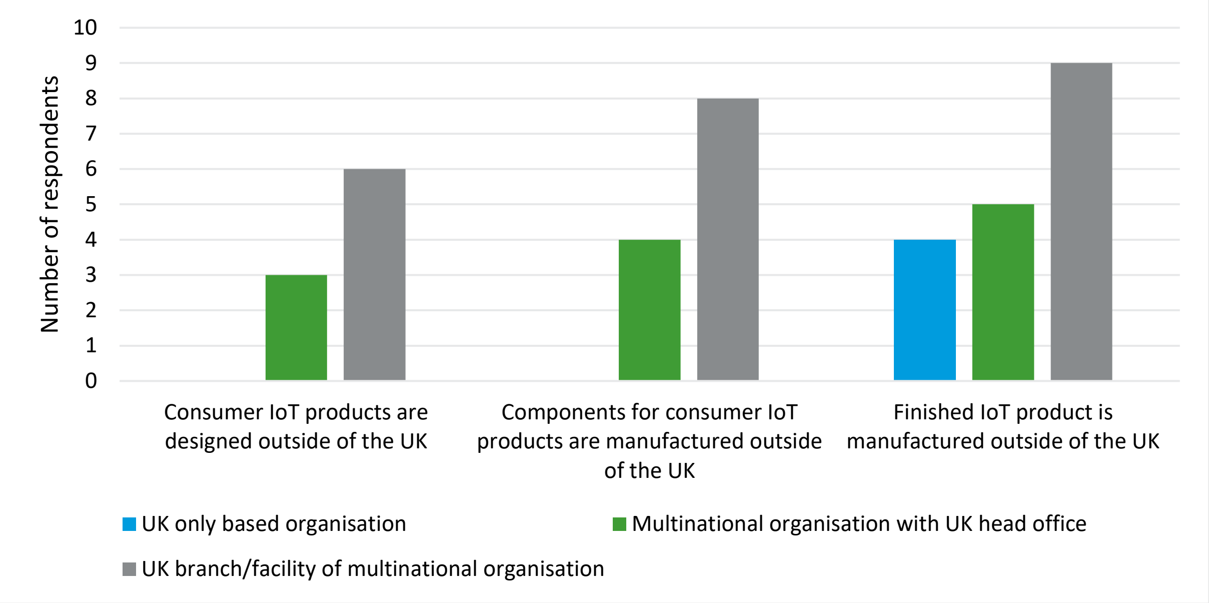
Table 47: Regions where non-UK based suppliers are located

Region	Number of organisations producing in this region	Percentage of organisations producing in this region
Asia	17	94%
Europe	5	28%
North America	2	11%
South America	1	6%
Africa	0	0%
Oceania	0	0%

Manufacturers Survey Q18 (n= 18)

All but one said that some or all of their overseas supply chains were based in Asia, with Europe the second most common location. 17 respondents used suppliers based in China, three had suppliers in Vietnam and two with suppliers in Taiwan, while one used suppliers in Japan.

Figure 8: Activities of companies in non-UK supply chain by type of organisation



Source: Manufacturers' Survey Q16, March 2020 (n=18)

Respondents were asked which of their IoT devices were manufactured outside the UK. Results are shown only for where the whole device was manufactured outside the UK. Some explained it was therefore hard to answer this question because components were often produced overseas and the final assembly was UK based. For example, the 'dumb' device was constructed overseas and the 'smart' technology was installed in the UK. Results are summarised below by product category.

Table 48: Whole devices manufactured outside the UK

	Number of devices wholly manufactured outside the UK
Big ticket items	11
Connecting the home	24
Consumer lifestyle	14
Total	49

Source: Manufacturers Survey Q17, March 2020 (n=19)

Table 49: Product development lifecycle

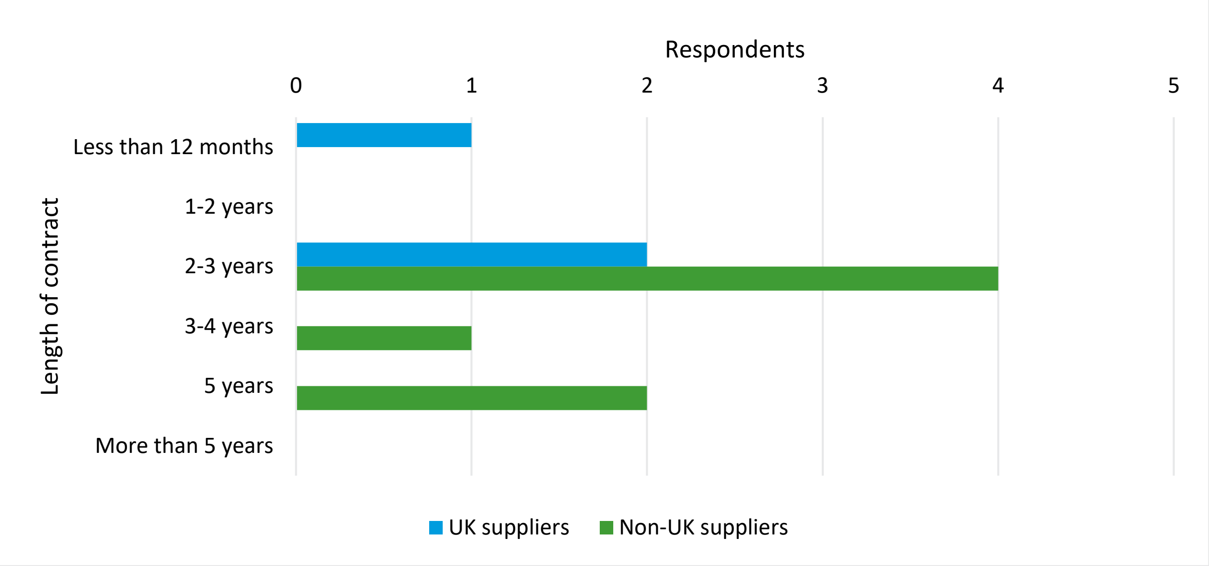
	Less than 12 months	12-18 months	18-24 months	2-3 years	4-5 years	More than 5 years	Average (months)
Big ticket items	0	1	3	1	0	0	22.8
Connecting the home	0	9	5	0	0	0	17.1
Consumer lifestyle	0	7	2	0	0	0	16.3
Total	0	17	10	1	0	0	17.9

Manufacturers' Survey Q20 (n=11)

Table 49 shows that most product development lifecycles are between one and two years. 'Big ticket' items on average have a longer development cycle than devices for 'connecting the home' or 'consumer lifestyle' devices, but this is based on a very small sample of 11.

Respondents were also asked about the length of contracts with suppliers:

Figure 9: Length of contract by supplier



Source: Manufacturers' Survey Q21, March 2020 (n=8

Only eight manufacturers answered this question. The average contract length for UK suppliers was just over one year (16 months). The midpoint of the band has been used to estimate the average by multiplying by the number of responses in each band and dividing by the total number of respondents to the question. The average contract length for non-UK suppliers was 31 months. However, this is based on a low number of responses, which was three for non-UK suppliers, and seven for UK-based suppliers.

Manufacturer awareness of cyber security for consumer IoT

Manufacturers were asked about the security standards they used to design and manufacture IoT products. 16 respondents gave an answer, some mentioning multiple different guidelines and standards. Of these:

- 4 respondents said they were aware of the Code of Practice for consumer IoT security (CoP), and either contributed to its development or were early signatories. There were also two respondents who made reference to other UK guidelines for cyber security. Of these, one cited the National Cyber Security Centre Cloud Security Principles.[89] The other was a smart meter manufacturer who said that as part of the government smart meter programme there was a mandatory compliance test for device to meter communications;
- 8 said they used European standards including ETSI TS 103 645;
- 4 mentioned the ISO27000 series, which 'provides requirements for an information security management system'[90];
- 3 said they complied with the IoTSF guidelines;

[89] https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles

[90] https://www.iso.org/isoiec-27001-information-security.html

- 1 smart thermostat manufacturer said they used the ISA/IEC 62443 series guidelines, which provides a framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems[91];
- 1 respondent reported that they build to the NIST IoT Cybersecurity Framework[92];

The survey also asked about awareness of the UK Code of Practice for Consumer IoT Security before being contacted about the survey. There were 16 responses for this question of which 13 (81%) said they were 'well aware' of the CoP, and three (19%) said they were aware to some extent. None were unaware of it before responding to the survey.

Note on cost information

When asked to estimate staff costs arising from proposed new regulations, companies were asked to either summarise costs in cash terms or provide the amount of staff time that would be required. In the latter case, respondents were asked to provide staff cost estimates by job role and number of person days. These were then converted to a cash equivalent. Salary assumptions for this calculation are taken from national careers service data (nationalcareers.service.gov.uk), and have been adjusted to employment costs (including non-salary costs such as employer National Insurance contributions) and are summarised below:

Table 50: Salary assumptions

Role	Daily Rate	Annual	Job role from national careers service
IT or technical director or equivalent	£426	£110,663	Head of IT
IT specialist manager	£205	£53,345	Test lead IT
IT professional or technical role	£181	£47,103	Robotics engineer
Non-IT professional role (e.g. legal, accounting)	£229	£59,588	Company secretary
Administrative	£116	£30,078	Office manager
Sales and marketing professional	£166	£43,130	Retail merchandiser
Other	£124	£32,284	Average national wage (ONS)

Source: National Careers Service average salary data

Each job description provides a salary range for each role and the annual salary is the median point of this range. Daily rates are calculated from the annual figure using https://wageindicator.co.uk/pay/hourly-pay-converter .

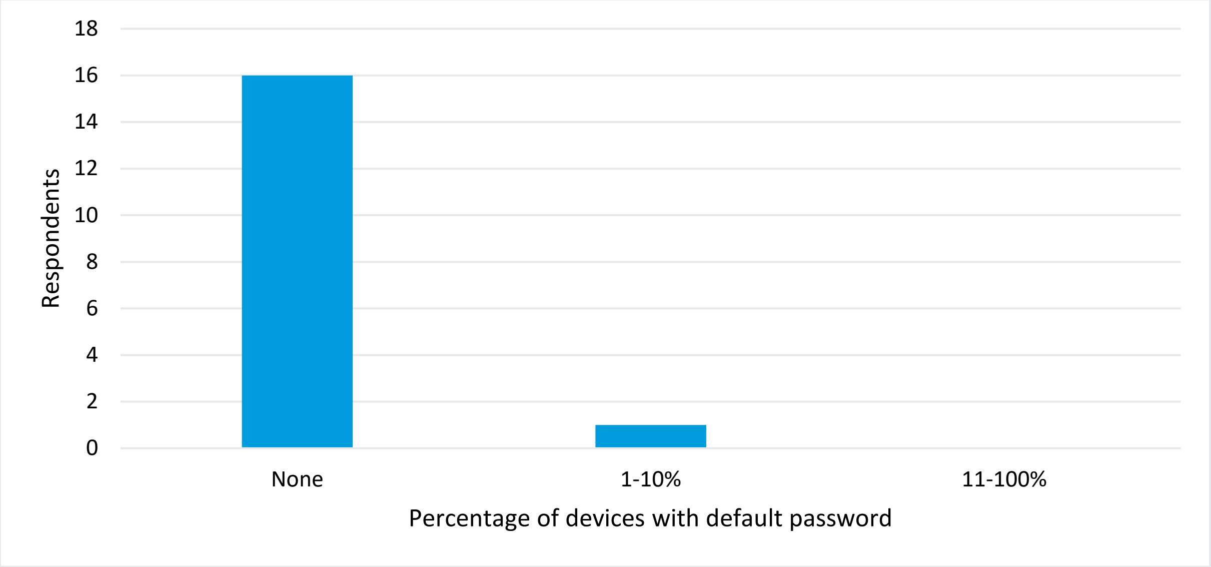
Tables showing the staff costs for each element of the proposed regulations follow in the analysis below. Please note that in each case, the contribution of each role to the overall cost is averaged across all respondents; if there are 10 respondents to a question, and only 1 of them assigned a cost to their IT director, and that cost was £1000, the average contribution to overall costs of IT directors would be £100 (£1,000/10).

Default passwords

In order to assess the potential impact of mandating aspects of the top three CoP guidelines, respondents were asked about their production in relation to the use of default passwords.

[91] https://www.isa.org/intech/201810standards/
[92] https://www.nist.gov/itl/applied-cybersecurity/iot-cybersecurity

Figure 10: Proportion of products manufactured with default passwords



Source: Manufacturers' Survey Q24 (n= 17)

Only one of the 17 respondents indicated that any of their devices are produced with a default password, and this was only the case for 1-10% of their products. This reflects the fact that many organisations are already aware of the security issues caused by the use of default passwords, and as such are already compliant with the first UK CoP guideline that devices should not be sold with default passwords.

However, it is worth noting that six of the survey respondents did not answer this question. There is an incentive for respondents not to provide an estimate of products produced with default passwords as this would indicate that their organisation is currently not compliant with the voluntary UK CoP. It is possible that this was the case for the respondents that chose to skip this question, resulting in a bias for only complaint companies answering this question.

The one organisation that indicated that some of their devices are produced with default passwords is a small multinational organisation, which has produced for over 10 years. The products they produce include smart speakers, smart security cameras, smart doorbells, smart home thermostats, smart lighting, and 'other' connecting the home products.

The respondent indicated that all of their 'other smart consumer lifestyle devices' are currently produced with a default password. This was detailed by the respondent to include a 'driver manager unit for home automation'. They were asked how they would respond to regulation mandating that all passwords for consumer IoT products must be unique and not resettable to a universal factory setting, and answered that their organisation would redesign some consumer IoT products for sale in the UK to have a unique password.

They said that this would involve:

- redesigning existing product lines to comply;
- use of an alternative method of authentication (eg remove the use of passwords); and
- remotely updating passwords so that they are unique.

The one option offered that they did not believe their organisation would pursue as a result of the proposed legislation was to 'completely remove any default passwords in IoT devices'. The indication of multiple responses perhaps suggests that this non-compliant company was unsure of how best to redesign or adjust product lines in order to become compliant with the no default password guideline of the UK CoP. Alternatively, it is possible that different responses could be expected to be used for different kinds of products, as this respondent indicated that they produce several types of consumer IoT device.

The respondent was also asked about the expected staff time costs to redesign products to comply with the regulation. However, they were unable to estimate both the expected staff time and overall cost of implementation. The respondent did, however, indicate that none of the costs associated with measures to ensure compliance would be passed on to the consumer.

When asked about the impact of any potential future legislation mandating that devices are sold without default passwords, they reported that old product lines would be redesigned, while newer versions would all have unique passwords. They did not indicate that any product lines would have to be discontinued as a result of the changes in legislation.

The respondent indicated that they did not know how long it would take to implement the new requirements.

Vulnerability disclosure policies

Overall, 12 respondents (out of 16 who answered the question) indicated that they have a vulnerability disclosure policy, while three said that they did not, and one indicated that they did not know whether this is currently in place. They were then asked how they would respond to the proposed policy option of mandating a vulnerability disclosure policy, with respondents able to select multiple relevant answers.

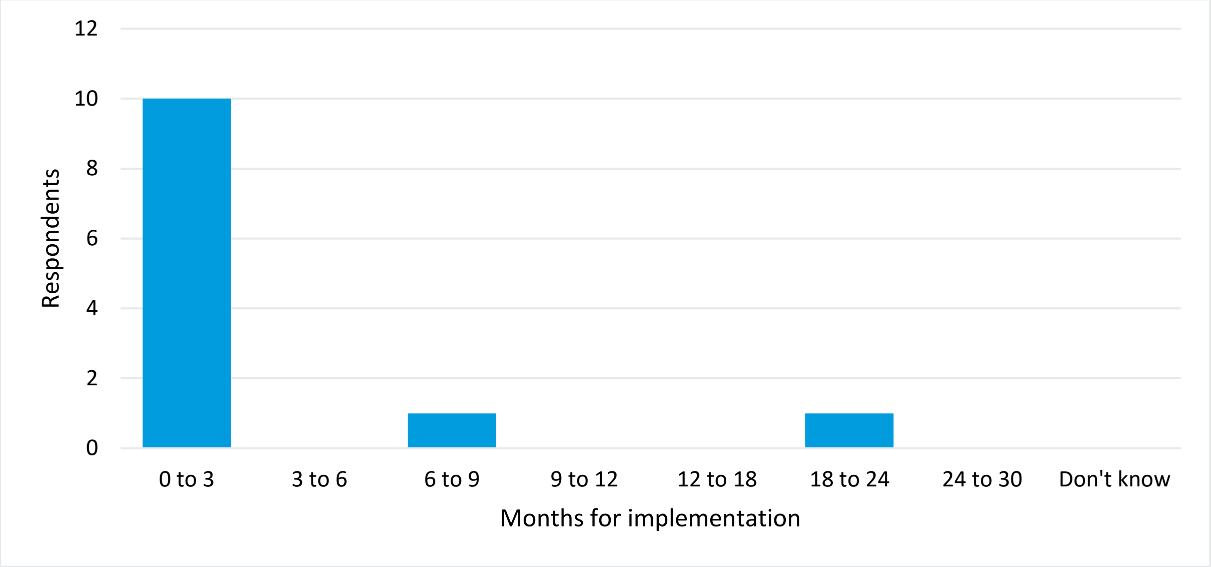
Table 51: Response to proposed vulnerability disclosure policy

	Respondents
Take no action	6
Introduce a public point of contact and VDP/CVD for SOME consumer IoT products in the UK market	0
Introduce a public point of contact and VDP/CVD for ALL consumer IoT products in the UK market	5
Stop producing SOME consumer IoT products in the UK market	0
Stop producing ALL consumer IoT products in the UK market	0
Stop selling SOME consumer IoT products to the UK market	1
Stop selling ALL consumer IoT products to the UK market	0
Continue to produce these products without a public point of contact in other markets outside the UK	0

Source: Manufacturers' Survey Q50, March 2020 (n=12)

The table above shows that the majority of respondents who answered this question would not have to take any action if a vulnerability disclosure policy was mandated. This reflects that most respondents indicated that their organisation already has a vulnerability disclosure policy in place. The most common response would be to introduce a public point of contact and vulnerability disclosure policy for all consumer IoT products in the UK market, directly addressing the issue. One respondent indicated that they may stop selling some consumer IoT products to the UK market, but this was the only response suggesting that legislation would affect the production or sale of an organisations' products. Overall, it appears that most organisations would choose to directly address the fact that they do not have a vulnerability disclosure policy in place, and simply implement one as their response.

Figure 11: Time required to implement the requirement for a vulnerability disclosure policy



Source: Manufacturers' Survey Q51, March 2020 (n=12)

As shown here, most respondents believed that the time taken to respond to legislation mandating the use of a vulnerability disclosure policy would be under three months.

The respondent that indicated a six to nine month timeframe noted that they do already have a vulnerability disclosure policy in place, but would need additional legal advice to ensure that their policy was compliant and in line with the wording of any potential legislation. The respondent that indicated an 18 to 24 month timeframe indicated that their action would involve the implementation of a vulnerability disclosure policy, but may also require their organisation to stop selling some consumer IoT products to the UK market. This was a UK branch/facility of a large multinational organisation.

Manufacturers were asked to estimate the amount of staff time that would be needed in order to implement any changes as a result of legislation mandating the use of a vulnerability disclosure policy.

Table 52: Staff cost estimates to implement vulnerability disclosure policies

	Average Number of Person Days	Total estimated costs	Respondents who say this job role would be involved
IT or technical director or equivalent	3.6	£1,516	4
IT specialist manager	3.9	£798	2
IT professional or technical role	14.4	£2,613	2
Non-IT professional role (eg legal, accounting)	1.0	£236	2
Administrative	4.0	£465	3
Sales and marketing professional	1.0	£171	1
Other (please specify)	0.0	£0	0
	28.0	£5,799	4

Source: Manufacturer Survey Q53 (n=4)

There were a mix of responses, with one organisation indicating that time would likely be used across all the job roles listed above. On average, respondents said it would take 28.0 person-days per year and would mostly be the responsibility of IT professional or technical staff.

Six other respondents provided cash estimates directly. Of these, five said the cost would be £0, while one stated the cost would be one day (but did not specify the job role, so it has been coded as "other"). Results of all cost estimates range from £0 (because VDPs are already being implemented) to £15,863 by one larger company – this is however equivalent to less than 0.01% of their IoT turnover. **The average cost per manufacturer to implement a vulnerability disclosure policy, taking into account those who are already compliant and estimate the cost at zero, is £1,938** (the average of the non-zero responses is £4,652).

Table 53: Summary of costs reported for implementing vulnerability disclosure policies

Size (Employees)	Size (Turnover)	Estimated staff costs	As % of turnover
Medium	£10m - £25m	£0	0%
Large	Over £25m	£0	0%
Medium	Over £25m	£936	<0.01%
Large	Over £25m	£15,863	<0.01%
Small	£2m - £4.9m	£6,025	0.19%
Medium	£10m - £25m	£0	0%
Small	£2m - £4.9m	£62	<0.01%
Small	£2m - £4.9m	£0	0%
Large	Over £25m	£0	0%
Unknown	Unknown	£0	0%
Medium	Over £25m	£373	<0.01%
Medium	Over £25m	£0	0%

Source: Manufacturer Survey Q52 & Q53 (n=12)

Manufacturers were also asked to provide an estimate of the annual staff cost of providing a public point of contact. Eight out of 14 indicated that the additional cost to their business would be zero as this is already provided. Just one of the those who indicated that there would be costs was able to estimate these, and estimated staff cost to be £5,000.

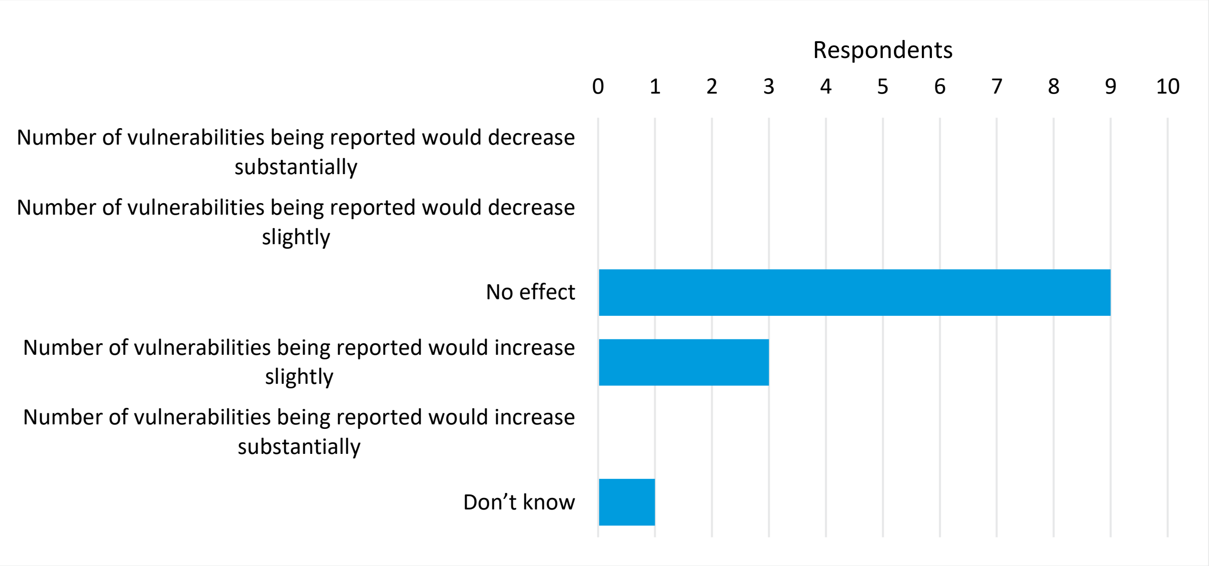
Respondents were then asked to estimate the total annual cost of implementing a public point of contact for vulnerability disclosure reporting, including the staff time already estimated, and any additional costs such as external advice or hiring/training staff. Again, the majority of responses indicated that there would be no additional cost as their organisation was already compliant. Of the others:

- One respondent indicated that the overall cost would be negligible when considered in relation to the cost of doing business and the money already spent on security such as penetration testing.
- One respondent suggested that the only cost would be in relation to law (eg certification of timeline) but that this cost could not be quantified without reviewing the wording of any potential legislation.
- One respondent did provide an estimate of a figure for the overall total cost, which was £12,000.

- One respondent reported that as well as the staff costs, they had a £100,000 bounty held in escrow with the reporting company.

The table below shows the anticipated impact predicted by respondents of mandating that manufacturers have a public point of contact and implement a vulnerability disclosure policy on the number of vulnerabilities that are reported.

Figure 12: Impact of proposed legislation on number of vulnerabilities reported

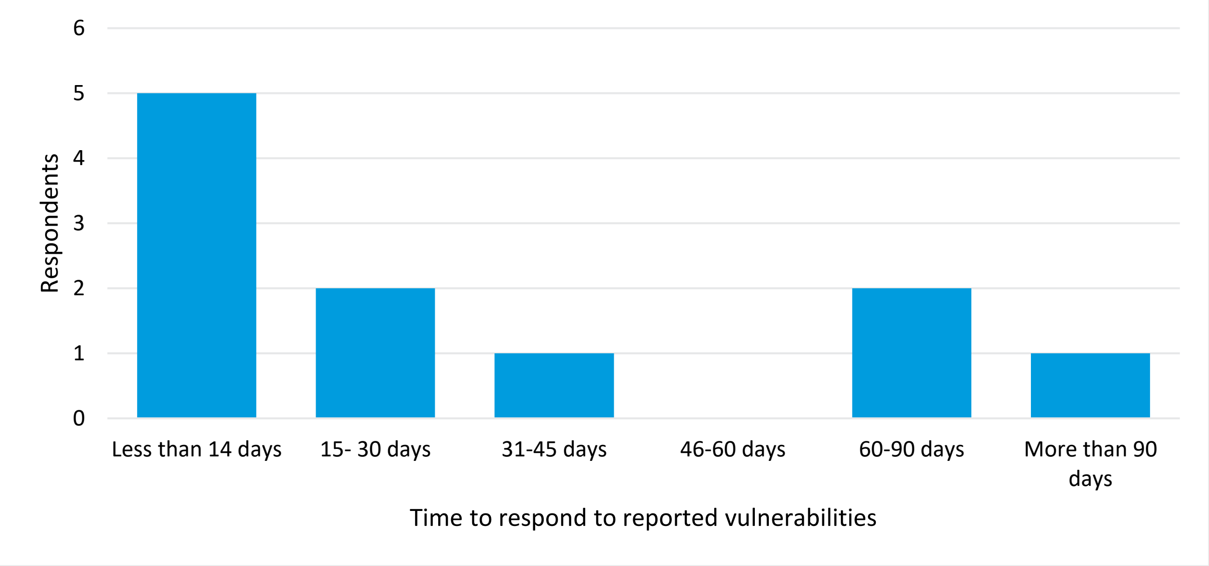


Source: Manufacturers' Survey Q55 (n=13)

Figure 12 shows that the majority of respondents suggested that the mandatory implementation of a vulnerability disclosure policy would not have an impact on the number of vulnerabilities reported. Only one respondent indicated that they thought this would increase the number of vulnerabilities reported, and this was suggested to be only slightly.

Finally, respondents were also asked about how long it would take to respond to a reported vulnerability.

Figure 13: Time taken to respond to reported vulnerabilities



Source: Manufacturer' survey Q56 (n=13)

These answers reflect that the response time for reported vulnerabilities can vary by organisation, and several respondents noted that response time within organisations tends to vary depending on the type and extremity of the vulnerability reported.

Providing security update information

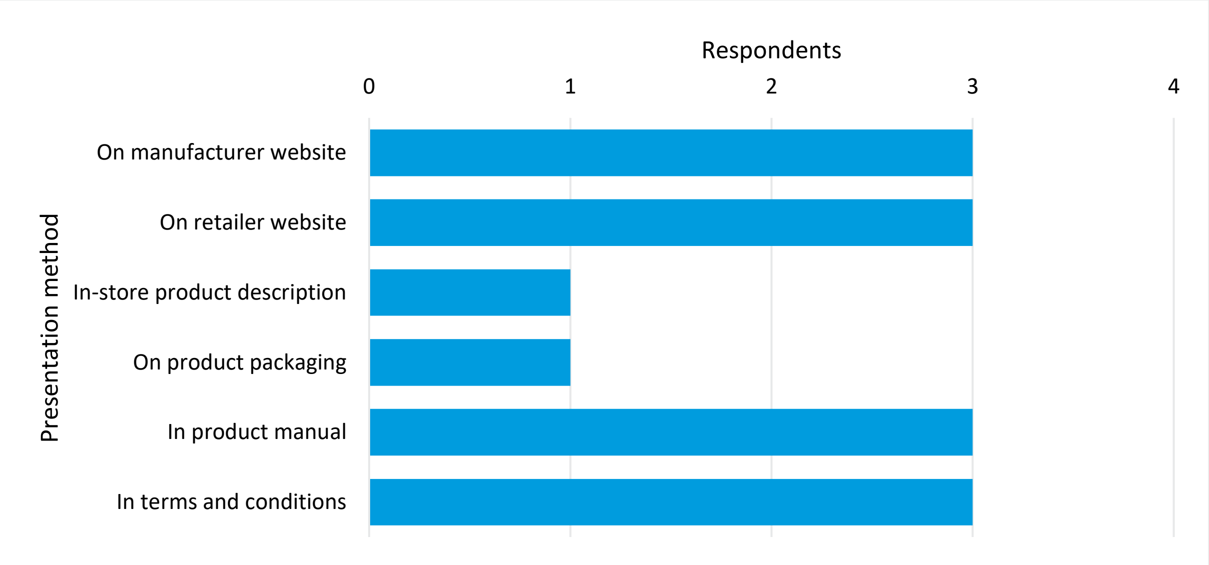
Respondents were asked for details about their current compliance with the third UK CoP guideline - that devices should have timely updates and it should be explicitly stated the minimum length of time for which these security updates will be supported.

Seventeen respondents answered this question, of which:

- four (24%) responded that all of their products provided this information;
- one (6%) responded that between 11 and 20 percent of their products provided this information; and
- 12 (71%) responded that none of their products provided this information.

The five respondents who did provide this information on at least some of their products were asked how it was provided:

Figure 14: Current presentation of security update information



Source: Manufacturers' Survey Q36, March 2020 (n=14)

This shows that security update information currently provided by manufacturers is presented to consumers in a range of ways. The use of retailer websites, product manuals, and manufacturers websites were the three most common responses, with three respondents indicating each of these methods. One respondent from a large multinational company commented that on-product packaging was of decreasing relevance for a number of different types of product (e.g. big-ticket items and mobile phones, which are often sold online or from a showroom without the packaging ever being seen) and that online information was much easier to deploy as it could be updated remotely.

Table 54: Response to proposed declaration of minimum period for security updates at point of sale

	Respondents
Take no action	0
Provide information on minimum period of security updates at the point of sale for SOME consumer IoT products for sale in the UK	0
Provide information on minimum period of security updates at the point of sale for ALL consumer IoT products for sale in the UK	12
Stop producing SOME consumer IoT products in the UK	1
Stop producing ALL consumer IoT products in the UK	0
Stop selling SOME consumer IoT products to the UK market	2
Stop selling ALL consumer IoT products to the UK market	0
Continue to produce products without stating minimum periods for security updates in other markets outside the UK	0
Total responding to this question	12

Source: Manufacturers' Survey Q37, March 2020 (n=12)

All respondents to this question indicated that they would act directly in order to become compliant, by providing information on the minimum period of security updates for all of their consumer IoT products for sale in the UK. Respondents were able to select more than one course of action and two organisations also indicated that they would stop selling some of their consumer IoT products as a result of the proposed legislation, and one would stop producing some of their products. None of the respondents indicated that they would have to stop producing or selling all of their consumer IoT products, and none would choose to continue producing products without stating the security update periods for markets outside of the UK.

The table below shows which job roles organisations believed would be involved in implementing the necessary changes, as well as the expected amount of staff time needed for the redesigning of processes and products to this effect. Overall, five respondents answered this question, with all but one indicating that staff from multiple job roles would be required.

As with estimates for implementing a vulnerability disclosure policy, there were a mix of responses for this question. There were several respondents indicating that time would be needed for each of the roles defined in the question. On average, respondents indicated that it would take 91.4 person-days to implement the changes needed to become compliant with the proposed legislation (one off cost). Their answers suggested that this would be mostly within IT professional/technical roles, and sales and marketing roles. The cash equivalent of this time is estimated at £17,631, as set out in the table below.

Table 55: Staff costs to provide security update information

	Average Number of Person Days	Total estimated costs	Respondents who say this job role would be involved
IT or technical director or equivalent	10.1	£4,287	4
IT specialist manager	10.34	£2,114	3
IT professional or technical role	14.6	£2,653	5
Non-IT professional role (eg legal, accounting)	11.6	£2,650	4
Administrative	16.2	£1,877	5
Sales and marketing professional	11.9	£1,975	5
Other (please specify)	16.7	£2,075	2
Total respondents	91.4	£17,631	6

Source: Manufacturer Survey Q40 (n=6)

Respondents were also able to respond to this question in free text, and three respondents did not provide an estimate for their staff cost but suggested that it would likely be low, with one saying that it would be minimal as it would only involve updating online/user guide content.

Table 56: Summary of staff costs to implement security update information

Size (Employees)	Size (Turnover)	Estimated cost	As % of turnover
Medium	£10m - £25m	£400	<0.01%
Large	Over £25m	£5,989	<0.01%
Medium	Over £25m	£0	0.00%
Large	Over £25m	£72,525	0.01%
Small	£2m - £4.9m	£0	0.00%
Small	£2m - £4.9m	£2,729	0.14%
Medium	Over £25m	£16,394	0.02%
Medium	Over £25m	£7,752	0.01%

Manufacturer Survey Q39 & Q40 (n= 8)

Manufacturers were also asked to estimate the total annual cost of implementing and publishing a minimum security update period, including the cost of staff time and additional costs, such as external advice or training/hiring new staff. Only two respondents provided an estimate, which were £10,000 and between £25,000 and £50,000 respectively. Three respondents indicated that it would be difficult to estimate this cost in such a short time.

The overall annual average, including detailed responses itemising the staff time, and direct estimates of total costs, is £13,224 per manufacturer.

The overall lack of cost estimates by respondents likely reflects the perceived difficulty in estimating these costs without further details of the legislation and more time to calculate a figure.

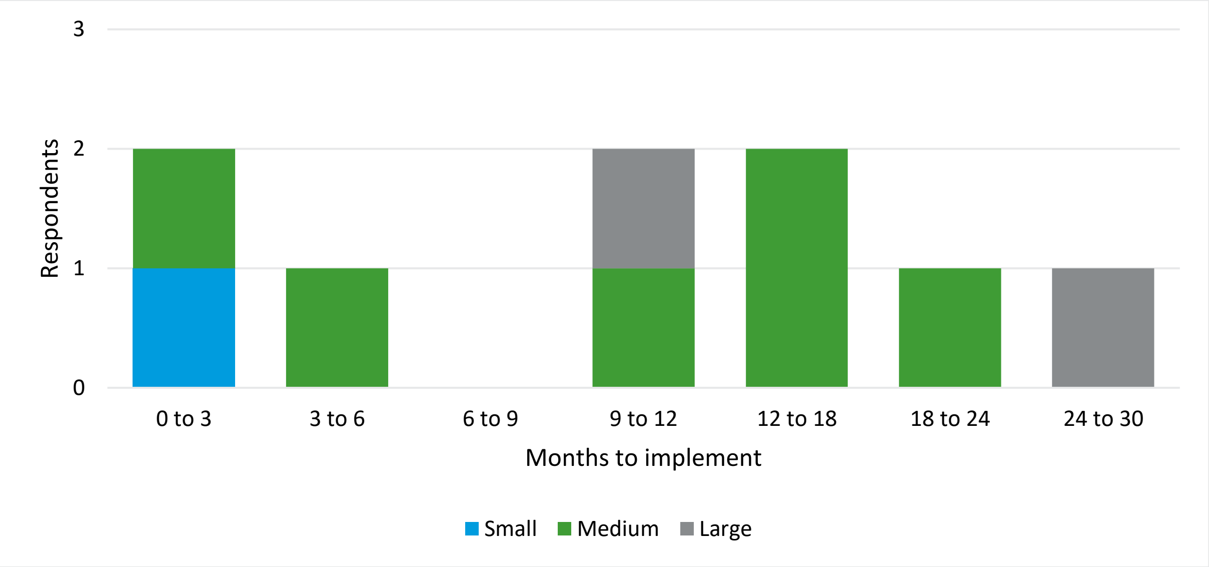
Respondents were also asked to estimate what percentage of the cost of their response to the legislation would be passed on to their consumers. Eight answered this question of which:

- 3 said that 100% of costs would be passed to the consumer;
- 2 said that some of the costs would be passed to the consumer; and
- 3 said that none of the costs would be passed to the consumer.

There did not appear to be a strong relationship between distribution of cost and organisation size, particularly as the majority of respondents (63%) were of the same organisation size (medium). The two large organisations that responded both indicated that none of the costs would be passed to consumers. Only one small firm answered this question, and indicated that some of the costs would be passed to consumers. However, of the remaining medium sized firms that responded, three indicated that all costs of implementing this requirement would be passed to consumers, one that none would be passed along, and one indicated that some of the costs would be passed to consumers.

The survey also asked respondents to estimate approximately how long it would take to implement a minimum security update period for their consumer IoT products, and present this to consumers.

Figure 15: Time to implement a minimum period for security updates for consumer IoT products by manufacturer size



Source: Manufacturers' Survey Q43, March 2020 (n=9)

This graph reflects that the time taken to implement any changes needed to become compliant varies by organisation, with the results spread fairly evenly from zero to 30 months. The small organisations that responded to this question indicated the shortest expected length of time to respond to the proposed legislation, perhaps because they produce fewer products.

Finally, respondents who had indicated that they do not currently state the minimum length of time for which security updates will be supported were asked the reasons for which this has not yet been presented to consumers.

- 6 respondents stated that these details were not part of the organisation's design process;
- 10 respondents selected 'other'. One respondent highlighted that their end of life policy depends on several factors such as customer demand, supply of components, user experience of the impact of updates, and the cost of supporting a product or service. As such, they do not always implement an update policy upfront. Another respondent suggested that it is difficult to give details of and guarantee a minimum time period as this could be impacted by external factors such as operating systems not being supported. One respondent highlighted that their organisation currently provides security

updates as vulnerabilities are reported. One said they already support all products with the security updates they require, but can't predict when those might be needed, and are reluctant to state because they would still update after that period was over.

None of the respondents selected any of the following reasons for not already stating the minimum period of security updates:

- was not aware this was an issue; or
- don't know.

Impact on manufacturers of self-assessing compliance

The survey asked how organisations might redesign or change processes to comply with aspects of the top three CoP guidelines, and 15 responses were received for this question.

Table 57: Redesigning and changing processes

	Respondents
All older versions of the product would be re-designed and newer versions of those products would be compliant	4
Some older versions of the product would be re-designed and newer versions of those products would be compliant	2
Older versions of the product would be discontinued and only newer versions of the product that are compliant would be produced	2
No versions of the product (old or new) would be compliant and therefore would not be sold in the UK	0
Already compliant	4
Other	3
Total (Respondents)	15

Source: Manufacturers' Survey Q57, March 2020 (n=15)

Four respondents said they were already compliant with the relevant aspects of the top three guidelines, so would not need to take any action. One respondent said the only thing they would need to add was information about security updates and this would not require significant redesign or changes to their processes. None of the respondents said they would stop making products for the UK market.

The survey asked if people would pay for external assurance or consultancy services for familiarisation or self-assessment of compliance. Four of the 13 respondents said they would pay for self-assessment, one said they would pay for both and the rest said they would not pay for either. When asked to estimate costs for this process, they reported that it was difficult to estimate, but seven respondents were able to break down the costs of self-assessment in staff time, as shown below.

Respondents were asked to estimate the number of person-days undertaken by each job role that may be involved in the self-assessment process. To estimate the average number of person days, we have used the mid-point number of hours in each band multiplied by the number of responses, and divided by the total number of respondents (seven), and then divided by eight to show the results in person days. On average respondents said it would take around 30.1 person days per year and would mostly be the responsibility of IT or technical directors, managers and/or professionals. The cash equivalent of this time is estimated at £6,575, as set out in the table below. This represents the total overall cost per year for the organisation.

Table 58: Staff costs of self-assessment/compliance

	Average Number of Person Days	Total estimated costs	Respondents who say this job role would be involved
IT or technical director or equivalent	4.2	£1,782	6
IT specialist manager	5.6	£1,149	3
IT professional or technical role	17.8	£3,233	5
Non-IT professional role (e.g. legal, accounting)	1.0	£219	3
Administrative	1.0	£111	4
Sales and marketing professional	0.4	£73	3
Other (please specify)	0.1	£9	1
Total respondents	30.1	£6,575	7

Source: Manufacturer Survey Q62 (n=7)

Respondents were also able to provide this estimate as a free text question. One medium sized company estimated costs at £100,000 (equivalent to 0.04% of their overall turnover), but said this was based on the overall costs to test a device, i.e. not just for top three compliance. Excluding this response as an outlier, **the average cost of compliance is £6,261 as set out above.** This represents the total overall cost per year for the organisation**.** The impact varied by size of company, as set out in Table 59 Table 59 below; in no case was it greater than 0.11% of company IoT turnover.

Table 59: Summary of responses

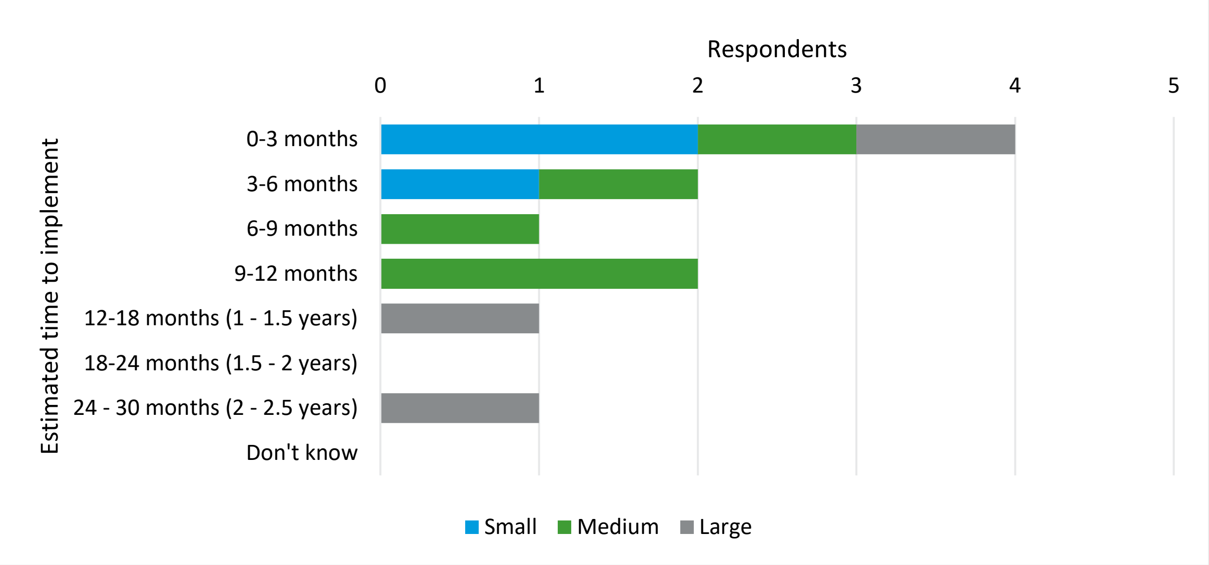
Size (Employees)	Size (Turnover)	Estimated staff cost	As % of turnover
Medium	£10m - £25m	£3,457	0.02%
Large	Over £25m	£3,682	<0.01%
Medium	Over £25m	£100,000	0.04%
Large	Over £25m	£24,212	<0.01%
Small	£2m - £4.9m	£3,465	0.11%
Small	£2m - £4.9m	£1,872	0.09%
Small	£2m - £4.9m	£878	0.06%

Source: Manufacturer Survey Q61 & 62 (n=7)

Costs to manufacturers of compliance labelling

One option for proposed legislation is to mandate an IoT security label that indicates whether the products adhere to the three consumer IoT security requirements. The survey asked about the costs to manufacturers of compliance labelling, including how long it would take to implement this label.

Figure 16: Estimated time taken to implement a mandatory security label



Source: Manufacturers' Survey Q65 (n=11)

Just over a third (36%) of these respondents felt it would take up to three months to implement a label. One was not sure how long it would take to implement the label but reported it might take up to two years for products to 'wash-through' the retail process. One was unable to say without knowing the extent to which packaging may need to be redesigned to include this label.

Respondents were asked about the annual staff time required to implement mandatory labelling and four provided this information.

Respondents were asked to estimate the number of person-days undertaken by each job role who may be involved in implementing a mandatory label on the banding in the header row. To calculate the average number of person days, we have used the mid-point number of hours in each band multiplied by the number of responses, and divided by the total number of respondents (four), divided by eight to show the results in person days. The average estimate for the number of person days spent to implement mandatory labelling was 20.7 person days.

Table 60: Staff costs of affixing a physical label

	Average Number of Person Days	Total estimated costs	Respondents who say this job role would be involved
IT or technical director or equivalent	8.9	£3,784	2
IT specialist manager	0.1	£26	1
IT professional or technical role	0.5	£93	1
Non-IT professional role (eg legal, accounting)	1.0	£236	2
Administrative	0.5	£60	1
Sales and marketing professional	4.8	£796	2
Other (please specify)	4.8	£596	2
Total respondents	20.7	£5,590	4

Manufacturer Survey Q67 (n=4)

Three respondents provided an estimate of the staff cost in the free text box. There are some large cost estimates of £500,000, £60,000 and “£25,000 to £50,000”. Including these estimates (which were a valid way of responding to the survey if it were considered difficult to break down the staff time required), **the total average cost for each manufacturer is £100,630** (or a median of £18,434). The impact by company size is shown in Table 61 below; please note that the respondents to this question are among the largest in the sample, and that although the cost in cash terms is the highest among all the components of the proposed options that we tested, it is still relatively low as a share of company’s IoT related turnover.

Table 61: Summary of responses

Size (Employees)	Size (IoT Turnover)	Estimated staff costs	as % turnover
Medium	£10m - £25m	£60,000	0.28%
Large	Over £25m	£3,909	<0.01%
Medium	Over £25m	£4,369	<0.01%
Small	£2m - £4.9m	£3,000	0.09%
Small	£2m - £4.9m	£32,500	1.63%
Medium	Over £25m	£500,000	0.79%

Source: Manufacturer Survey Q66 & 67 (n=6)

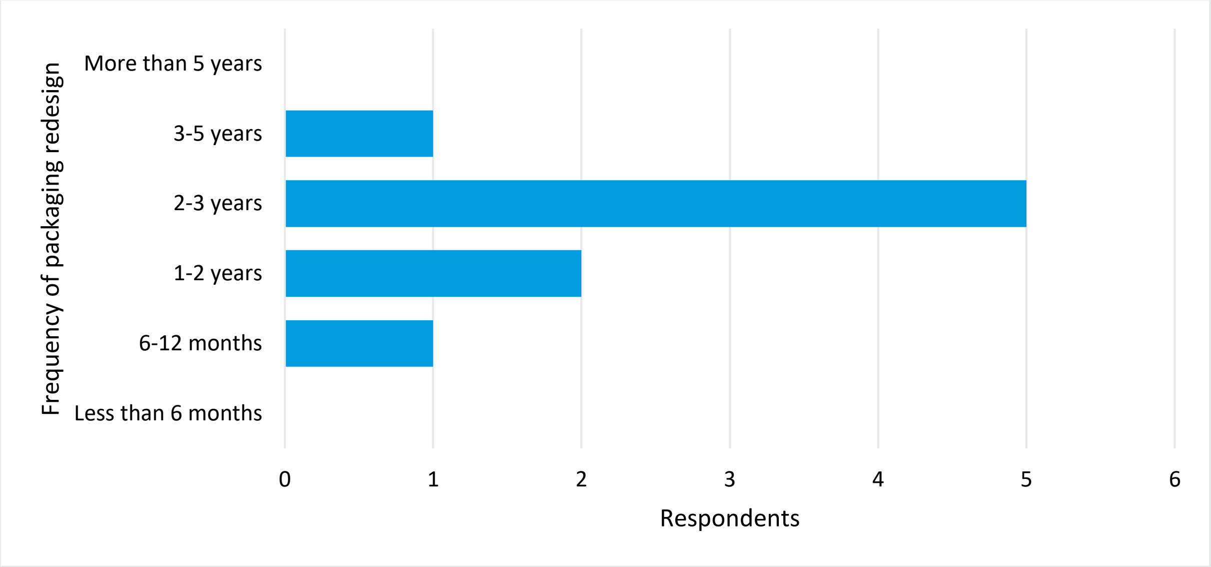
Most of these responses were not supportive of mandatory compliance labelling on physical packaging and one said it would be prohibitive and not feasible. One respondent estimated the cost at around 10p per label per unit. Three respondents were unsure and unable to provide an estimate of the cost of implementing mandatory compliance labelling. Three others reported concerns about standardisation of packaging across Europe, such as: ‘This is a challenge for us as for environmental reasons we standardise across Europe. Segregating UK/EU would be a big challenge and have significant costs.’

Two others felt this was a more relevant concern for the retail side. One stated that they work with other organisations who providing the packaging and selling the good on, while one respondent questioned whether consumers actually get to see the physical packaging when they buy devices in store or online.

The survey also asked how much of this cost would be passed on to consumers and six respondents answered. Of these, three said all of the cost of mandatory compliance labelling would be passed on to the consumer, and two said they would not pass on any of the cost. The final respondent said they would pass on between 1% and 10% of the cost.

Manufacturers were asked how frequently packaging for their products was re-designed and seven respondents answered this question and reported that on average packaging for the devices they produce was redesigned every 30.3 months. The average is calculated based on multiplying the midpoint of the bands by the number of responses and dividing by the total number of respondents.

Figure 17: How often is packaging redesigned?



Source: Manufacturers' Survey Q71 (n=9)

If packaging is redesigned every 30.3 months on average - around 2.5 years - then with sufficient lead-in time, the labelling requirement could be built in to regular packaging redesign, thus reducing the cost. No respondents said that redesign was less frequent than 3-5 years, and only one said that it happened as infrequently as every 3-5 years; if this is true of the market, then a 3 year lead-in time would remove most of the need for companies to redesign packaging specifically for the labelling requirement.

Respondents were generally reluctant to affix a physical label, and estimate the costs of this to be quite high.

Familiarisation costs for manufacturers

Respondents were asked to estimate the number of person-days undertaken by each job role who may be involved in the familiarisation process to understand any new regulation on compliance with aspects of the top three CoP guidelines. To calculate the average number of person days, we have used the mid-point number of hours in each band multiplied by the number of responses, and divided by the total number of respondents (four), divided by eight to show the results in person days.

Five manufacturers said it would be a responsibility of an IT or technical director and four said it would be the responsibility of someone in a professional IT or technical role. The overall average estimate of how long it would take is 15.2 person days.

Table 62: Staff costs of familiarisation for compliance with aspects of the top three CoP guidelines

	Average Number of Person Days	Total estimated costs	Respondents who say this job role would be involved
IT or technical director or equivalent	1.9	£813	5
IT specialist manager	1.5	£302	3
IT professional or technical role	7.3	£1,317	4
Non-IT professional role (eg legal, accounting)	1.0	£219	3
Administrative	1.3	£153	4
Sales and marketing professional	1.6	£268	5
Other (please specify)	0.7	£82	2
Total respondents	15.2	£3,154	7

Source: Manufacturer Survey Q59 (n=7)

Respondents were also asked about this in a free text format. One said they thought it would take around three months to ensure the entire business was aware of the legislation. Two said they would anticipate very low costs – one thought it would take the chief product officer a few hours to read some documents and have some discussions. The other said that the actions are 'well-scoped and digestible' so thought it would be "quite quick". Responses are summarised below: **the overall average was £2,465**.

Table 63: Summary of responses

Size (Employees)	Size (Turnover)	Estimated costs	As % of turnover
Small	Unknown	£296	No data
Medium	£10m - £25m	£823	<0.01%
Large	Over £25m	£2,124	<0.01%
Medium	Over £25m	£1,370	<0.01%
Large	Over £25m	£5,968	<0.01%
Small	£2m - £4.9m	£9,742	0.30%
Medium	£10m - £25m	£103	<0.01%
Small	£2m - £4.9m	£1,756	0.09%
Large	Over £25m	£0	0

Source: Manufacturer Survey Q58 & 59 (n=9)

They had similar views as to how long it would take to familiarise themselves with the labelling scheme.

Respondents were asked to estimate the number of person-days undertaken by each job role who may be involved in the familiarisation process for mandatory labelling on the banding in the header row. To calculate the average number of person days, we have used the mid-point number of hours in each band multiplied by the number of responses, and divided by the total number of respondents (four), divided by eight to show the results in person days.

For familiarisation for the mandatory labelling scheme respondents felt it would mostly be the responsibility of professional roles in IT and other areas such as legal or accounting. The overall average amount of time spent on this would be 11.8 person days, based on four responses.

Table 64: Familiarisation with security labelling

	Average Number of Person Days	Total estimated costs	Respondents who say this job role would be involved
IT or technical director or equivalent	1.3	£545	3
IT specialist manager	1.5	£317	2
IT professional or technical role	4.0	£716	3
Non-IT professional role (eg legal, accounting)	1.0	£236	1
Administrative	2.9	£338	2
Sales and marketing professional	1.0	£171	1
Other (please specify)	0.0	£0	0
Total respondents	11.8	£2,324	4

Source: Manufacturer Survey Q73 (n=4)

One person provided additional information, anticipating that the familiarisation costs for labelling would be zero as they had maintained familiarity with the legislation throughout its development. **The total average estimate of familiarisation costs is just £1,585 per organisation.**

Table 65: Summary of cost estimates

Size (Employees)	Size (Turnover)	Estimated staff costs	as % turnover
Medium	£10m - £25m	£0	0%
Large	Over £25m	£3,913	<0.01%
Medium	Over £25m	£2,245	<0.01%
Small	£2m - £4.9m	£1,383	0.04%
Medium	£10m - £25m	£213	<0.01%
Small	£2m - £4.9m	£1,756	0.09%

Source: Manufacturer Survey Q72 & Q73 (n=6)

5. RETAILERS OF IOT DEVICES

Summary

This section of the research is based on a survey of 12 UK retailers which sell consumer IoT products. The retailers surveyed sold products from across the three product groups; almost half sold over 50 individual product lines. All had been trading for over 12 months, most were UK-based, as opposed to multinational, and almost all had turnovers from sales of consumer IoT goods under £1m. A little under half (45%) had an awareness of the Code of Practice for Consumer IoT Security. The retailers had a low level of understanding of whether there would be any cost to them in obtaining, requesting, or storing information from producers about the compliance of products with proposed regulatory options.

Costs to retailers of presenting compliance information at the point of sale: Retailers were asked to consider their familiarisation costs for understanding the Government's proposed legislation if the top three security requirements were mandated for consumer IoT products produced or sold in the UK. They typically responded that these would be low: up to one person-week across a range of roles, but most commonly managers or directors. Two-thirds of respondents felt that they would not need to use external advice or consultancy as part of the familiarisation process.

Retailers believed that the cost of a **labelling scheme** to them would be minimal, amounting to up to a person-day for each of a range of occupations including manager, legal/contract professionals, sales advisors, customer service, and admin. Only one respondent believed that external advice or consultancy would be necessary.

Retailers suggested a wide range of methods for presenting product security information, including online, in technical specifications, in-store labels, brochures, and price tickets, with a range of costs.

Profile of survey respondents

In total, 1,886 retailers were directly invited to take part in this survey. In addition, two retailer umbrella bodies were contacted and asked to share the survey with their members, and we also publicised the survey through our social media channels. The survey received 12 valid responses, five of which were fully complete and seven partially complete. This is likely due to COVID-19 and many businesses focusing on their response to the situation, as well as several retail stores closing operation. Due to the low response rate, these results are indicative and should be interpreted with caution. The full questionnaire can be found in chapter 10 of the accompanying technical report.

The survey asked respondents which of the below categories best described their organisation, and the number of people employed in their organisation in the UK, through which we determined whether they were a small, medium or large business. The table below shows the type and size of the retailers that responded to the survey.

Table 66: Types of organisation by size

Employee size	Online retailer based in the UK	Online retailer based outside the UK	High street store	High street store with online presence	Respondents
Small (1-49)	2	0	2	3	7
Medium (50-249)	0	0	0	0	0
Large (250+)	0	0	0	5	5
Total	2	0	2	8	12

Source: Retailers' Survey Q5 and Q9, March 2020 (n= 12)

All but two retailers[93] (83%) said that they use their own website to sell these products. Four retailers indicated that they use third party online marketplaces and platforms, with two of these using both their own website and third party marketplaces.

Respondents were asked whether they sell new and/or second-hand IoT products, and whether they undertake tests on their second-hand products.

Table 67: New and second-hand sales

	Respondents	Undertake checks on second-hand products
Exclusively new IoT products	7	0
Mostly new, some second-hand IoT products	4	3
Mostly second-hand products IoT products	1	0
Total	12	3

Source: Retailers' Survey Q7, March 2020 (n= 12)

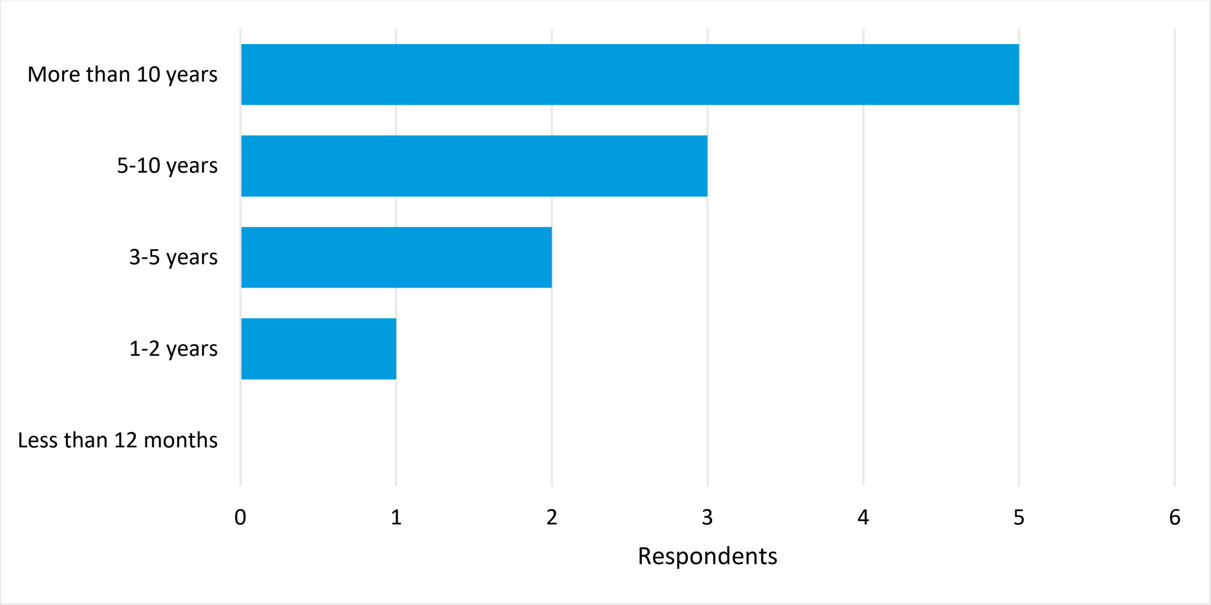
Only one organisation mostly sold second-hand IoT products, with most exclusively selling new IoT products and some selling mostly new and some second-hand products.

Of the four organisations who sell mostly new and some second-hand IoT products, three indicated that they undertook checks on the security of second-hand products, while the one organisation that mostly sells second-hand IoT products reported that they did not undertake these checks.

The survey asked how long organisations had been selling consumer IoT devices in the UK and all had been selling these devices for at least one year:

[93] n=12

Figure 18: Length of time selling consumer IoT devices in the UK



Source: Retailers' Survey Q14, March 2020 (n= 11)

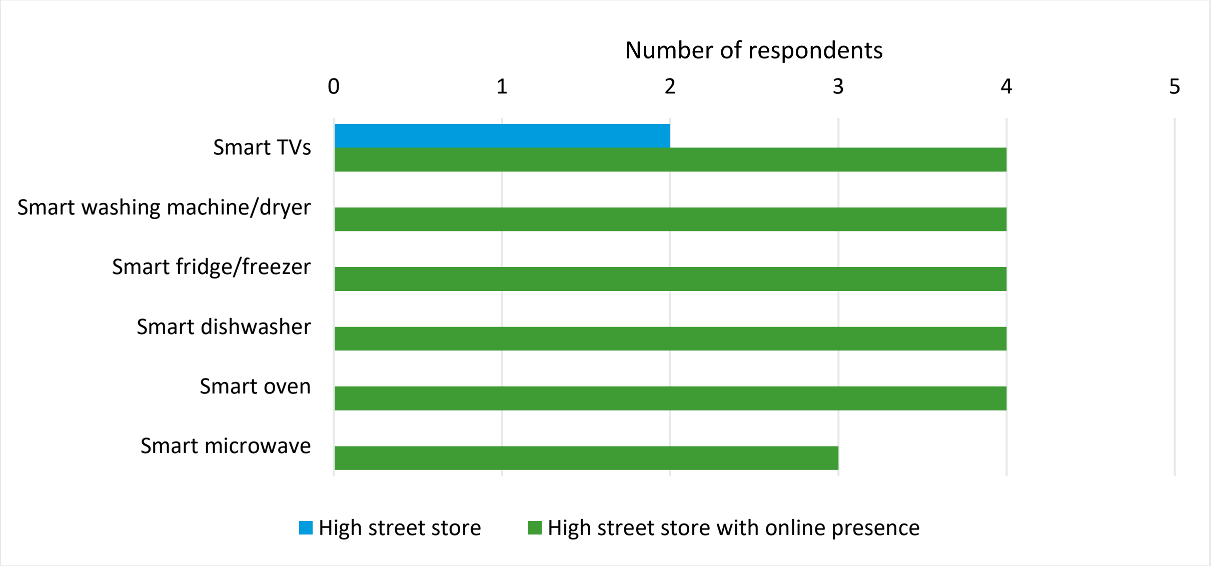
73% of respondents had been selling IoT devices for at least five years and five organisations had been selling them for more than ten years.

Devices sold

We asked respondents about the consumer IoT products that they sell within the three product groups used in this research. The three figures below show the devices that retailers sell within these groups and what type of organisation that retailer is.

There was a wide range in the consumer IoT products that respondents sell in the UK.

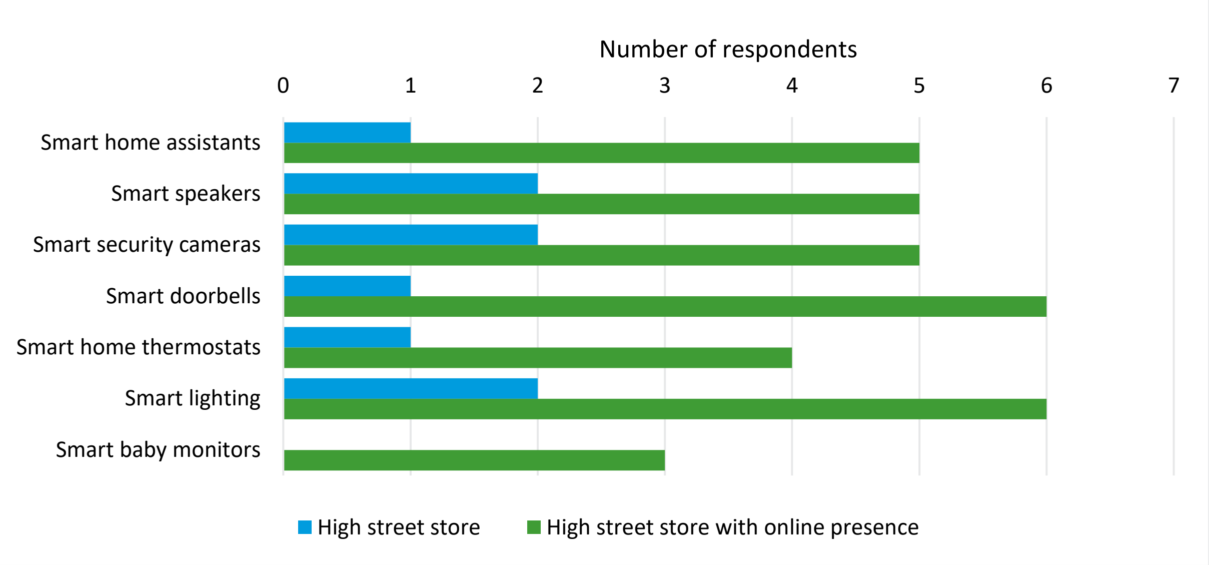
Figure 19: Type of organisation and device sold – Big ticket items



Source: Retailers' Survey Q10, March 2020 (n= 11)

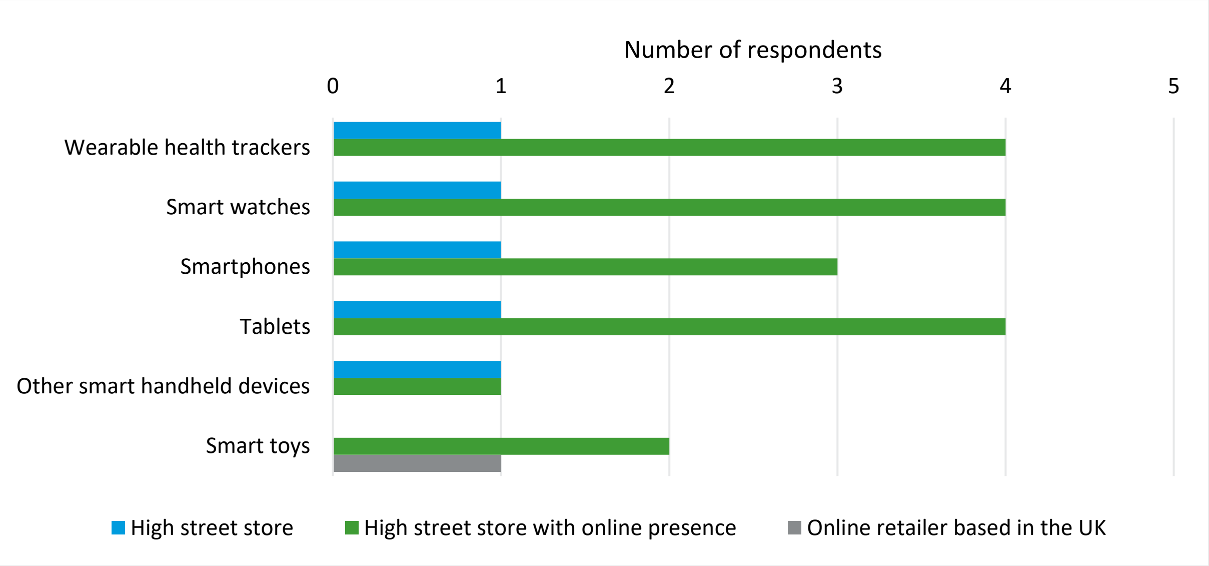
The retailers that answered this question (Q10) were mostly high street stores with an online presence, but did include two high street only stores.

Figure 20: Type of organisation and device sold – Smart connecting the home devices



Source: Retailers' Survey Q11, March 2020 (n= 11)

Figure 21: Type of organisation and device sold – Smart consumer lifestyle devices

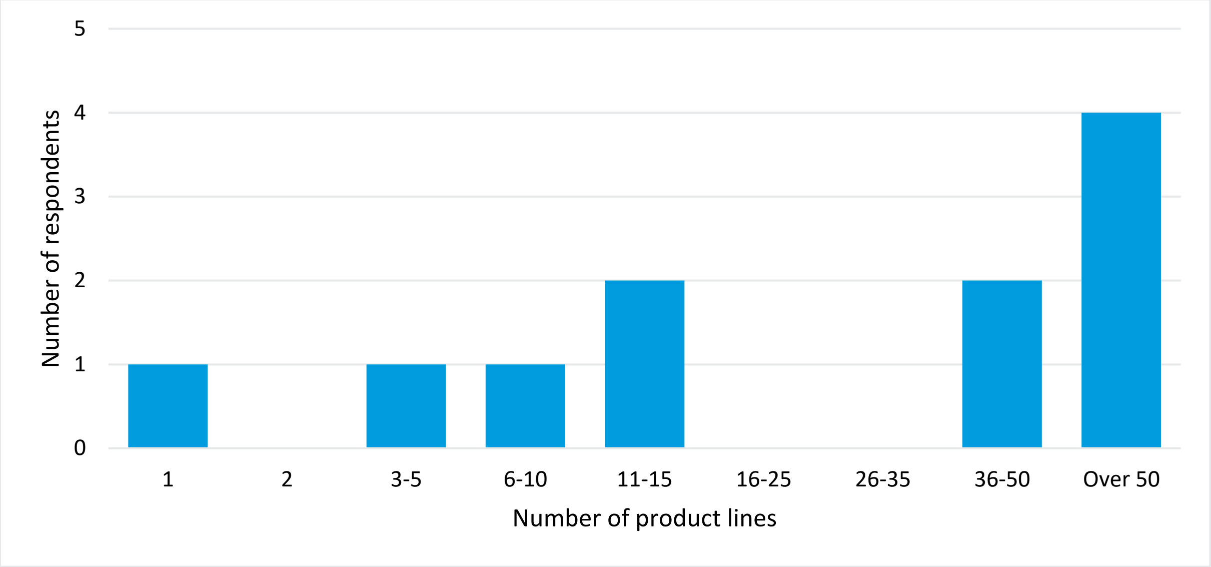


Source: Retailers' Survey Q12, March 2020 (n= 11)

More than half of respondents reported that they sell smart speakers, smart security cameras, smart doorbells and smart lighting. Several also sold smart TVs, smart home assistants, smart home thermostats, wearable health trackers, smart watches and tablets. A few organisations sold products that did not fit into our categories, such as sim-connected smart devices, eg pet trackers, SOS/fall detection wearables, luggage trackers, tracking kids watches, and smart food thermometers. The online retailers did not report selling any big ticket items or connecting the home devices (they sold smart toys and smart food thermometers).

The survey asked respondents how many consumer IoT product lines they currently sell in the UK in total.

Figure 22: Number of consumer IoT product lines sold by retailers



Source: Retailers' Survey Q13, March 2020 (n= 11)

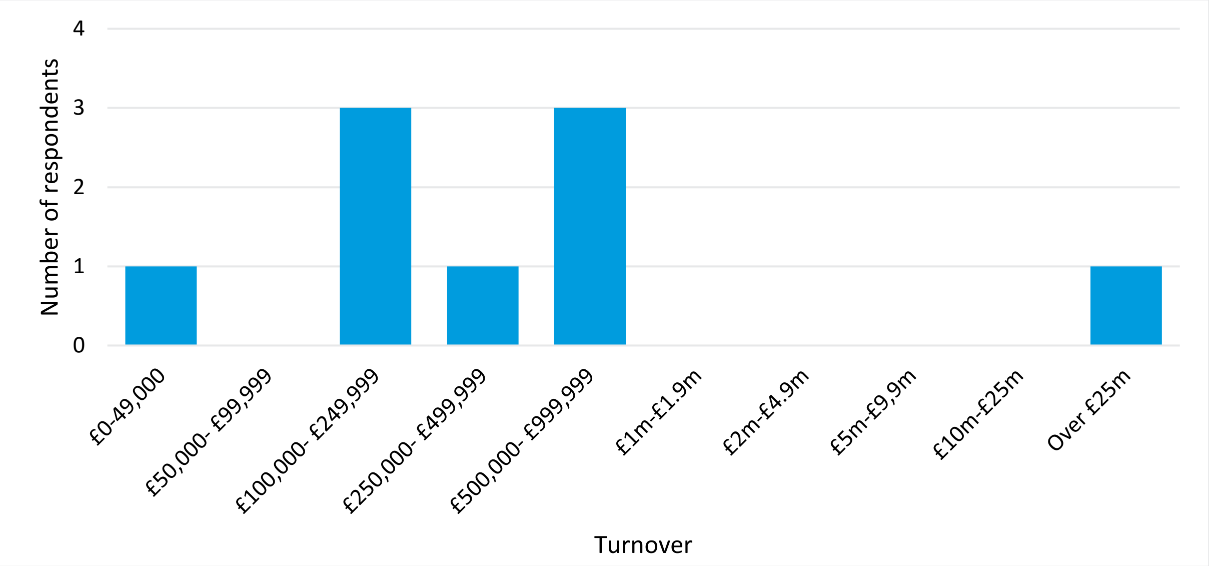
The information above can be used to estimate an approximate average number of product lines per retailer. Assuming that the "over 50" category represents an average of 100 products (based on written-in responses from firms), the average number of product lines sold is 38 for small businesses, 76 for large businesses, and 56 overall.

As shown in the graph above, over half of respondents indicated that they sold more than 36 consumer IoT product lines in the UK. Three of these organisations sold over 100 consumer IoT product lines, with one respondent saying that they stock new products every six weeks. On the other hand, just one organisation indicated that they only sold one consumer IoT product line, with the remaining organisations selling between three and 15 product lines.

The median number of product lines sold for all respondents was 43. This varies significantly for small businesses, which have a median number of product lines sold of 13. The median number of product lines for large businesses was over 50. There were no medium-sized retailers that took part in the survey.

The survey asked organisations what their approximate turnover had been from selling consumer IoT products in the last 12 months:

Figure 23: Turnover from sales of IoT products in the last 12 months



Source: Retailers' Survey Q15, March 2020 (n=10)

All but one organisation had a turnover from IoT of less than £1 million, with the other organisation reported having an IoT related turnover of over £25 million. Most respondents said their turnover was between £100,000 and £1 million, but there was also another outlier with a turnover of less than £50,000.

Retailer awareness of cyber security for consumer IoT

Awareness of the UK CoP

The survey asked respondents whether they had been aware of the UK Code of Practice for Consumer IoT Security before they were contacted for this research.

Table 68: Awareness of the UK CoP

	All Respondents
Yes, well aware	3
Yes, to some extent	2
Not aware	6
Total	11

Source: Retailers' Survey Q16, March 2020 (n=11)

The table above reflects that retailers are not particularly aware of the CoP guidelines, with over half (55%) of respondents for this question indicating that they were not at all aware of the guidelines prior to completing the survey. This is in contrast to consumer IoT manufacturers, where 82% of respondents said that they had been aware of the guidelines before completing our survey. It can therefore be seen that manufacturers have a better understanding of the CoP than retailers.

Costs to retailers of supplying security compliance information at point of sale

Costs of obtaining, requesting or storing compliance information

The survey asked retailers if there would be any cost to them in obtaining, requesting or storing any information or assurance from the producer to ensure that any products meet the security requirements.

Table 69: Costs of obtaining, requesting or storing compliance information

	Respondents
Yes	2
No	0
Don't know	6
Total	8

Source: Retailers' Survey Q22, March 2020 (n=8)

Only two respondents said that there would indeed be costs associated with obtaining, requesting or storing compliance information, while all other respondents said that they did not know if there would be costs associated with these activities.

Costs to supply chain of obtaining compliance information

Retailers were asked whether their supply chain would face any additional costs as a result of obtaining compliance information.

Table 70: Costs to supply chain of obtaining compliance information

	Respondents
Yes	1
No	0
Don't know	7
Total	8

Source: Retailers' Survey Q23, March 2020 (n=8)

Of the eight retailers who answered this question, only one said that there would be costs to their supply chain of obtaining compliance information, with all other respondents saying that they did not know whether there would be costs to their supply chain associated with this.

Familiarisation costs for retailers

The survey asked retailers to estimate the one-off familiarisation costs to their organisation, in terms of staff time, to read and understand proposed legislation, if the three security requirements were mandated for consumer IoT products produced, sold or supplied in the UK.

Nine retailers answered this question. All respondents said that there would be one-off familiarisation costs from administrative, sales advisor or customer services representative level to corporate manager and director level, involved in reading/ being trained in the guidance. However, the estimated costs to organisations to read and understand proposed legislation in corporate manager or director days did not exceed four or five days, whereas the costs in administrative, sales advisor and customer services representative days was estimated to be five to ten person-weeks for some organisations (presumably spread amongst a team of people in at least some cases).

Table 71: Estimated costs for retailers' familiarisation with top three CoP guidelines

	Average Number of Person Days	Total estimated costs	Respondents who say this job role would be involved
Corporate Manager, director or equivalent	1.8	£599	9
Manager	2.4	£473	8
Legal and contract professional	2.3	£533	7
Commercial and procurement roles	4.2	£825	7
Administrative	4.4	£509	7
Sales and marketing professional	4.4	£625	7
Customer services representative	4.5	£414	8
Other (please specify)	6.5	£803	3
Total respondents	30.4	£4,781	9

Source: Retailer Survey Q18 (n=9)

Table 72: Summary of costs

Size (Number of employees)	Size (Turnover)	Estimated cost	as % of turnover
Large	Over £25m	£26,856	<0.01%
Large	Over £25m	£6,285	<0.01%
Large	Over £25m	£1,808	<0.01%
Small	No data	£2,949	No data
Small	No data	£655	No data
Small	No data	£925	No data
Small	No data	£1,604	No data
Small	No data	£1,294	No data
Small	No data	£655	No data

Source: Retailers' Survey Q17 & Q18 (n=9)

The average estimated cost of familiarisation for retailers was £4,781.

Respondents were then asked whether they would pay for external advice or consultancy services as part of the familiarisation process of compliance with these security requirements.

Table 73: Use of external advice or consultancy as part of the familiarisation process for security requirements

	All Respondents
Yes	1
No	6
Don't know	2
Total	9

Source: Retailers' Survey Q19, March 2020 (n=9)

Six of the nine retailers who answered this question said they would not pay for these services, with only one organisation saying that they would pay and two others saying that they do not know.

Costs to retailers of compliance labelling

Retailers were asked what the one-off familiarisation costs might be to their organisation, in terms of staff time, to read and understand proposed legislation if an IoT security label that indicates whether products adhere to the three consumer IoT security requirements was mandated.

Five retailers answered this question. All but one said that there would be costs in person days from administrative, sales advisor or customer services representative level, through to corporate manager and director level. However, in this case, the maximum estimated costs to organisations to read and understand proposed legislation would be one to two person weeks, and that would be for managers or those in commercial and procurement roles, while for administrative, sales advisor and customer services representative roles there would only be a maximum cost of two to three person days.

Table 74: Cost of familiarisation in person-days

	Average Number of Person Days	Total estimated costs	Respondents who say this job role would be involved
Corporate Manager, director or equivalent	1.5	£520	5
Manager	1.9	£376	5
Legal and contract professional	0.3	£69	3
Commercial and procurement roles	2.5	£498	4
Administrative	0.3	£35	3
Sales and marketing professional	0.6	£87	3
Customer services representative	0.7	£66	4
Other (please specify)	0.2	£25	2
Total respondents	8.1	£1,676	5

Source: Retailers' Survey Q25, March 2020 (n=5)

Retailers were asked whether they would pay for external advice or consultancy services as part of the familiarisation process of the labelling scheme and none of the five respondents to this question said they would.

Table 75: Summary of costs

Size (number of employees)	Size (Turnover)	Estimated costs	As % of turnover
Large	Over £25m	£3,669	<0.01%
Large	Over £25m	£655	<0.01%
Small	Unknown	£3,023	No data
Small	Unknown	£717	No data
Small	Unknown	£314	No data

Source: Retailers' survey, March 2020 (n=5)

The survey asked retailers how they would present consumer IoT product security information to meet the requirement to explicitly state at the point of sale the minimum length of time for which the consumer IoT product will receive security updates, if individual product labelling was not mandatory.

Table 76: Methods for presenting minimum security update support period at point of sale

Presenting minimum update period	All Respondents
Provide information in product listing online	2
Provide information in product description online	3
Provide information in product technical specification online	3
Provide information in product description in store	2
Provide information in product technical specification in store	3
Provide information in in-store brochure	1
Provide information in-store on pricing/display ticket	1
Adding a voluntary label to the product itself	3
Other (please specify)	2

Source: Retailers' Survey Q29, March 2020 (n= 6)

Of the six organisations that responded to this question, each said they would use a combination of methods, with half saying that they would either provide information in the product description online, provide information in the product technical specification online, provide information in the product technical specification in store, or add a voluntary label to the product itself.

6. MANUFACTURER VULNERABILITY DISCLOSURE POLICY IMPACT ON SECURITY RESEARCH

This chapter considers whether a manufacturer publishing a point of contact as part of a vulnerability disclosure policy would impact on the ability of security researchers and cyber security professionals to effectively report vulnerabilities to a company. For robustness, it needs to consider the current baseline situation as well as any likely changes due to Government policy. Therefore, the three key questions for this section are:

- Whether security researchers would normally report vulnerabilities to a company;
- Whether the affected companies would usually take subsequent action as a result of the reported vulnerability (and what kind); and
- What would be the impact of the proposed regulations on researcher and company behaviour.

There is very little information available with a specific focus on IoT, so evidence is taken from the general vulnerability disclosure market. Questions on the current behaviour of security researchers were also included in the survey of manufacturers.

Vulnerability disclosure policies provide a safe route for 'white hat' or ethical hackers to report vulnerabilities to companies. Researchers have stated that the implementation of a vulnerability disclosure policy is a good compromise between heavy-handed regulation and private measures to promote security research and allow companies time before publication of vulnerabilities to address them.[94]

Summary

Current researcher behaviour in reporting vulnerabilities: Recent survey evidence[95] suggests that researchers are proactive about reporting vulnerabilities; some companies offer 'bug bounties' to encourage this but researchers report that companies are becoming more open to receiving vulnerability information and working with them. If companies release their vulnerability disclosure policies, security researchers will use them to report bugs and companies will take action in response to reports. Much of the information currently available in the literature is based on reporting vulnerabilities in computer software. IoT devices are complex due to them being less secure, less powerful, and more likely to be remotely deployed.

Manufacturer behaviour in accepting and handling vulnerability reports: The majority (71%) of companies in our survey sample have some form of public route for vulnerabilities to be disclosed, even if this is not through a dedicated portal, but this is not frequently used by security researchers and virtually never by members of the public. The companies surveyed had a range of timeframes for dealing with vulnerabilities ranging from under 14 days to over 90, although this depends upon the comprehensiveness of the response and the nature of the vulnerability. It is worth noting that secondary research generally suggests a lower availability of public routes to report vulnerabilities, perhaps indicating that those responding to our manufacturer survey are more aware of security issues for consumer IoT.

Impact of proposed regulatory options: The companies in our survey therefore do not anticipate that introducing legislation on vulnerability disclosure policies will lead to a great

[94] IoT Security for Policymakers (2018) Internet Society 2017 Global Internet Report
[95] HackerOne (2018) 'The 2019 Hacker Report'

increase in their use. The typical length of time to respond to vulnerabilities varies greatly between companies, but also from report to report depending upon the nature of the vulnerability.

Regardless of any policy interventions, as the number of items of this type continues to increase, and reported vulnerabilities are seen to be addressed properly, vulnerability disclosures are likely to increase, and the challenge then becomes whether companies can keep up.

Behaviour of manufacturers

The main element of a vulnerability disclosure policy is the agreement that the finder will not publish details of the vulnerability before some time is allowed for it to be addressed, and the threat of disclosure encourages the manufacturer to take action to fix the vulnerability. [96] In practice there is often a time limit (around 45 to 60 days) before the vulnerability is publicised, regardless of whether it is fixed.[97]

An alternative approach is to offer a 'bug bounty' where researchers are paid for finding bugs but there is no onus on the company to fix them and some may also include a non-disclosure agreement to not make the bug public. VDPs are considered best practice but the risk of disclosure means it is sometimes hard to achieve buy in to implement these policies.[98] The IoT Security Foundation recommends that contact details for a nominated responsible person are easy to find so that any individual who discovers security vulnerabilities (whether a security researcher or a member of the public) can seamlessly make contact.[99]

There are many issues with the vulnerability disclosure process.[100] These include problems with 'safe harbour' frameworks that shield researchers from legal action if a manufacturer threatens legal action on the grounds of compromising its technology.

For IoT specifically, there is a lack of standards, as each IoT vendor has its own set of rules and processes for how to deal with disclosure, and staff roles or teams that are responsible.[101] Our consultation with stakeholders included an interesting example of this. White goods IoT manufacturers see vulnerabilities as a device safety issue and would expect vulnerabilities to be reported to the same point of contact as other safety issues (eg. fire hazards). Other manufacturers reported that they had used the same team responsible for their GDPR response for their vulnerability reporting. While putting cyber security on a similar level to other product safety issues is well-intentioned, it is not clear if cyber security researchers would typically take the step of contacting a product safety team or GDPR team. There was also some discussion about whether retailers or manufacturers were the point of contact in these cases.

IoT wrestles with supply chain issues more than other areas of technology. The weakest security link in a system can be a tiny component, and penetration testing on these systems can involve multiple vendors across multiple legal jurisdictions. Protection is needed for researchers, but device manufacturers also need rules around auto-update features, timelines on fixing bugs and disclosure and third-party oversight.[102]

A 2020 IoTSF survey aimed to discover whether companies making consumer IoT devices have dedicated channels for vulnerability disclosure and reviewed disclosure practices of 331

[96] IoT Security for Policymakers (2018) Internet Society 2017 Global Internet Report
[97] Peeters G (2017) 'Strengthening the digital Achilles heel of the European Union: Make use of ethical hackers to find vulnerabilities in information systems?'
[98] Porup, JM (2020) 'Bug bounty platforms buy researcher silence, violate labor laws, critics say'
[99] IOTSF (2018) 'Understanding the Contemporary Use of Vulnerability Disclosure in Consumer Internet of Things Product Companies'
[100] Spring T (2018) 'The Vulnerability Disclosure Process: Still Broken' Threatpost
[101] Spring T (2018) 'The Vulnerability Disclosure Process: Still Broken' Threatpost
[102] Spring T (2018) 'The Vulnerability Disclosure Process: Still Broken' Threatpost

companies across the world to assess whether they possessed a public disclosure policy.[103] Some key findings were:

- As of March 2020 only 13% (of that sample) had a vulnerability disclosure policy;
- Of those companies with a vulnerability disclosure policy, 46% gave no indication of the expected disclosure timeline;
- Of those companies with a vulnerability disclosure policy, 41% also had a bug bounty programme;
- Of the companies reviewed, those based in Europe had the lowest vulnerability disclosure policy percentage (6%) as compared to the US (16%) and Asia (16%).

Overall, very few companies actually have a vulnerability disclosure policy in the market. The report notes that 93% of the Forbes Global 2000 do not have a known vulnerability disclosure policy, compared to 94% of the 2016 list. This is a surprisingly slow uptake especially given there are published standards[104] and templates provided online.[105] The Forbes Global 2000 is a list of the largest publicly owned companies and includes a range of organisations in different sectors and concerns around vulnerability disclosure may be more relevant in some than others. This may mean adoption will be slow for the IoT as well, unless government or industry bodies intervene in some way.

Most of the information about vulnerability disclosure policies focuses on the computer software market, but the IoT is likely to require a more streamlined approach and one that accounts for the cyber-physical nature of IoT. IoT devices are ubiquitous, small, connected and likely to become more prevalent in the future, so processes about disclosure timing, co-ordination, scanning, and patching that apply to traditional computer software may be less appropriate for IoT devices. This is partly because of their nature and their varied user interfaces - updating a smart light bulb presents a different challenge to updating a laptop - and also their sheer volume as the market grows presents problems of scale. To quote one report: ‘As vulnerability discovery tools and techniques evolve into this space, so must our tools and processes for coordination and disclosure’.[106]

Organisations are motivated to participate in vulnerability disclosure for the security and economic benefits; to raise awareness and engage with the community; in response to customer demand; and for ethical or social responsibility reasons. Companies also adopt vulnerability disclosure policies in response to legislation and peer pressure.[107]

Barriers for organisational participation include a lack of awareness or understanding; costs of implementing and operating vulnerability disclosure; a lack of management support; a lack of organisational or technical capacity; and legal barriers or uncertainty.[108]

Behaviour of security researchers

Currently, ‘bug bounties’ encourage competition between security researchers to find vulnerabilities, and participating companies pay rewards to researchers for finding them. They do

[103] IOTSF (2020) ‘Consumer IoT: Understanding the Contemporary Use of Vulnerability Disclosure 2020 Progress Report’

[104] ISO (2018) ‘ISO/IEC 29147:2018: Information technology - Security techniques - Vulnerability disclosure’

[105] https://cyber.dhs.gov/bod/20-01/vdp-template/

[106] Householder AD, Wassermann G, Manion A & King C (2017) ‘The CERT Guide to Coordinated Vulnerability Disclosure’ SPECIAL REPORT CMU/SEI-2017-SR-022

[107] Bugcrowd (2019) ‘Why every company should have a vulnerability disclosure program’

[108] Silfversten E, Phillips W, Paoli GP & Ciobanu C (2018) ‘Economics of Vulnerability Disclosure’ ENISA

help to ‘keep vulnerability disclosure relationships on an even keel’[109], but only the first person to find a bug gets the bounty money and it can lead to researchers being caught in a non-disclosure agreement and no incentive on the manufacturer side to fix the vulnerability.

HackerOne is a bug bounty facilitator firm who undertake an annual survey of security researchers. The most recent annual HackerOne Hacker report[110] includes a survey of 3,667 security researchers, and indicates that:

1. Just under 2% of hackers surveyed hack IoT devices;

2. Just over a third (36%) of hackers choose to work with companies based on how responsive they are to reports, and this was the third most important factor behind the challenge or opportunity to learn (60%) and liking the company (40%); and

3. Companies are becoming more open to receiving vulnerabilities than they were before. When hackers were asked about their experiences when reporting a vulnerability, a combined 69% noted that companies were becoming more open to receiving reports.

The ENISA report on the Economics of Vulnerability Disclosure[111] considers the incentives and barriers to the hacker as well as to the organisation. Incentives for white hat security researchers include profit; career advancement; for the challenge; and for ethical or ideological reasons. Barriers to researcher participation include fear of hostility or punishment; legal barriers or uncertainty; lack of appropriate avenues for disclosing vulnerabilities; and insufficient or slow communication with vendors or co-ordinators.

This last finding is supported by the NTIA Awareness and Adoption Group. A 2015 report[112] mentions that ‘When security researchers have gone a different route to responsible vulnerability disclosure (e.g. public disclosure) it has generally been because of frustrated expectations, mostly around communication [with the vendor].’ This may suggest that for the IoT, if such an official route is not present, researchers may publicly disclose vulnerabilities, especially if they have contacted the organisation and not received a satisfactory response.[113] Conversely, if more companies had a vulnerability disclosure policy, researcher frustration leading to public disclosure of vulnerabilities could be expected to fall, and if company vulnerability disclosure teams were sufficiently responsive then disclosures would be made through the official channels.

While companies are known to provide ‘bug bounties’ for evidence of vulnerabilities in their products, researchers may also choose not to contact companies to report vulnerabilities if there are more lucrative opportunities such as selling them away from official channels.[114] Trading in vulnerabilities unofficially, or even criminally, would be the aim of black hat researchers/hackers.

Findings from manufacturer survey

Manufacturers who participated in our survey were asked if they had a vulnerability disclosure policy. Of the 16 respondents who answered this question, 12 (75%) reported that they did have such a policy. These were mostly larger multinational companies, but did include two UK only based manufacturers, one small and one medium-sized. Three respondents (19%) said they did not have a policy in place and one did not know. They were also asked if they had a public point of contact for reporting vulnerabilities. Of the 15 that answered this question, 11 (73%) reported

[109] Spring T (2018) ‘The Vulnerability Disclosure Process: Still Broken’ Threatpost
[110] HackerOne (2018) ‘The 2019 Hacker Report’
[111] Silfversten E, Phillips W, Paoli GP & Ciobanu C (2018) ‘Economics of Vulnerability Disclosure’ ENISA
[112] NTIA Awareness and Adoption Group (2015) ‘Vulnerability Disclosure Attitudes and Actions’
[113] Gatlan S (2019) ‘Ethical Hacker Exposes Magyar Telekom Vulnerabilities, Faces 8 Years in Jail’ BleepingComputer.Com
[114] Thompson, I (2018) ‘So you’ve got a zero-day – do you sell to black, grey or white markets?’ https://www.theregister.co.uk/2018/04/15/mature_bug_bounty_market_bsidessf/

that they did have a public point of contact (this mostly included larger multi-national companies), three said they did not and one did not know.

Fifteen respondents also answered a question about the channel for reporting vulnerabilities and most (12) said vulnerabilities were reported through the public point of contact either always (five responses) or most of the time (seven responses). One response from a small company who make devices for connecting the home said they did not have a public point of contact, so reports came through the customer service ticketing process, which has a 24-hour response time. Another respondent (a small manufacturer of wearable health trackers) said they did not deal with IT security directly and that 'the end users and resellers of our products/modules in consumer products do, and they would be responsible.'

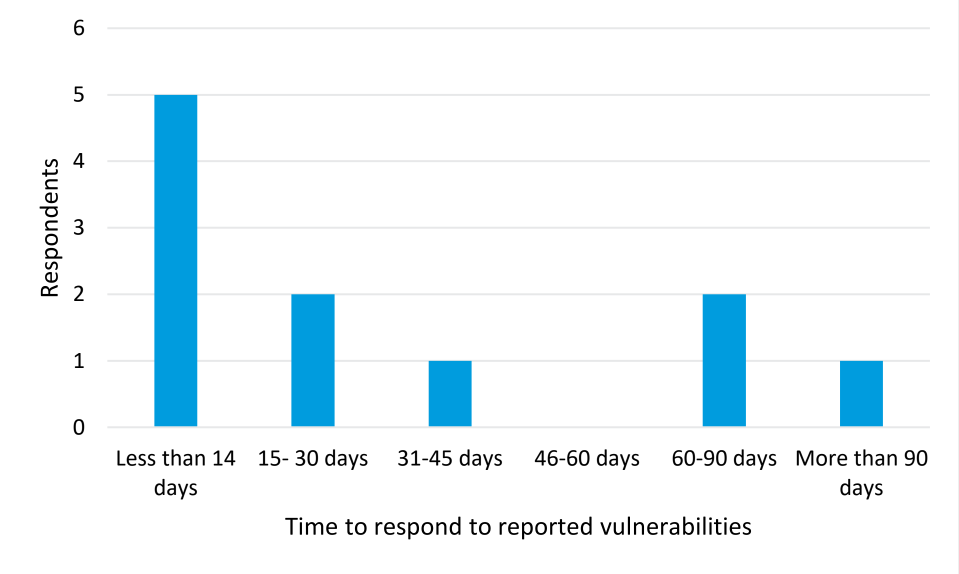
Whatever channels were available, actual reports of vulnerabilities were infrequent; 1-2 times per year for 50% of the respondents (of which there were 14 in total), and never for 21%. See Table 77 below.

Table 77: Frequency of reports of vulnerabilities

	Respondents	Percentage
Never	3	21%
1-2 times per year	6	43%
3-5 times per year	1	7%
6-10 times per year	2	14%
11-20 times per year	0	0%
More than 20 times	2	14%
Respondents	14	100%

Manufacturers' Survey Q47 (n=12)

Figure 24: Length of time to respond to reported vulnerabilities



Manufacturers' Survey Q56 (n=11)

Eight of the 11 respondents who answered this question said their response time for responding to reported vulnerabilities was less than 45 days; see Figure 24 above for the full breakdown of responses. The companies with the longer response times were larger companies and two produced a large number of product lines. The companies with the shortest response times were small to medium sized organisations with a smaller number of devices, mostly in the connecting the home product category. Those manufacturers who gave qualitative explanations for their answers typically said that while the majority of vulnerabilities were discovered through their own testing (internal or subcontracted), they would take vulnerability reports seriously as their credibility in the market would be damaged by reports of an unpatched vulnerability.

7. DISPOSAL OF NON-COMPLIANT STOCK

Summary

This section deals with the research objective to provide evidence on the following:

- Estimated costs associated with disposing of non-compliant stock after any sell-through period (i.e. grace period) has expired and any subsequent estimated impact on consumer IoT resale and waste/recycling (e.g. cost of carbon from waste disposal).

Evidence on current consumer disposal behaviour comes from our consumer survey:

- Currently, only 17% of consumers dispose of IoT products by throwing away; the remainder remain within the product lifecycle by being retained, passed onto someone else, given to charity, or resold. There was however some variation by type of device, with smart home thermostats (32%) and smart lighting devices (20%) most likely to be thrown away when replaced.
- On average, IoT devices *that have already been replaced to date* were replaced within a range of 24-42 months since the original purchase date; this evidence comes from a small sample of early adopters. Comparable non-smart white goods and electrical goods have lifetimes of 9-13 years; lifetimes of novel products such as smart speakers, toys and wearables are not yet known but may not be as durable.

Evidence on activities and costs borne by businesses comes from our surveys of manufacturers and retailers:

- Estimates of the cost of disposal of non-compliant stock ranged between 0.5% and 1.6% of turnover for three manufacturers who gave estimates. Two more said the cost would be "negligible".
- Strategies for disposal varied, with some manufacturers favouring re-shipping to other jurisdictions, trying to sell all stock within a grace period, disposing as refuse or destroying products.
- Retailers were not able to relate costs to their turnover without information on the grace period; unit costs for disposal ranged from £10-£50 per unit, or free of charge if this was provided for in their relationship with their supplier.
- The most common retailer strategies for disposal were returning to the manufacturer, disposing as refuse, or destruction.

Wider environmental costs (including changes in fuel usage and release of carbon dioxide) were sought in the literature, but an adequate evidence base could not be derived as the relevant information was not presented in the studies accessed. Some sources of benchmark data are provided in the main body of this chapter.

Overview

The introduction of regulatory changes is likely to present consumers, manufacturers and retailers with options for the disposal of non-compliant stock; these include recycling, reshipping to other countries to be sold, and destruction of the products. This section of the report aims to provide evidence on the costs associated with disposing of non-compliant stock after any sell-through period (or "grace period") between the announcement and full commencement of the regulations has expired, and any subsequent estimated impact on consumer IoT resale and waste/recycling. It uses evidence from the surveys of consumers, manufacturers, and retailers, and corroborative evidence (where available) from the literature review.

The research findings outlined below attempt to present evidence to support a Green Book compliant analysis of the costs of disposal. This includes consideration of both public (i.e. cost of recycling or destruction of non-compliant products) and private costs (i.e. costs to manufacturers, retailers and consumers) and the whole-life costs of implementing the regulatory changes. However, as outlined below, there is an absence of cost information in academic and market research. Therefore, the evidence was limited to that developed through the primary research conducted in this report. Given the low response rate to the manufacturer and retailer surveys, a robust evidence base could not be compiled for analysis of the cost of disposal of non-compliant stock.

Consumer Disposal Behaviours

As highlighted in the consumer survey findings outlined previously, under normal circumstances (i.e. without considering the impacts of any new legislation) only 17% of consumers disposed of their products by throwing them away. The remainder of products were either retained, passed onto someone else or to charity, or resold, therefore remaining within the product lifecycle. There was however some variation by type of device. In particular, 32% of smart home thermostats and 20% of smart lighting devices were thrown away when replaced; this may be a function of their small size and ease of disposal. Smart TVs were more likely than the average to be passed on to an acquaintance; smart domestic appliances and smart toys / baby monitors were the most likely to be sold on.

Table 35 in the chapter on consumer survey results outlined evidence on the average lifetimes of devices. Those devices that have already been replaced by consumers had been in use for 24 to 42 months, depending upon the category; however, this is based on a small sample of consumers who had already disposed of smart devices, and is likely to be biased towards “early adopters” that upgrade more rapidly than the population at large, many of whom have yet to buy their first smart device. Literature on smart goods (where available) and equivalent non-smart products suggests expected lifetimes of 9-13 years. This suggests that it is likely that non-compliant stock will remain in circulation for many years after the introduction of the regulations. However, it should be noted that based upon the disposal preferences of consumers, it is likely that non-compliant stock will be circulated within the total market stock for a longer period through the devices that are retained by consumers as spare devices[115], and possibly through retailers and charities selling non-compliant used devices.[116]

Hainault and Smith (2000)[117] studied activities to combat the circulation of non-compliant stock. They show that special drop-off events that take place at retail stores are the single most successful method for consumer disposal of unwanted products, when measured by the percentage of participants or by cost per participant.

[115] Spare devices can be both active and 'inactive' in the sense that they will never be utilised again.

[116] While specialist technology resale companies such as CEX may have stringent internal policies about re-selling stock that is non-compliant, high street charity shops and other generic high street second hand retailers may lack the awareness of the regulation and sell non-compliant stock.

[117] Hainault T, Smith DS. Minnesota’s multi-stakeholder approach to managing electronic products at end-of-life. In: *Proceedings of IEEE international symposium on electronics and the environment*; 2000. p. 310–7

Manufacturers and Retailers Disposal Behaviours

At the point where any new regulations come into effect that prohibit the sale of non-compliant consumer IoT devices, manufacturers and retailers may bear the costs of disposal of any stock that they hold that cannot be sold. The level of costs, and who bears them, will depend upon:

- the length of any "grace period" between the announcement of the regulations and their enforcement date, which will allow manufacturers to update their products and both manufacturers and retailers to focus on removing them from their supply chain (which may involve selling at a discount);
- where in the supply chain the products reside by the enforcement date;
- the nature of any contracts between retailers, wholesalers, and manufacturers, which may set out responsibilities for disposal and who bears the costs; and
- the method of disposal, which could include:
  - disposal of non-compliant products and packaging;
  - refurbishment of non-compliant products;
  - recycling; and
  - reshipping items back to their country of origin, or to another country for sale.

Both manufacturers and retailers were asked whether they would bear the costs associated with the disposal of non-compliant stock in two scenarios: if aspects of the top 3 guidelines of the Code of Practice for IoT Security were mandated in law, and if a security label were mandated. Thirteen manufacturers and five retailers answered this question.

Table 78: Businesses' views on whether they would or would not bear the costs associated with disposal of non-compliant stock

	Manufacturers		Retailers	
	Non-compliance with top 3	Non-compliance with mandatory label	Non-compliance with top 3	Non-compliance with mandatory label
Would bear the cost of disposal	7	6	2	2
Would not bear the cost of disposal	5	3	1	1
Don't know if would bear the cost of disposal	3	5	2	2
Respondents	15	14	5	5

Source: Manufacturers' Survey Q74 and Retailers' Survey Q32 March 2020

Table 78 suggests no common approach to the incidence of the costs associated with the disposal of non-compliant stock (ie. where in the value chain the costs would be borne). However, it is possible that the nature of the regulations themselves, when published, would influence the approaches that were subsequently adopted by businesses by the time of the date of enforcement.

In the survey, retailers and manufacturers were also asked whether or not they had specific policies in relation to the reuse of components of non-compliant stock (see Table 79).

Table 79: Number of respondents that stated if they had policies for reuse of components

	Manufacturers	Retailers
Yes	4	2
No	3	2
Don't know	5	0
Respondents	12	4

Source: Retailers' Survey Q35 & Manufacturer's Survey Q76, March 2020

The data provided in Table 79 above indicates that whilst some retailers and manufacturers will reuse components, there is likely to be a significant portion of stock that is disposed of following the introduction of regulatory changes.

Manufacturers

Manufacturers did not provide specific information on their individual policies for disposal. They were asked about the costs associated with different methods of stock disposal. Seven answered this question, and two reported they were not able to do so. They were asked to provide estimates of costs for:

- disposal of non-compliant products and packaging;
- refurbishment of non-compliant products;
- recycling; and
- reshipping items back to their country of origin or to another country.

Table 80: Summary of characteristics of companies and their estimated costs of disposal

Company (Size)	Turnover	Type of products	Estimated cost of disposal
Company 1 (Medium)	£10m - £25m	Fewer than 10 product lines, connecting the home category	Estimate of £0 for disposal of non-compliant products and packaging, unable to estimate for other options.
Company 2 (Large)	Over £25m	Fewer than 10 product lines, connecting the home category	Would plan to sell through any stock if it existed, anticipates a grace period of 12 months would be sufficient to do this.
Company 3 (Small)	£2m - £4.9m	Fewer than 10 product lines, connecting the home category	Estimate of £20,000 for disposal, refurbishment or recycling and £15,000 for re-shipping to another country (all lines)
Company 4 (Medium)	£10m - £25m	Fewer than 10 product lines, connecting the home category	Estimate of cost to dispose of packaging - for a small item eg a plug this would cost £2,000 to £5,000 but for high volume product would be 10 times more, possibly higher. Their packaging is B2B2C so is just a plain cardboard box with CE mark, other essential information.
Company 5 (Small)	£2m - £4.9m	More than 50 product lines, connecting the home category	Estimate of £25,000-£50,000 for disposal of non-compliant stock (all lines)
Company 6 (Unknown)	Unknown	More than 50 product lines across all product categories	Cost would depend on grace period as big ticket items can spend long time in the retail chain. Subsequent costs would be borne by factories (downtime associated with switching from EU to UK specifications)
Company 7 (Medium)	Over £25m	Between 36 and 50 product lines, big ticket items, consumer lifestyle categories	Anticipates all products will be compliant by the time regulation is enforced, so no additional costs are envisaged

Source: Manufacturers' Survey Q8, Q9, Q10, Q11, Q13 and Q75

The sources and values of costs varied throughout the sample. Company 2 and Company 6 explicitly mentioned the grace period in their response and this is clearly a factor for any company which holds stock in warehouses for a period of time. Company 2, which produces connecting the home devices, believed that selling through their non-compliant stock would be feasible given a 12 month grace period, and Company 7 said they anticipated being compliant before the regulations are introduced.

The costs also depend upon company size and the nature of products. Company 1, Company 3, Company 4 and Company 5 gave cost estimates for disposing of stock, ranging from £0 to £50,000. The smaller estimates are from companies who mostly make connecting the home devices and produce a smaller number of product lines. Company 5 has the largest estimate and has a larger number of product lines.

Company 3 was the only one to provide estimates of the costs of all the different options (disposal, refurbishment, recycling or re-shipping). They reported that re-shipping their devices to another jurisdiction would be the cheapest option and estimated the cost for this at £15,000, equivalent to around 0.5% of their annual IoT turnover. Company 4 had previously had to dispose of a small electrical product (smart plugs) due to a safety issue, and based their estimate of £2,000 to £5,000 disposal costs on this experience; they also said that for higher volume products, the costs might be more than ten times this amount.

Based on responses from three manufacturers, the estimated cost of disposal as a percentage of IoT turnover was between 0.5% and 1.6%. There were also two respondents who did not provide a cost estimate but said they thought the cost would be negligible, which does not necessarily contradict the estimations made by other companies, as their circumstances may be different (their contractual arrangements may dictate that others bear any costs).

The estimates in Table 81 below use data from the market study on unit costs to convert each company's IoT turnover into an estimate of units sold, and presents their estimated cost of disposal as a percentage of their IoT turnover. It does not include those who said the costs would be "negligible", but it is likely that these are represented in the wider market; in that case, the average cost to manufacturers would be lower than the 0.5-1.6% range represented here.

Table 81: Estimates of costs of disposal for manufacturers who stated non-zero cost

	Estimated IoT turnover	Average Unit cost of devices sold	Estimated units sold in the last year	Disposal cost as % of IoT turnover based on estimate
Company 3 (Small)	£3.2m	£351.92	9,093	0.5%
Company 4 (Medium)	£24.7m	£108.22	228,239	1.4%
Company 5 (Small)	£2m	£123.86	16,147	1.6%

Source: Manufacturer Survey Q13 and Q75 (n=3), March 2020

Retailers

Few retailers provided specific information on their stock disposal policies. One said their policy was not discarding or selling to third parties any products, so they would either return to the supplier in the UK or recycle at the supplier's cost using a Waste of Electrical and Electronic Equipment (WEEE) compliant recycler. The only other retailer to provide information about this question said they would work with third parties who could recycle any valuable components.

Retailers were asked about the costs of:

- disposal of non-compliant products and packaging;
- return items to UK manufacturers;
- return items to non-UK manufacturers;
- recycling; and
- re-shipping items back to their country of origin or to another country.

Table 82: Summary of disposal costs for retailers

	Size	Turnover	Products sold	Cost estimates
Company 1	Large	Over £25m	Over 50 product lines, all product categories	Estimates of £10 per unit for disposal, £30 per unit for return to UK manufacturer or recycling, £50 per unit to return to non-UK manufacturer/re-ship overseas.
Company 2	Large	Over £25m	Over 50 product lines, connecting the home and consumer lifestyle	Anticipate returning non-compliant stock to UK manufacturer would be at manufacturers cost. It would not be cost effective to ship back stock overseas, so they would write off cost price and WEEE recycle. Estimated cost of £600 per trailer to recycle stock.
Company 3	Large	Over £25m	36-50 product lines, all product categories	Depending on contract, they would want to return free of cost to UK/non-UK manufacturers. The cost incurred for the purchase would be the recycle cost as that product would be obsolete.
Company 4	Small	Unknown	3-5 product lines, consumer lifestyle	The cost of recycling would be the cost of the stock.

Source: Retailers Survey Q9, Q10, Q11, Q12, Q15, and Q34

The responses suggest retailers estimated the costs based on their experience in similar situations and therefore this cost might not necessarily be specific to IoT, or to issues around regulatory compliance. The costs for this are likely to depend on the size of the stock they have to dispose of and the contractual arrangements made with suppliers or contractors.

Four retailers answered this question, including three larger retailers. One who sells a range of smart devices in all three product categories estimated that it would cost around £30 per unit to return items to a UK-based manufacturer or recycle them. Simply disposing of the items in refuse or destroying them would cost an average of around £10 per unit (depending upon product size/type). Either returning items to a non-UK manufacturer or re-shipping items to a different jurisdiction would be the most expensive option for them, costing around £50 per unit. These estimates do not include any loss of revenue from not being able to sell the items; knowledge of the length of any grace period is fundamental to this calculation. This retailer is a large department store and was unable to provide estimates of how much of their turnover comes from the sale of smart devices.

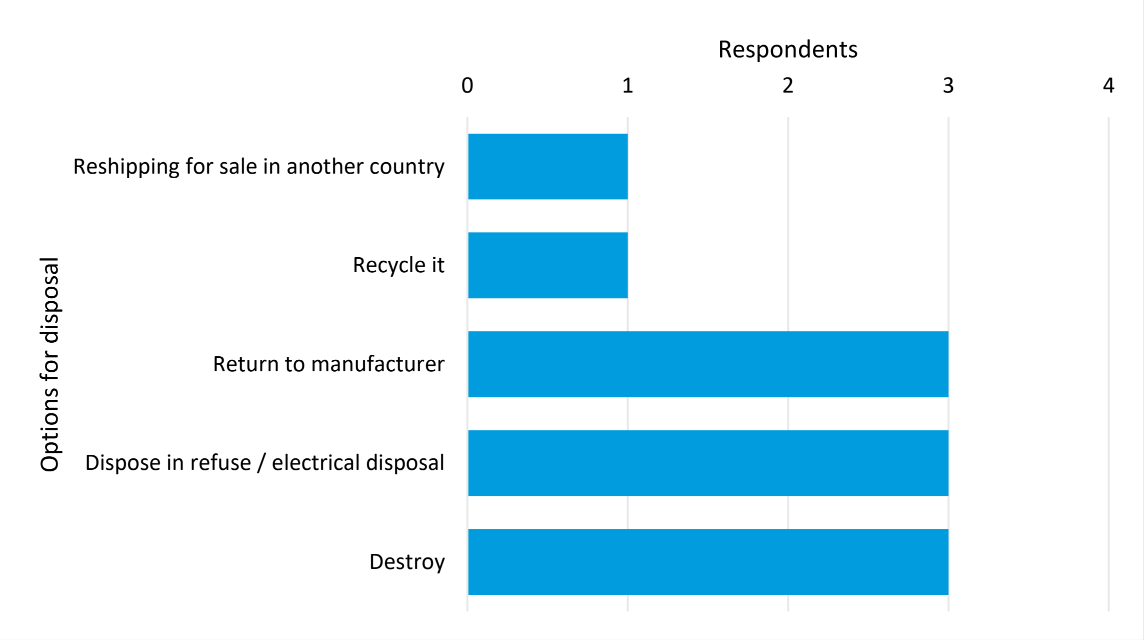
One of the other larger retailers who sells devices for connecting the home and consumer lifestyle devices reported that it would not be cost effective to re-ship items or return them to a non-UK based manufacturer, so they would look to recycle. This survey respondent estimated the cost of recycling any non-compliant stock at £600 per trailer-load, but the volume would depend upon the item and the length of the grace period. They also said that returning stock to UK-based manufacturers would be at supplier cost.

Another larger retailer who sells mostly connecting the home and consumer lifestyle devices said that it depended on the contract with the supplier, but they would look to return any non-compliant stock free of cost. They also said the cost incurred for the purchase would be the recycling cost, as the product would be obsolete. The small retailer that mostly sells smart toys and radio control models also shared this view.

One potential source of cost benchmarking information could be to review WEEE-compliant schemes for disposal of electrical waste. Companies that produce more than 5 tonnes of waste per year must sign up to such a scheme in order to recycle electrical waste.[118] These schemes provide costs per tonne; one example offering public information gave a benchmark price of £110 per tonne to recycle.[119] Although the details of these schemes may vary and be customised depending upon the nature and throughput of waste, this provides an additional route to give recycling cost estimates once the nature of any future legislation and length of any grace period have been confirmed.

Figure 25 highlights retailer strategies for disposal of non-compliant stock (respondents were able to select multiple options). This suggests that whilst a significant percentage of non-compliant stock is removed from circulation (i.e. destroyed or disposed of in refuse), retailers will employ a number of strategies for disposal.

Figure 25: Retailer methods for disposing of non-compliant stock



Source: Retailer survey Q33, March 2020 (n=5)

Summary of impacts on manufacturers and retailers

There were only a small number of survey responses from both manufacturer and retailers. Manufacturer estimates for the cost of disposal ranged from £0 to £50,000, depending on the size of the company and the number/type of products they would need to dispose of. It would also depend on the grace period as different product categories having different sell-through periods (larger items would likely have a longer sell through period). Only one manufacturer provided costs of each of the different options for disposal. They estimated that re-shipping products would be slightly cheaper than the other options (£15,000 compared to £20,000).

This is difficult to compare with retailer estimates of costs for disposing of non-compliant stock, as these have been provided on a per unit or per trailer basis. One company gave estimates of £10 and £50 per unit, with re-shipping items to non-UK manufacturers as being the most expensive option. Another large retailer estimated the cost of disposal at £600 per trailer.

[118] See https://www.gov.uk/guidance/electrical-and-electronic-equipment-eee-producer-responsibility
[119] See https://b2bweee-scheme.com/services/pricing

Impact of banning non-compliant stock

The supply chain mapping approach below, which reflects the guidance in the HM Treasury Green Book[120] on considering costs at all stages of the project lifecycle and at which stage in the value chain they are borne, and the supplementary guidance on environmental impacts[121], is summarised in the following table and figures. Table 83 overleaf summarises the likely areas of costs at each stage of the supply chain in relation to disposal of non-compliant stock; the relevant assumptions are set out below the table.

[120] https://www.gov.uk/government/publications/the-green-book-appraisal-and-evaluation-in-central-governent

[121] https://www.gov.uk/government/publications/green-book-supplementary-guidance-environment

Table 83: Likely areas of cost to dispose of non-compliant stock at each stage of the supply chain

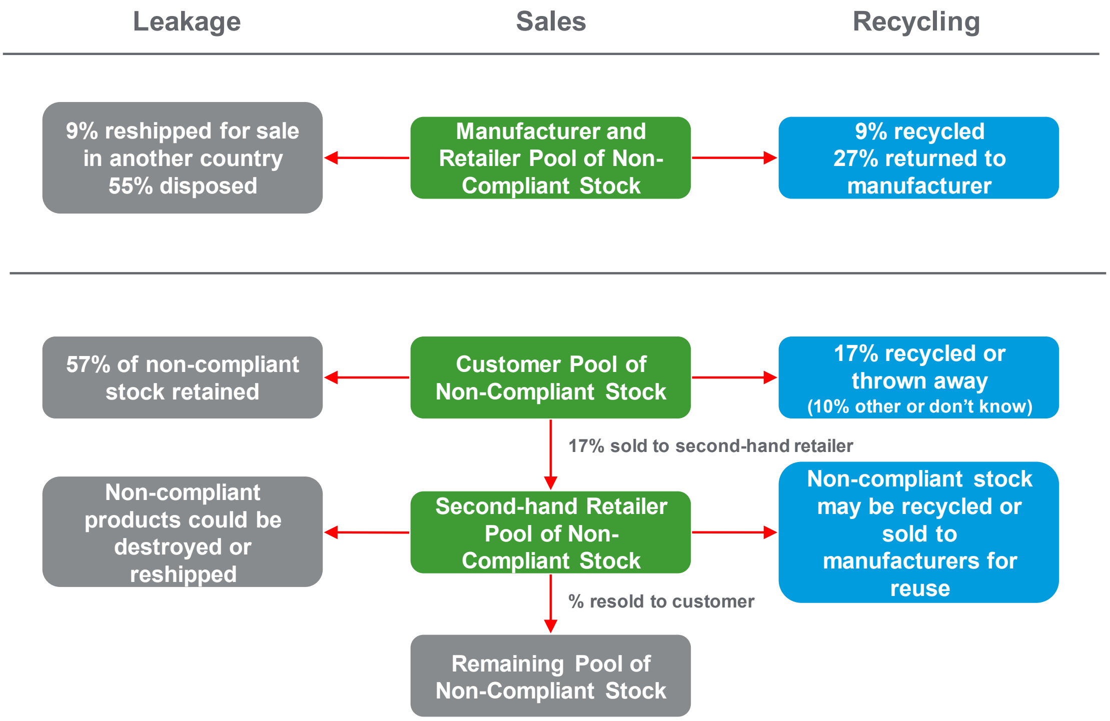
	Manufacturers	*Sells to*	Wholesaler	*Sells to*	Retailer	*Sells to*	Customer	*Sells to and buys from*	Second-hand retailers
Likelihood to retain non-compliant stock	**Low** - manufacturers will have adapted to new regulations and are unlikely to hold any non-compliant stock beyond the grace period.		**Low** - purchasing directly from manufacturers, the flow on non-compliant stock will decrease following implementation of regulations.		**Medium** - depending on sales, there may be some stock retained. This will be determined by the contract in place with manufacturers and potentially the retailers recycling partners.		**High** - depending on customer type, some customers will regularly upgrade to newer devices, while some will retain older devices for longer periods (which may have further consequences in terms of security, privacy, data integrity).		**High** - likely to hold a high level of non-compliant stock from older devices and from accepting new stock from customers disposing of non-compliant stock.
Likely Mitigation	Early implementation of regulations to avoid retaining non-compliant stock.		Discounted sales to retail outlets or recycling of products (through manufacturers).		Discounted sale prices to offload non-compliant stock or recycling of products (through manufacturers).		Recycling of products (through manufacturers) or re-sale to second-hand retailers or through private sales markets (e.g. eBay, Amazon etc.).		Recycling of products, labels added to non-compliant stock, awareness campaign in-store for consumers; training for staff to identify and reject non-compliant products.
Cost to dispose of non-compliant stock	Admin/ process costs associated with implementation of new policy/ regulation. Costs associated with recycling of non-compliant stock. Cost associated with loss of revenue due to lower price/sales.		Cost associated with loss of revenue due to non-sale or lower price. Cost of recycling.		Cost associated with loss of revenue due to non-sale or lower price Cost of recycling.		n/a		Cost to dispose or recycle non-compliant products. Lost income due to lower demand for non-compliant products being resold.

The table above is informed by the following assumptions:

- Recycling of non-compliant stock is managed / paid for by the manufacturer
- There is an administration cost associated with implementing new regulations for manufacturers
- Some small proportion of retailers would continue to sell non-compliant stock to customers (without any mitigation)
- Where this occurs, it is assumed that there is no cost associated with disposal
- Some customers would purchase new compliant devices due to the change in regulation, where otherwise they would not have purchased a new device
- The price of non-compliant stock (that is marked as such), products displaying a shorter minimum support period, or, under the labelling scheme, stock marked with a label stating non-compliance with top 3 security principles, decrease due to lower demand
- We only account for costs associated with one journey through the supply chain (i.e. when non-compliant stock has reached the customer, if they choose to replace and dispose of a non-compliant device, a cost is identified, if they choose not to dispose at that point and retain the device, no cost is assumed. If a non-compliant device is sold to a second-hand retailer, there are costs associated with disposal of that stock to the second-hand retailer, however, if another customer subsequently purchases a non-compliant device (that is clearly marked as such) then there are no costs associated with the customer's later disposal.

The figure below shows an example "product journey" for goods following regulation being implemented which makes them unsaleable. This has been informed by the behaviours evidenced in the consumer, manufacturer and retailer surveys.[122]

Figure 26: Product Journey following the introduction of regulatory changes


Leakage
Sales
Recycling
9% reshipped for sale in another country 55% disposed
Manufacturer and Retailer Pool of Non-Compliant Stock
9% recycled 27% returned to manufacturer
57% of non-compliant stock retained
Customer Pool of Non-Compliant Stock
17% recycled or thrown away (10% other or don't know)
17% sold to second-hand retailer
Non-compliant products could be destroyed or reshipped
Second-hand Retailer Pool of Non-Compliant Stock
Non-compliant stock may be recycled or sold to manufacturers for reuse
% resold to customer
Remaining Pool of Non-Compliant Stock

Note: "Leakage" here refers to products leaving the "value chain" of sales in compliance with UK regulations or recycling of materials, by leaving the UK or being destroyed / disposed of to waste.

[122] Please see Table 34 from the consumer survey, Table 81 (and discussion of open text responses) from the manufacturer survey and Figure 25 from the retailer survey.

Environmental Cost of Disposal

The rapidly evolving nature of IoT technologies (in terms of manufacturing processes, recycling processes, and the devices themselves), the sizes of devices and their material composition, make estimating carbon emissions difficult. However, there is evidence[123] that in terms of the environmental impact of microelectronics: recycling accounts for just 1% of whole lifecycle greenhouse gas emissions, with production being by far the biggest contributor (around 80%), followed by customer use (10-20%). Recycling can have important and direct consequences on the people actually involved in the recycling, and through reuse of the material recovered.

It has been estimated that over 80% of the total cost of recycling represents collection and transportation costs.[124] Evidence however has shown that where there is co-existence of waste collection programs, such as the electronic waste collection operating alongside an existing curbside waste collection procedure, this can substantially reduce the operating costs [125]

There is a significant body of literature pointing to the fact that the general costs of recycling in countries in south east Asia and Africa are much smaller compared to the costs of recycling in the US or Western Europe, due to wage differentials, access to resources, and lower industrial standards.[126] This suggests that costs for recycling may increase over time as wages in developing countries increase; also if the scarce materials recovered during recycling become more valuable as global stocks diminish.

The total costs for treating electronic waste (e-waste) from IoT at material recovery facilities is expected to be at least comparable to non-IoT equipment because the most important cost drivers are material costs, which includes the costs to recycle or outsource the recycle of materials, and labour costs.[127]

The fact that complex devices such as smartphones, tablets and smart TVs are among the most commonly own smart devices (as compared with relatively less complex smart devices such as smart lighting and thermostats) suggests that costs for recycling of IoT devices will be comparable to conventional ICTs and smartphones. These are costly for several reasons, including the fact that the complexity of intermediate materials cannot be kept to a lowest possible value, and recycling these materials creates relatively complex mixtures of scrap and recyclate products (e.g. liquid metal during processing to refined products and alloys) that negatively affects final recovery.[128]

Smart devices typically obey the same rule of thumb as other products: that shorter lifespans typically equal greater environmental costs. In addition, it is likely that smart devices would fit into current estimates according to which only around 15-16% of global e-waste is recycled in the

[123] Greenpeace. Guide to Greener Electronics, 2017

[124] Hainault T, Smith DS. Minnesota's multi-stakeholder approach to managing electronic products at end-of-life. In: *Proceedings of IEEE international symposium on electronics and the environment*; 2000. p. 310–7

[125] Kang, H-Y and Schoenung, J.M. 2005. Electronic waste recycling: A review of U.S. infrastructure and technology options. In *Resources, Conservation and Recycling* 45 (2005) 368–400.

[126] The Basel Action Network and Silicon Valley Toxics Coalition, exporting harm. The high-tech trashing of Asia; 2002; Jung LB, Bartel T. An industry approach to consumer recycling: the San Jose project). In: Proceedings of IEEE international symposium on electronics and the environment; 1998. p. 36–41; Hainault T, Smith (2000) quoted above; Greenpeace. 2016. Resource Efficiency in the ICT Sector. Final Report, November 2016; The Electronics Recycling Landscape Report, The Sustainability Consortium, May 2016)

[127] Kang, H-Y and Schoenung. 2006. Economic Analysis of Electronic Waste Recycling: Modeling the Cost and Revenue of a Materials Recovery Facility in California. In *Environ. Sci. Technol*. 2006, 40, 1672-1680

[128] See Fairphone's Report on Recyclability: "Does modularity contribute to better recovery of materials?" 2017

formal sector[129], while materials recovered compared to annual material use can be as low as 11% in the most successful cases. “Recycled” e-waste can, depending on local regulations and enforcement, end up at informal recyclers and handled in ways that endanger worker health and the local environment.

The discussion above covers the cost metrics at the equipment level. However, the facility level metrics for IoT devices and corresponding services provide an additional overhead to the existing mobile infrastructure that is difficult to estimate, especially because of the different possible network architectures, routing and distribution aspects.[130]

Cost of Disposal of Non-Compliant Stock

Following a review of relevant literature, market research and the consumer, retailers and manufacturers survey, an adequate evidence base for costs could not be derived. At a high level, we could expect the cost of disposal to be between 0.5%-1.6% of manufacturers’ IoT turnover (where borne by manufacturers), based on the findings of the survey. This cost estimate is based on a small number of responses, and therefore the cost of disposal of non-compliant products could not be estimated robustly within this research. Our literature review of the impacts of similar regulatory changes highlighted the absence of cost data available.

There is uncertainty over customer behaviour with regard to passing non-compliant stock onto second-hand retailers, and whether all second-hand retailers (e.g. non-specialists) would be aware of the regulations; it is likely that some sale of non-compliant goods would continue.

The Green Book’s supplementary guidance for calculating environmental costs provides a methodology for estimating changes in fuel usage and production of carbon, and costs associated with these; however, this requires baseline evidence on the level of energy required for disposal of IoT devices which is not present in the literature. As outlined in the evidence gathered in our primary research (surveys with manufacturers and retailers), approximately 55% of the non-compliant stock would be disposed of and would incur disposal costs in relation to carbon as outlined above.

In summary, the areas of disposal are likely to include:

- The costs of disposing, recycling or reshipping non-compliant products
- Loss of sales revenue from non-compliant products
- Cost to the environment (in relation to the costs of carbon) of potential increased disposal of devices

The only quantitative evidence available for this study is therefore the evidence collected in our primary research with consumers and businesses, as set out above in this section. This suggests that the monetary costs to businesses of disposal are low, relative to the level of IoT turnover (up to 1.5%). This is also consistent with the estimated contribution recycling has to the greenhouse gas emissions of microelectronics (as reported by Greenpeace in 2017[131]).

[129] Greenpeace. Guide to Greener Electronics, 2017

[130] For a wider review of methods to measure energy consumption and costs see A. P. Bianzino, A. K. Raju, and D. Rossi, ``Apples-to-apples: A framework analysis for energy-efficiency in networks,'' ACM SIGMETRICS Perform. Eval. Rev., vol. 38, no. 3, pp. 81_85, 2011

[131] Greenpeace. Guide to Greener Electronics, 2017

8. THE IMPACT ON INTERNATIONAL TRADE

This section deals with the following research objective on international trade:

- Quantitative and qualitative evidence on the short, medium and long term impacts of a proposed ban on non-compliant products for UK trade and investment, including trade with suppliers in China/South East Asia. This could include existing evidence on impacts in other sectors as a result of similar proposals.

It is based upon:

- a review of published information and data on industry trends and regulatory challenges, and the potential economic implications from the proposed requirements for businesses affected by the regulation;
- a review of industry intelligence regarding the impact of regulatory requirements related to DCMS's current proposals, including impact assessment and studies of comparable regulations;
- analysis of the consumer and business survey data on current market activity and expected responses to any change in regulations; and
- model-based simulation of the impacts of higher costs of production brought about by the regulations, and a proposed full import ban for non-compliant products.

Summary

Quantitative and qualitative evidence was collected on the short and medium-term impacts of a proposed ban on non-compliant products for UK trade and investment, including trade with suppliers in China/South East Asia, from survey research and review of relevant literature and data. A trade model was built to estimate the impacts of two policy options: mandating aspects of the top three CoP guidelines, and the mandatory security labelling requirement.

Under both policy options, overall economic activity in the UK will remain largely unaffected by the proposed measures. UK trade volumes will only marginally decrease in response to the implementation of the policy measures. The highest relative impacts would likely result from costs related to the disposal of non-compliant products. These costs are, however, temporary. Foreign suppliers are expected to amend their products and make sure to comply with UK regulations. Given the relatively low additional cost that would result from the proposed measures, including one-off and recurring costs, UK production as well as UK trade would remain largely unaffected.

Even though the aggregate impacts are relatively low, often negligible, for the entire UK economy, the costs impacts will be different for different types of companies, depending on their business model, the share of imports, import partners and other characteristics.

Generally, SMEs would be more affected than large companies as they face higher compliance costs per unit of production/imports, which may decrease their domestic and international competitiveness.

Given that the magnitude of the estimated effects is relatively small, we expect the impact of the proposed regulations on product innovation, domestic and international demand and domestic and international supply to be relatively low. As concerns investment in the UK, we neither expect investment to decrease as a result of the regulations, nor do we expect a deterioration of the UK's investment climate because of the regulations.

The effects on UK trade and investment will be even smaller still if more countries proceed with the implementation of similar sets of regulations. International cooperation aiming for harmonised standards would contribute to maintaining high trade volumes in the medium- and long-term, while the proliferation of diverse unilateral measures would increase distortions in international trade.

Methods and assumptions

The estimation of medium- and long-term effects is based on a general equilibrium model simulation and conducted on the basis of the GTAP Model by the Global Trade Analysis Project (GTAP). The model is comparative static. It has been applied frequently in studies about impacts of trade policy, including tariffs and non-tariff barriers to trade. We apply a multi-regional, multi-sector, computable general equilibrium model that is characterised by perfect competition, constant returns to scale and Armington elasticities. The model assumes full mobility and employment of factors of production, i.e. all factors of production including labour will adjust until they are fully absorbed after the policy change. The costs are expressed in the form of tariffs and are borne by the importing companies in the first instance.

Our model does not account for endogenous productivity growth and may thus under- or over-predict changes in welfare, investment, economic output and trade volumes that result from trade policy changes. Like any applied economic model, the model is based on a number of assumptions which simplify the complex policy framework governing the national economies and the global economy. The results of the estimations therefore only have indicative character. It should be noted that it is not possible to forecast the precise impact of changes in trade policy variables on macro-economic variables, mainly due to lack of empirical data and real world complexities, i.e. the influence of too many different factors and non-constant causal relationships.

As base data we use the most up-to-date GTAP 10 database, which was released in July 2019. The database contains global trade data for the years 2004, 2007, 2011 and 2014 based on input output tables and trade protection data. The GTAP 10 dataset on the global economy is extrapolated to reflect the “best estimate” of the global economy today. The exogenous variables which are shocked for the extrapolation include the most relevant macroeconomic variables, i.e. population, labour force, total factor productivity and capital endowment. A coding scheme was devised for the consumer IoT products using the Harmonised Standard coding system used in trade statistics to map the three product groups.

A full literature review was carried out to provide corroborating evidence on costs and impacts of similar legislation. It was divided into three parts:

- Regulatory proposal-related literature and the impact on costs and the implications on trade and investment.
- Subject-related literature and the impact on costs and the implications on trade and investment; and
- Policy intervention-related literature and the impact on costs and the implications on trade and investment.

Modelling impacts of policy options

We have considered two distinct policy options.

Policy option 1 (mandating a security label) includes the cost of physical labels, and costs related to recurring self-assessment.

Policy option 2 (mandating aspects of the top 3 CoP requirements) included costs related to default passwords, vulnerability disclosure policies, minimum security update period, costs related to recurring self-assessment, and costs related to the disposal of non-compliant goods.

In both cases we distinguish between a) short- to medium-term effects (including familiarisation cost and annual recurrent cost) and b) longer-term effects (including recurrent costs only). It is assumed that companies have to bear additional costs from becoming familiar with new regulations and from setting up new processes respectively. We also assume that in the long-run, a high proportion of substantive compliance costs are integrated into firms' product design cycles.

Impact of company size on compliance costs

The numbers stated by the survey respondents are to the largest extent numbers stated by large multinational companies. Trade data show that UK trade in "computer, electronic and optical products" and "electrical equipment" is dominated by large companies (both for exports and imports). Measures in terms of total import values, in "computer, electronic and optical products" large companies account for 78% of UK imports. In "electrical equipment", large companies account for 59% of UK imports.

It should be noted that SMEs account for lower shares of imports in both sectors, but generally face a higher compliance cost burden by unit (evidenced in the literature review and the survey of manufacturers).

Adjusting for trade by company size results in different cost impacts for different sizes of companies. Generally, smaller companies would have to bear a much higher additional cost burden per unit than larger companies, whereby the burden per unit is lowest for companies with more than 250 employees (which are the UK's major importers). It should be noted that we do not account for differences in the magnitude of the additional costs that accrue for exporters in different countries. We assume the effect to be equal in relative terms for all trading partners.

Summary of model results

Overview

We estimate the impacts for two policy options over a period of 5 years after the implementation, for which, however, the economic impacts (changes in production and trade) are not distributed equally over the whole period, i.e. each year. For example, the combined effect from additional regulation-induced fixed cost (e.g. familiarisation and implementation cost) and additional variable cost would impact more on trade in the time period that immediately follows the implementation of a policy. Further into the future, there will be no additional fixed (one-off) costs.

Some of the impacts of policy option 1, (mandating a security label) occur in the short term, corresponding to a period of time in which UK importers and foreign exporters/manufacturers need to become familiar with the new regulations. We assume that the familiarisation costs take effect immediately after the measurers are implemented and, accordingly, start to impact on UK importers and foreign manufacturers/exporters. In addition, we assume that related compliance costs, both administrative (e.g. documentation) and substantive (e.g. testing for conformity) will also unfold their effects within the first year following the implementation. Due to the model's characteristics, the overall results of policy option 1 (our model's output) would materialise within the first 5 years after the implementation of the policy measures, whereby the impact of the familiarisation costs would likely be highest within the first two years after the implementation.

Policy option 2 (mandating aspects of the top 3 CoP guidelines) is most impactful in the short-to-medium term, taking into account that in the long run a high share of firms in the UK and abroad become familiar with the new regulatory requirements and adapt. Temporary non-compliance would reduce exports to the UK in the short- to medium-term. In the longer term, the negative impacts are assumed to gradually phase out as a higher share of companies become more compliant, which is reflected by annualised changes in trade volumes that are nearer to the baseline position, particularly in the second half of the 5-year time horizon.

Assuming that a high proportion of companies that still import/export to the UK will manage to become compliant within the first two years after the implementation, **the impacts under policy**

option 2 are of lower magnitude than the results for policy option 1 after the first two years, as the negative impacts are assumed to gradually phase out and a higher share of companies become more compliant; this is reflected by the annualised reductions in trade volumes becoming lower, particularly in the second half of the 5-year time horizon. By way of comparison, the costs for labelling and self-assessment under policy option 1 persist into the medium and longer-term.

Various caveats should be taken into consideration when reading the summary findings with regard to the impact of additional costs on UK trade in the affected product categories. Firstly, the survey data are not representative. The cost estimates indicated by firms reflect their representatives' perceptions. The numbers are nevertheless broadly in line with those of other studies that addressed the impact of related policies on companies' compliance costs.

Secondly, our model is comparative static. CGE models generally suffer from some shortages with respect to data inputs, the assumptions underlying policy changes and the equational frameworks. It should be noted that the output of any model will never be of higher quality than the data put into it, including data for policy options and the state of the economy. However, as recently discussed by European Commission (2019), for example, alternatives to CGE models have not yet proven to be sufficiently reliable for ex-ante analyses of economy-wide effects of trade policy changes.[132]

The results of the model should not be read as point estimates. The results indicate the direction of the development of economic variables, e.g. changes in domestic production, changes in exports, changes in imports and changes in overall economic activity. The results should also be benchmarked against the magnitudes of the impacts from other trade policy measures, e.g. high tariff and non-tariff barriers.

That said, for both policy options the estimated changes that result from the policy measures proposed by DCMS are relatively low and often negligible in magnitude. For both policy options, overall economic activity will not be affected, neither in the UK nor in the trading partners' countries. Summaries are provided below. The overall change in UK imports and exports are also very low.

Policy option 1: Physical security label

For policy option 1, we do not find significant one-off or familiarisation cost. Recurring activities for companies' self-assessment include activities to become familiar with labelling requirements. Accordingly, the results reflect longer-term impacts for a 5-year time horizon after the implementation of the proposed policies.

Under policy option 1, UK domestic industry output slightly increases across the board for the sectors affected by the policy measures. The highest relative increase is recorded for smart electrical equipment (+0.32%), followed by smart computer and electronic products (+0.3%). As the changes materialise over a 5-year period, the annual changes are relatively small.

UK production would be affected by higher regulatory costs, which in turn have an impact on UK suppliers' relative international competitiveness. The negative effects are only marginal though. UK aggregate export volumes in the sectors affected by the policy measures would only marginally decrease. The highest decreases are estimated for the smart computer and electronic products sector and for smart electrical equipment (-0.21%). As the numbers reflect changes for a 5-year time horizon, the annualised numbers are negligible. This is also true for smart boilers and for smart toys and video games.

UK aggregate import volumes in the sectors affected by the policy measures would also slightly decrease as importers would have to bear higher costs. The highest relative decrease is

[132] European Commission (2019). Reflection on the Economic Modelling of free Trade Agreements. Chief Economist Note. Issue 2, 2019.

estimated for smart toys and video game consoles (-0.63%). As the numbers reflect changes for a 5-year time horizon, the annualised numbers are negligible. This is also true for other sectors affected by the proposed regulations.

Bilateral imports from the UK's key trading partners are estimated to only slightly decrease in all sectors affected by the regulations. Recognising that the changes would materialise over a period of 5 years, the annualised changes are negligible.

Policy option 2: Mandating aspects of the top 3 CoP requirements

The estimates in policy option 2 account for both short- to medium-term and longer-term effects. The relatively significant one-off costs that are related to the disposal of non-compliant goods are reflected by the estimates for short- to medium-term effects. Since we assume that companies increasingly comply with the new regulations over time, and amend products respectively, the costs of disposal of non-compliant products have been excluded from estimates for longer-term effects, which only include recurrent costs.

Under policy option 2, UK industrial output would slightly increase across the board for the sectors affected by the policy measures (relative to the baseline). In the model, the increase in UK domestic output results from a temporary lack of competitiveness of companies that import to the UK. In practice, UK production would substitute for non-compliant products that were previously imported to the UK. The highest relative increase is recorded for smart electrical equipment (+1.52%), followed by smart computer and electronic products (+1.42%). It should be noted that the changes would likely materialise within the first two years of the 5-year period modelled for this policy option. However, even for a 2-year time horizon, the annual changes in production volumes would be relatively small. The effects would phase out over the longer term. Over the longer term, the impact of recurrent compliance cost would be marginal, leaving UK production largely unaffected.

For the sectors affected by the policy measures, UK aggregate export volumes would initially slightly decrease for all product categories (from -0.56% for smart toys to -0.99% for smart electrical equipment). In the short- to medium-term, the decrease in the UK's aggregate export volumes results from temporary lack of competitiveness of companies that import to the UK. UK production would satisfy domestic demand, which results in lower aggregate exports from the UK. It should be noted that these effects would likely materialise within the first two years of the 5-year projection period. However, even for a 2-year time horizon, the annual changes in aggregate export volumes would be relatively small. As with the impacts on domestic output, the effects would phase out over the longer-term, leaving UK exports largely unaffected.

Bilateral imports from the UK's key trading partners are estimated to only slightly decrease in all product groups affected by the proposed regulations. The impacts are generally less pronounced than decreases in UK exports. In the short- to medium-term, the decrease in the UK's aggregate import volumes results from a temporary lack of competitiveness of companies that import to the UK, resulting in lower aggregate imports to the UK. It should be noted that these effects would likely materialise within the first two years of the 5-year projection period. However, even for a 2-year time horizon, the annual changes in aggregate import volumes would be relatively small. The effects would phase out over the longer-term. The regulations' effects, particularly the cost impact related to the disposal of non-compliant products, would phase out over time, leaving UK imports largely unaffected in the longer-term.

Summary

In both policy options, overall economic activity in the UK will remain largely unaffected by the proposed measures. UK trade volumes will only marginally decrease in response to the implementation of the policy measures. The highest relative impacts would likely result from costs related to the disposal of non-compliant products. These costs are, however, temporary. Foreign suppliers are expected to amend their products and make sure to comply with UK regulations.

Given the relatively low additional cost that would result from the proposed measures, including one-off and recurring costs, UK production as well as UK trade would remain largely unaffected.

Even though the aggregate impacts are relatively low, often negligible, for the entire UK economy, the cost impacts will be different for different types of companies, depending on their business model, the share of imports, import partners and other characteristics.

Generally, SMEs would be more affected than large companies as they face higher compliance costs per unit of production/imports, which may decrease their domestic and international competitiveness.

Given that the magnitude of the estimated effects is relatively small, we expect the impact of the proposed regulations on product innovation, domestic and international demand and domestic and international supply to be relatively low. As concerns investment in the UK, we neither expect investment to decrease as a result of the regulations, nor do we expect a deterioration of the UK's investment climate because of the regulations.

Any distortions in investment could be limited if UK regulators seek for international harmonisation of consumer IoT security standards and enforcement procedures. Similar considerations apply for competition and innovation. Non-discriminatory treatment of domestic and foreign suppliers would safeguard competition in the short-, medium- and longer-term. Non-discrimination would also allow UK companies and consumers to access and adopt innovation from abroad, and vice versa.

9. BENEFITS OF MANDATING SECURITY REQUIREMENTS TO CONSUMERS, BUSINESSES, AND SOCIETY

The research sought to explore benefits to (a) manufacturers (b) retailers (c) consumers (d) society that would be incurred from mandating a security baseline for IoT, with an estimated financial value placed on each of these groups.

The research therefore explored the perceived benefits of IoT goods to consumers; the likelihood (and estimated amount) of increased expenditure on consumer IoT goods if security information were provided, accruing as a financial benefit to producers and retailers; and benefits perceived by producers and retailers of the regulations on their companies, their sector, and consumers.

Benefits of device ownership to consumers

A key benefit to consumers is the functionality of the IoT products that they buy. Reasons for purchase of smart devices, as expressed by respondents to the consumer survey, are set out in Table 84 below; all responses are given, with those that express a benefit of IoT device ownership in blue font.

Table 84: Reasons that consumers purchase smart devices

Reasons for purchase	Percentage of respondents
My smart device(s) can synchronise easily with other devices (e.g. smartphone etc.)	20%
Better functionality than non-smart version of the product	17%
It's more convenient to check or change things in my house (e.g. playing music, changing temperature, turning lights on/off etc.)	15%
I like keeping up with the newest in technology and gadgets	13%
I was given the device as a gift/or part of a bundle	11%
I got a smart device when it was on offer as part of Black Friday, Cyber Monday or post-Christmas sales	9%
I got a smart device to make things easier in my routine (e.g. preheat my oven, monitor my babies' activity, observe my health)	9%
I got a smart device when it was on offer at other times of the year (i.e. NOT part of Black Friday, Cyber Monday or Christmas sales)	7%
I can keep an eye on my home and how different services are used	6%
It was better value than the non-smart version of the product	6%
I feel more secure (i.e. feeling safe inside my home etc.)	5%
I got a smart device for free when I bought another product	5%
Other	9%
Don't know	33%

Source: Consumer survey: Q6 Which if any of the following are reasons why you purchased smart devices, including smart appliances? Please tick all that apply. (n = 5,148 – all survey respondents)

The three most commonly cited reasons for purchasing smart devices were: the ability to easily synchronise with other devices (20%); better functionality than equivalent non-smart devices (17%); and convenience in managing household devices (15%). These reasons overlap to some degree; overall, the positive reasons highlighted above amount to around half of the responses, although it is notable that "don't know" is the single most common response, at 33%.

Improving the security provisions of smart devices and the information provided to consumers may encourage those who currently opt out of internet connectivity due to security/privacy reasons to reconsider using the 'smart' functionality of their devices. Our consumer survey found that on average, 25% of big ticket item owners had opted out of internet usage at some point, alongside 24% of consumer lifestyle device owners, and 15% of those owning 'connecting the home' devices. If security concerns are a reason for disconnecting devices, consumers would potentially benefit from improvements to security that give them the confidence to remain connected and able to benefit from the additional features and conveniences provided by internet connectivity.

Improvements in the provision of security information and features could also increase the sales of consumer IoT devices, as many respondents indicated that privacy and security concerns were factors in avoiding the purchase of smart devices. Overall, 30% of consumers who indicated that they are unlikely to purchase any smart devices in the next year stated that a reason for this was concern over the privacy of smart devices. Concerns over security (e.g. unauthorised access to devices) were also a key reason for not purchasing smart devices, with this being selected by 28% as one of the reasons for not purchasing.

In total, privacy was found to be a reason for not purchasing smart devices for 11% of the sample, and security for 10% of consumers. However, as the top reasons for not purchasing were “I am not interested in the smart home” (62%) and “There are not enough reasons for me to get any smart devices” (49%), there are clear limits to how much of an impact improved security features and information could make in increasing device take up.

In summary, improvements in security features and the provision of security information could therefore increase the utility of smart devices to UK consumers overall, as those who currently do not benefit from smart technology could begin to do so.

Evidence on consumer benefits from literature

PwC’s Connected Home 2.0 Report highlighted that before making a purchase, only one in five consumers expect to be positively impacted by a connected home device.[133] However, once purchased, consumers indicated much higher levels of actual consumer value. The perceived health benefits, for instance, of a smart hub/assistant were rated as important by 13% of purchasers prior to purchase, compared to 44% after purchase. Comfort value added by smart hubs/assistants also increased after purchase, almost doubling from 33% to 65%. Consumers of energy meters reported a pre-purchase impact value of 23% for comfort and 56% in financial terms before purchase, with these increasing to 54% and 72% respectively after purchase.

These findings reflect that many consumers do not expect the benefits of smart device ownership to be as significant as they find them to be after purchase. As security information and improved security features could increase the number of consumers of IoT devices, this growth could have a greater utility and comfort benefit than is expected by consumers.

Research by Park et al into Comprehensive Approaches to User Acceptance of Internet of Things in a Smart Home Environment[134] analysed the technology acceptance model (TAM) in order to assess the factors that determine user intentions with IoT technologies. They conclude that these factors contribute towards the perceived usefulness and ease of use of consumer IoT devices. ‘Perceived enjoyment’ was found to be one of the most notable motivations behind using consumer IoT devices, reflecting that users have fun interacting with IoT technologies and enjoy using these in a smart home environment. ‘Perceived connectedness’ was also a key advantage of using IoT technologies, with users hoping to benefit from convenient utilisation of their devices without physical interaction.

[133] Connected Home 2.0 (2018): www.pwc.co.uk/industries/power-utilities/insights/energy2020/connected-home.html

[134] Comprehensive Approaches to User Acceptance of Internet of Things in a Smart Home Environment (2017), Eunil Park, Yongwoo Cho, Jinyoung Han, Sang Job Kwon. IEE Internet of Things Journal, Vol 4, No. 6.

The EY Taking new steps into the smart home report[135] highlights that households are becoming increasingly receptive to smart home devices and cites greater levels of control, convenience, and efficiency as factors that are resonating with consumers.

Effect of security information on likelihood of purchase

The consumer survey explored the factors that encourage people to purchase smart devices, as shown in Table 85 (below).

Table 85: Factors that would encourage purchasing of smart devices

Factors to encourage purchase	Percentage of respondents agreeing
Independent certification/assurance scheme of adherence to a minimum security standard	28%
Transparency on the length of time that security updates will be provided	22%
Assurance that every device has a unique password	20%
Security information at point of sale	19%
Assurances from manufacturers on adherence to a minimum security standard (by 'manufacturers' we mean a business or company which makes goods in large quantities to sell)	19%
Assurance that any security issue or vulnerability can be reported to the manufacturer (by 'manufacturer' we mean a business or company which makes goods in large quantities to sell)	17%
Other	26%
Don't know	35%
Base	690

Source: Consumer survey Q119 You said that you were unlikely to consider purchasing consumer smart devices because you are concerned about security, privacy and the quality. Which, if any of the following would influence you to purchase a smart home device? Please tick all that apply. (n=690 – all unlikely to purchase smart devices due to security, privacy, or quality concerns)

This table helps pinpoint the factors that may encourage those who indicated that security, privacy, and quality concerns mean that they are unlikely to purchase consumer smart devices, to do so. The most popular feature that may encourage purchasing a smart device (given by 28%) was that an independent certification scheme of adherence to a minimum security standard. The second most popular feature (given by 22%) was transparency around the length of time that security updates will be provided. It is also worth noting that 35% of respondents indicated that they do not know what factors would influence them to purchase smart devices. Moreover, 26% of respondents chose ‘other’; when asked to give further details of this in an open text response, many consumers indicated that there are no factors that could convince them to purchase smart devices.

By product group, 92% of people own a “consumer lifestyle” device, 56% own a “big ticket item”, and 38% own a “connecting the home” device. The two sectors of the market where IoT features and security information could make the largest difference are therefore in adopting “connecting the home” devices (62% of the population do not own one) and adding smart features to big

[135] Taking New Steps into the Smart Home: Consumer Attitudes to the Connected Home (2019): https://assets.ey.com/content/dam/ey-sites/ey-com/en_uk/topics/technology-media-entertainment-telecommunications/ey-taking-new-steps-into-the-smart-home.pdf

ticket devices (44% of the population do not own a smart big ticket item, but are likely to own a non-smart equivalent).

Benefits to businesses

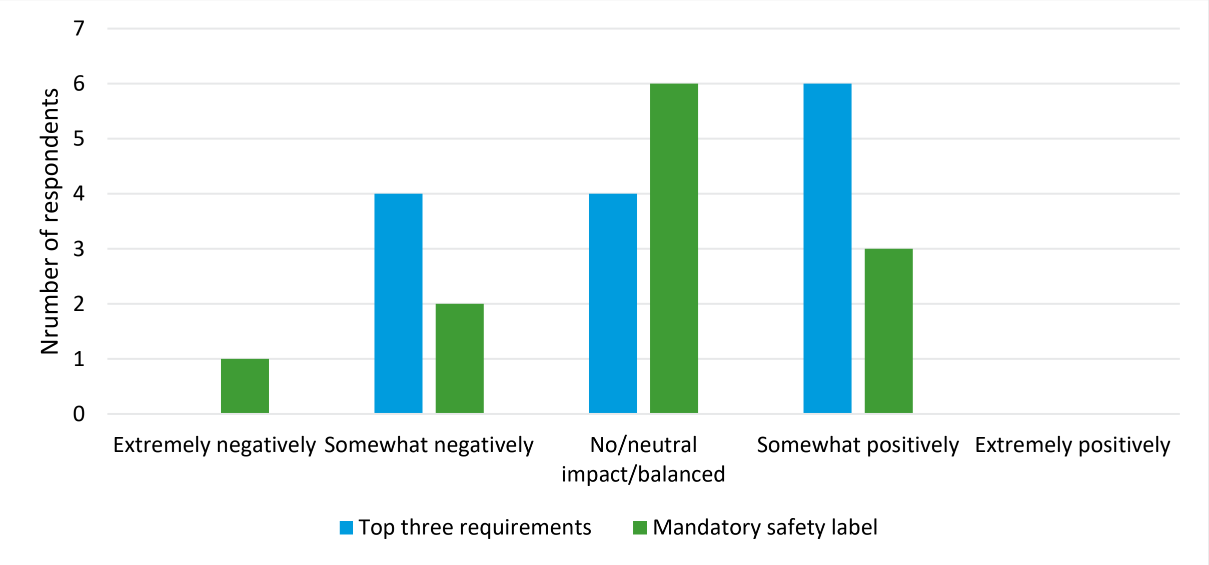
The consumer survey showed that mean expenditure per person over the last 12 months on IoT devices[136] is £124.21 across the whole adult UK population, but £302.76 among those who already own such a device. The scale of the potential benefit to manufacturers and retailers of IoT devices in the medium term could therefore be estimated to be £302.76 per person convinced to begin to adopt IoT devices.

It can be inferred from the evidence above on factors that would encourage consumers to purchase IoT devices (Table 85) that improved provision of security information could benefit both manufacturers and retailers of consumer IoT devices, as they may see increased sales if consumers perceive risks to be lower.

Benefits of proposed regulatory options for consumer IoT products – evidence from manufacturers

We asked manufacturers how the proposed regulations around compliance with the top three security requirements of the Code of Practice for Consumer IoT Security and mandatory labelling would affect them.

Figure 27: Expected impacts of proposed regulatory options on manufacturers



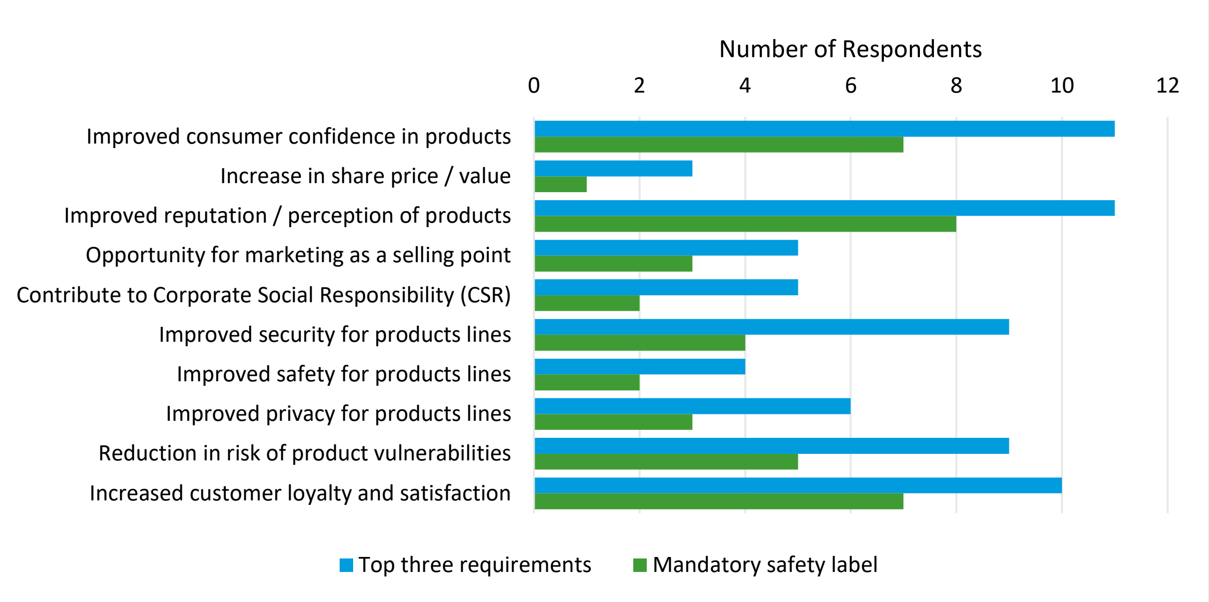
Source: Manufacturers' Survey Q77, March 2020 (n=14, n=12)

No manufacturers believed that the impact on them of these measures would be extremely positive, with most saying that this would impact them somewhat positively or there would be no/ neutral/ balanced impact. Two manufacturers believed that labelling measures would somewhat negatively impact them (17% total), only one said that mandatory labelling would impact them extremely negatively.

[136] Excluding smartphones and tablets, which were omitted from this section of the research in order to focus on less-ubiquitous devices and also as these take the form of enablers or interfaces for other smart devices

Respondents were then asked what the benefit to UK manufacturers would be if the top three security requirements of the Code of Practice for Consumer IoT Security and a security label that indicates whether the product adheres to these requirements became mandatory:

Figure 28: Benefits to UK manufacturers of proposed regulatory options



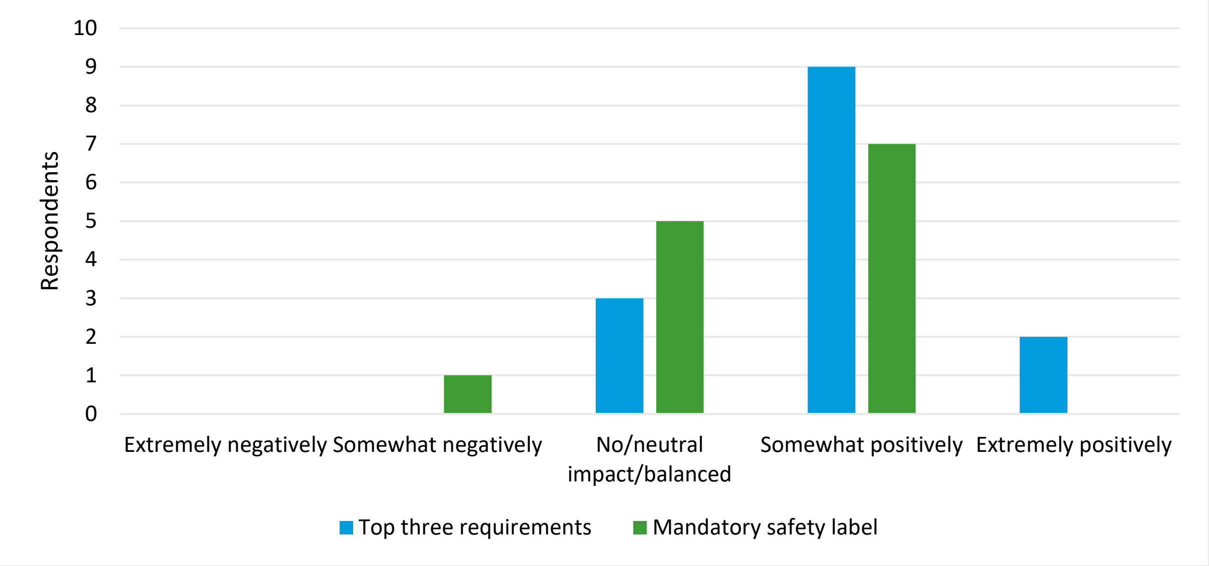
Source: Manufacturers' Survey Q78, March 2020 (n=14)

The most common responses were that mandating these measures would improve consumer confidence in products, improve the reputation or perception of products, increase customer loyalty and satisfaction, improve security for product lines, and reduce the risk of product vulnerabilities and. Very few manufacturers believed that this would increase the share price or value of UK manufacturers.

The manufacturers had a more positive view of mandating the top three security requirements of the Code of Practice than of labelling. The number of respondents stating a benefit from the top three was greater for every type of benefit than for the mandatory security label. Qualitative comments also questioned whether customers could understand labelling, describing labelling as having “value only if compliance is enforced” or “a game which big companies can afford to win”.

Manufacturers were also asked what they believed the expected impacts to UK consumers would be from mandating the top three security requirements and mandating physical security labels:

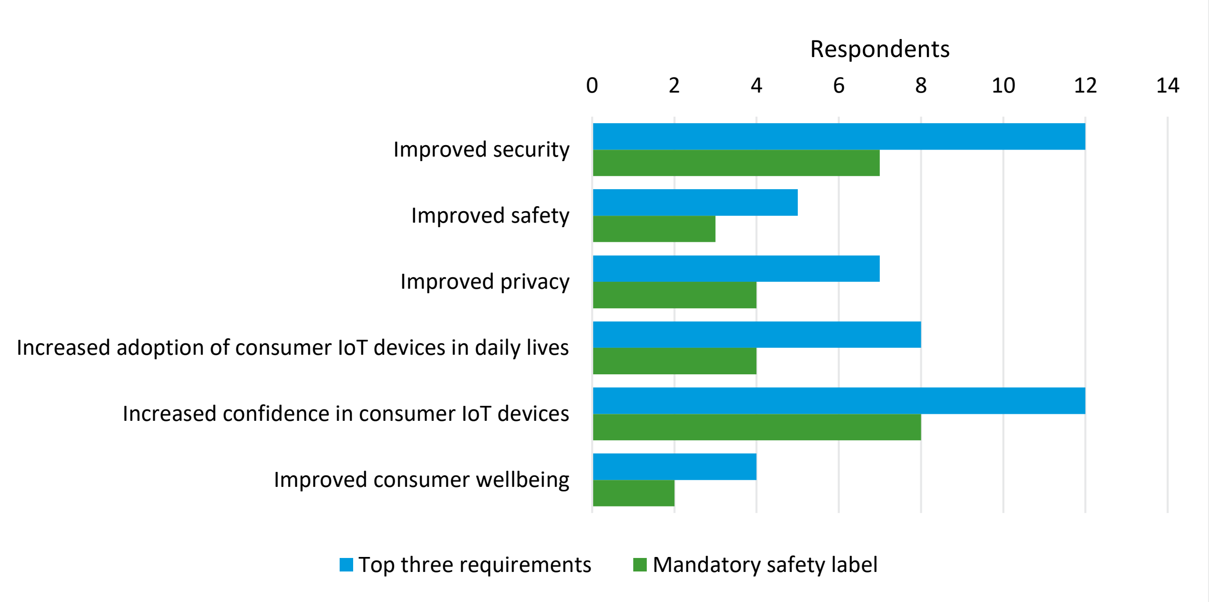
Figure 29: Expected impacts to UK consumers from proposed regulatory options



Source: Manufacturers' Survey Q79, March 2020 (n=14, n=13)

No respondents thought the expected impact of the proposed changes would be extremely negative for either mandating the top three requirements or mandatory labelling. No manufacturers thought that the top three security requirements would have any negative impact on UK consumers. Most believed that this would somewhat positively impact consumers, with several saying that there would be no impact, or a neutral/ balanced impact. Only two said that mandating the top three security requirements would have an extremely positive impact.

Figure 30: Benefits to UK consumers from mandating security requirements (perceived by manufacturers)



Source: Manufacturers' Survey Q80, March 2020 (n=14)

Most believed that this would lead to improved security and increased confidence in consumer IoT devices. However, a few manufacturers mentioned that mandating these measures may actually lead to UK consumers having a false sense of security in the level of protection provided by the security measures.

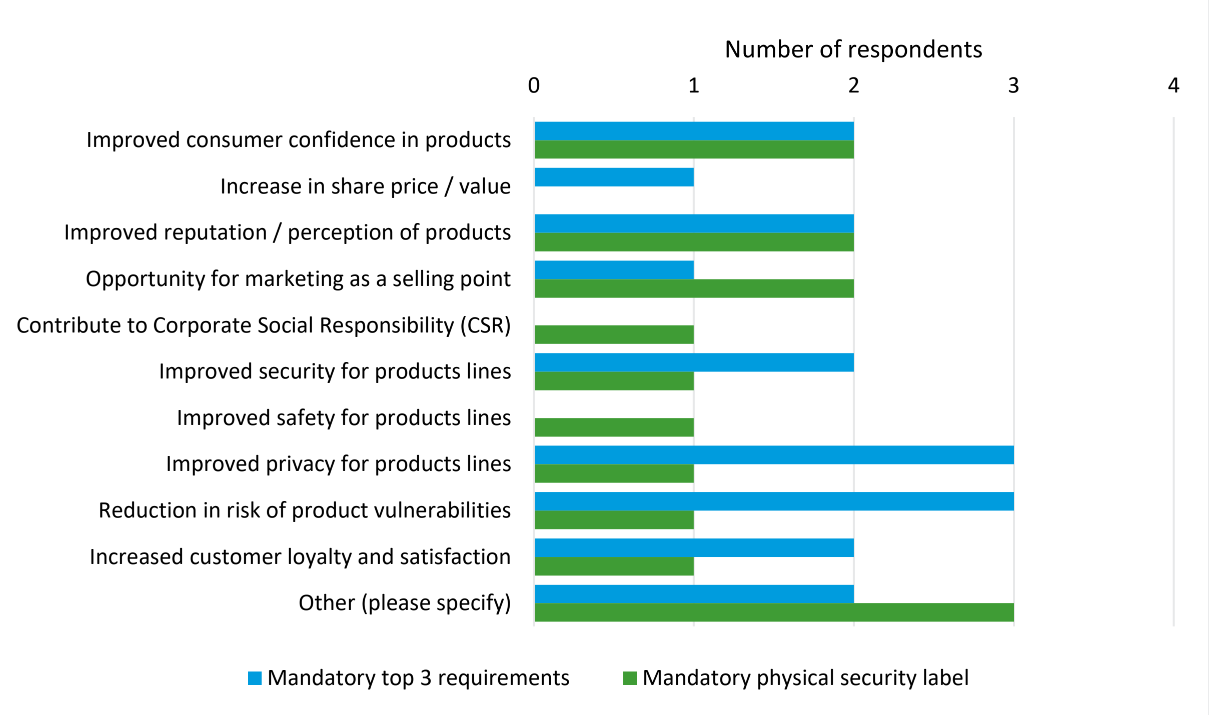
Benefits of proposed policy options for consumer IoT products: evidence from retailers

The retailer survey similarly asked retailers how the proposed regulations around compliance with the top three security requirements and mandatory labelling would impact their businesses.

It is important to note than only five retailers responded to this question. Notably, none of these retailers said that there would be an extremely positive impact from mandating the top three security requirements or mandatory labelling. Two retailers, however, believed that the expected impact of these measures would be somewhat positive. One said that the impact of these measures would be extremely negative, as this would present a huge admin cost for their organisation, which only employs two people.

Retailers were then asked what the benefits of mandating the top three security requirements and mandatory labelling would be to UK retailers.

Figure 31: Benefits to UK retailers of proposed options

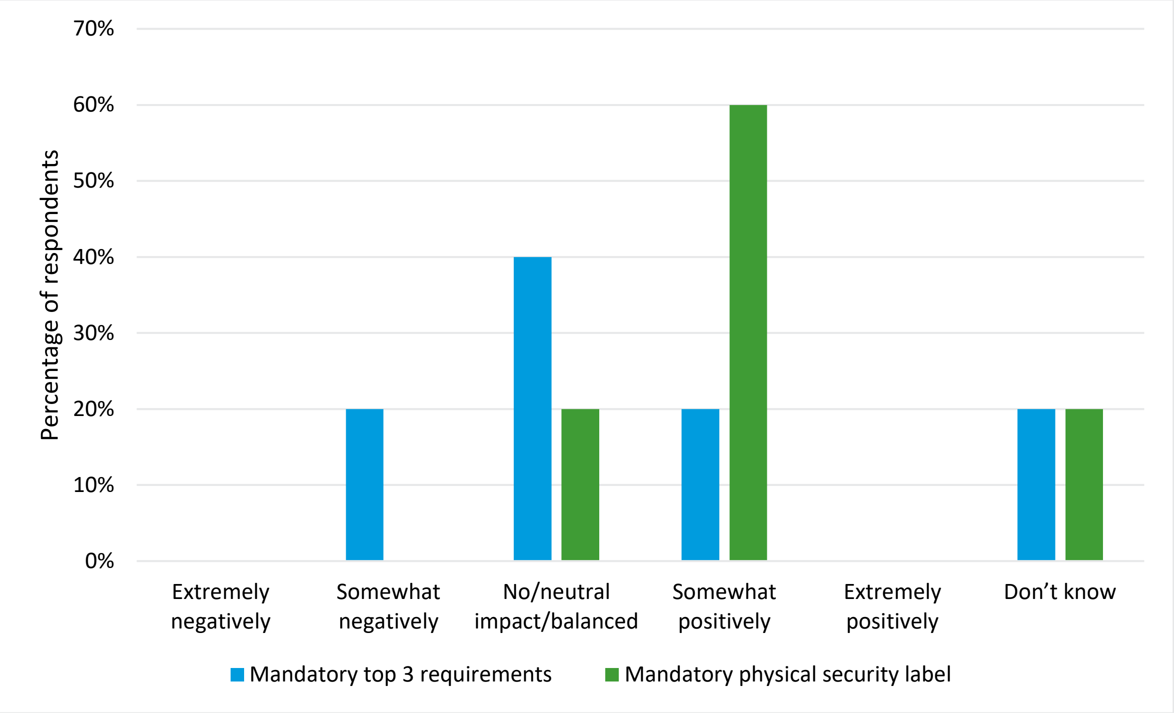


Source: Retailers' Survey Q37, March 2020 (n=5)

Retailers could select from a wide range of pre-coded responses to this question. The most common answers were that mandating the top three security requirements would improve privacy for product lines and reduce the risk of product vulnerabilities. At least two retailers said that either mandating the top three security requirements or mandating a physical security label would improve consumer confidence in products and improve the reputation/perception of products. One retailer said that these should not be requirements for retailers but that the legal requirement should be placed on manufacturers and then it should be up to retailers to ensure they are sourcing compliant products.

The retailer survey also asked respondents how they would expect UK consumers to be impacted by mandating the top three security requirements and mandatory labelling.

Figure 32: Expected impacts of proposed options on UK consumers (% of respondents)

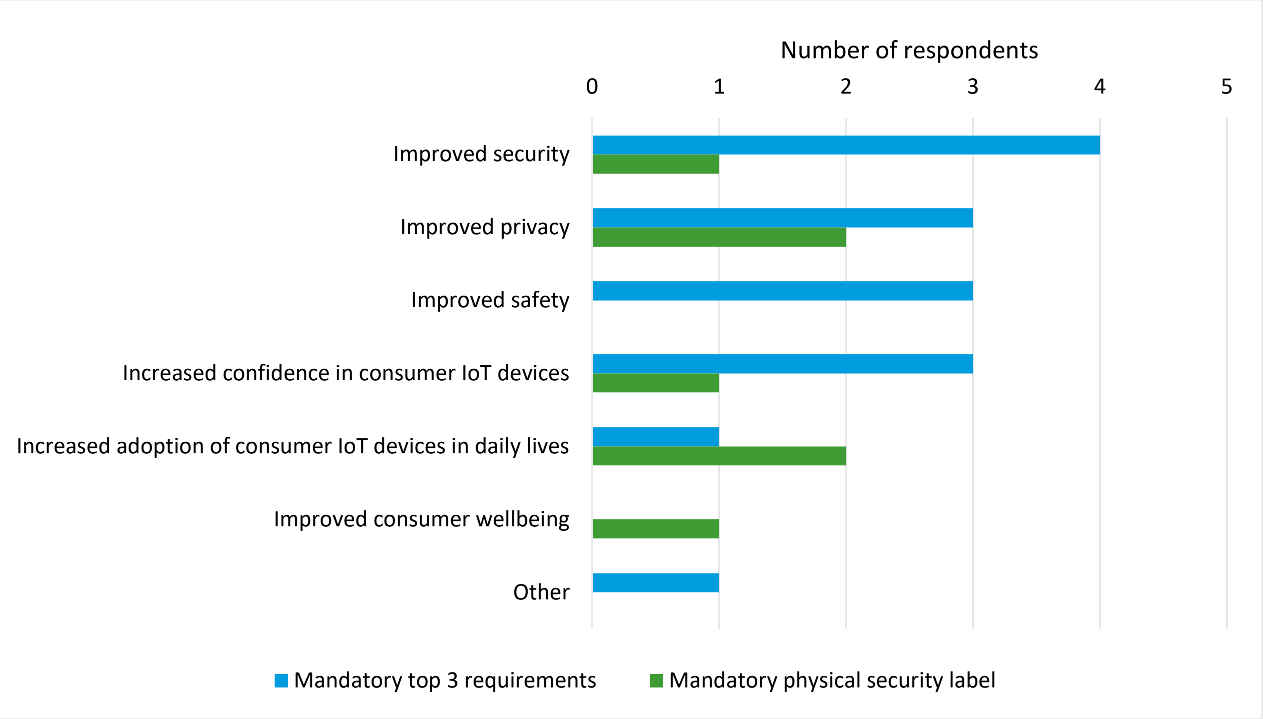


Source: Retailers' Survey Q38, March 2020 (n=5)

No retailers said that this would impact UK consumers extremely positively or extremely negatively. Most felt that mandating the top three security requirements of the Code of Practice for Consumer IoT Security would have no/ neutral/ balanced impact on UK consumers and that mandating a physical security label indicating whether products adhered to these requirements would somewhat positively impact UK consumers.

Respondents were then asked what the benefits to UK consumers would be of mandating the top three security requirements and mandatory labelling.

Figure 33: Benefits to UK consumers of proposed options



Source: Retailers' Survey Q39, March 2020 (n=4)

All of the retailers who responded to this question believed that mandating the top three security requirements would lead to improved security for UK consumers. Most retailers also believed that mandating the top three security requirements would improve the safety and privacy of UK consumers, as well as increasing confidence in consumer IoT devices. Retailers did not attribute the same level of benefit to UK consumers in mandating a physical security label; they were less likely in general to report benefits from this policy option than mandating the top three security requirements, particularly in the case of improved security and improved safety.

However, the retailers were more likely to report that the labelling option would increase adoption of consumer IoT devices in daily lives and improve consumer wellbeing than mandating the top three security requirements.

10. CONCLUSIONS

Overview

Business readiness: This varies greatly among the top three security requirements. There appears to be high market adoption of the "no default passwords" requirement. Information on vulnerability disclosure policies is mixed; these are not often clearly presented in product information but a majority of the manufacturers interviewed stated that they had these. The minimum security update duration was not in evidence in any of the products reviewed by the market study, although 24% of the manufacturers interviewed reported that they provided this information for all their products (6% - one respondent - provided it for some).

Regardless of the state of readiness of businesses, it is clear that publicly available information on the top three security requirements is close to zero. Mandating product security information at point of sale, or a labelling requirement, would address this and improve consumer knowledge, albeit with the risk of providing a false sense of security (as mandating the top three requirements would not prevent all product vulnerabilities).

Business costs: These are minimal, relative to company IoT turnover, and likely to be mitigated by expected sector growth. Modelling the impacts of policy on trade revealed virtually zero net effect, as UK production would rise to offset any banned imports from overseas. There is no expected impact on investment.

Consumer benefits: The scale of the potential vulnerability is large, as evidenced by the widespread adoption of IoT devices as set out in the consumer survey, and the potential benefits of the legislation in security terms are correspondingly great. Further benefits evidenced in this research appear to include an increased willingness to buy IoT products if assurances of security were provided. This was perceived as a greater barrier to adoption of IoT products than price.

Policy options: The policy option of mandating a security label was seen as less likely in general to produce benefits for consumers than mandating aspects of the top three guidelines of the Code of Practice. The costs, and the impacts on international trade and investment, were greater in the case of mandating aspects of the top three CoP guidelines, but neither were significant.

In summary: there is evidence that the proposed policies to improve consumer IoT security have potential benefits that greatly outweigh their potential economic costs. The section below lays out the key quantitative findings on the scale of vulnerabilities and evidence of potential impact.

Key quantitative findings

The **scale of IoT vulnerability** depends on the number of products owned by the UK population. From the consumer survey, average ownership is:

Group 1: big ticket items: 0.88 per household (1.59 per household that owning at least 1)
Group 2: connecting the home: 1.06 per household (2.94 per household owning at least 1)
Group 3: consumer lifestyle: 1.82 devices per household (2.01 per household owning at least 1)

Profile of manufacturers: We located 170 companies that manufacture and sell at least one consumer IoT product for the UK market. Considering only those products identified through searching online and offline retailers, most produced only 1 or 2 products, although one manufacturer included was found to produce 140. The average of the market study was 2.12.

Most of the manufacturers that responded to the survey (61%) produced between 1 and 15 product lines; the median was eight product lines. However, the average was 21, as the survey included some companies with a high number of IoT product lines.

Mandating the top 3 Code of Practice principles:

Default passwords: There is little explicit evidence of products with this vulnerability in the market. None of the products examined in our market study explicitly stated on packaging or at the point of sale that they were supplied with a default password; however, as many did not include any publicly-available security information, this is not conclusive evidence that the products are on the market have unique passwords (a finding repeated in the literature). The evidence from the manufacturer survey is more conclusive: among 17 respondents that discussed the issue, only one indicated that any of their devices are produced with a default password, and this was only the case for 1-10% of their products. The cost to manufacturers of removing default passwords in their devices were reported as negligible.

Vulnerability disclosure policies: There appears to be a disconnect between information readily available to consumers and company policies. Only 7% of "connecting the home" products, 8% of "consumer lifestyle" products, and no big ticket items at all came with information in packaging or online product description on such policies; however, 12 out of 16 respondents to the manufacturer survey stated that they had such a policy. As many companies believed that they were already compliant and would require no extra resources to implement such a policy, **the average cost of implementation across all manufacturers is just £2,530.**

It is not anticipated that regulation will affect disclosure of vulnerabilities by security researchers. The majority of companies in our survey sample already had some form of public route for vulnerabilities to be disclosed; they do not, therefore, anticipate that introducing legislation on vulnerability disclosure policies will lead to a great increase in their use. Surveys on security researchers indicate that they are already proactive in seeking routes to disclose vulnerabilities to companies.

Minimum support period for security updates: In our market study, we found no products that provided a minimum time period for which they would be available. This is corroborated by independent research[137] into 270 devices, none of which provided a minimum time period for security updates.

Among 17 respondents to our manufacturer survey that discussed the issue, four indicated that their products provided this information for all their products, and one for some (11-20%) of their products. However, the survey is likely biased towards early adopters of the Code of Practice who were willing to discuss the issues.

If aspects of this Code guideline were to become mandatory, ten companies said that they would implement it in full and provide the information for all of their consumer IoT products for sale in the UK. Two companies said they would stop selling some products in the UK, and one would stop producing some products in the UK.

Mandating aspects of this Code guideline potentially affects more of the market than the other two, and it is also viewed as more time-consuming to implement. **The average cash equivalent of the staff time to implement the policy (a one-off implementation cost) is estimated at £20,646.**

Physical labelling: Manufacturers estimated that an average of 20.7 person-days would be required to implement mandatory physical labelling on their products. Direct estimates of costs ranged from £37,500 to £60,000. Combining both methods of estimation, t**he average cost of implementation is estimated at £19,533.**

The manufacturers redesign their product packaging every 29.6 months on average, with most redesigning every 2-3 years. This suggests that with sufficient lead-in time, the labelling could be built in to regular redesign, thus reducing the cost.

[137] Blythe JM, Sombatruang N, & Johnson S (2019) 'What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?'

Presentation of compliance information at point of sale: Retailers had a low level of awareness of whether there would be any cost to them in obtaining, requesting, or storing information or assurances from producers about the compliance of products with the top 3 CoP guidelines. They suggested a wide range of methods for presenting product security information, including online, in technical specifications, in-store labels, brochures, and price tickets, with **estimates of one-off staff time costs averaging £4,781.** Two-thirds (67%) of respondents felt that they would not need to use external advice or consultancy.

Familiarisation: Manufacturers estimated that familiarisation with the legislation based on mandating aspects of the top three guidelines of the Code would require an average of 15.2 person-days, or a **cash equivalent of £2,779.** This varied from "a few hours for the chief product officer" to "over three months to ensure the entire business was aware of the legislation". The variation appeared to be a function both of the size of the businesses and their present level of readiness.

For the product labelling option, **manufacturers** estimated that 11.8 person days would be required on average for familiarisation. The overall **average estimate of familiarisation costs for a mandatory label was just £1,638. Retailers** believed that the familiarisation cost of a labelling scheme to them would be similarly low: **the estimated total was 8.1 person-days, costing £1,676.** In both cases, this is lower than the cost of familiarisation with the "top 3 guidelines" option.

Self-assessment: Manufacturers estimated that an average of 30.1 person days per year were required to undertake self-assessment of compliance of their consumer IoT products, as part of their self-declaration to retailers. More than half of this time would be the responsibility of IT professional or technical staff, with time also spent by IT/technical directors or specialist IT managers. **The cash equivalent of this time is estimated at £6,575 per company per year.**

Disposal of non-compliant stock: Manufacturers estimated the cost of disposal of non-compliant stock at between 0.5% and 1.6% of IoT turnover. Strategies for disposal varied, with some manufacturers favouring re-shipping to other jurisdictions, trying to sell all stock within a grace period, disposing to refuse or destroying products. **This is the single costliest element of the proposed legislative options, making the "top 3" option more costly than the "labelling" option.**

Retailers were not able to relate costs to their turnover without information on the grace period; unit costs for disposal ranged from £10-£50 per unit, or free of charge if this was provided for in their relationship with their supplier

Impact on UK trade and investment: Overall economic activity in the UK will remain minimally affected by the proposed measures in the short and medium term. UK imports and exports would both slightly decrease in response to the implementation of the policy measures; however, the impact on the UK economy would mostly be offset by an increase in UK production. The net impacts are very small. The highest relative impacts would likely result from the mandatory minimum period for security updates, which are costliest to implement for UK companies and foreign exporters. SMEs will be more affected than large companies, i.e. they will face higher compliance costs per unit, which may decrease their domestic and international competitiveness.

Other factors will likely have a greater impact on the affected industries over time, for example product innovation, domestic and international demand, and the development of domestic and international supply.

As concerns investment in the UK, investment is not expected to decrease as a result of the regulations, nor is a deterioration of the UK's investment climate expected due to proposed regulations.

Impact on consumer take-up: Concerns about the security of smart devices do appear to be a significant barrier to growth of the sector. Among consumers who said that they did not plan to purchase smart devices in the next 12 months, 28% said that they were concerned about the security of smart devices, and 30% were concerned about their privacy. It is notable that for consumers, independent assurance of standards was more commonly cited as a factor that would encourage purchasing of smart devices than manufacturer self-assessment.

CONTACTS

Jenny Irwin
Partner

Number One,
Lanyon Quay,
Belfast,
Northern Ireland,
BT1 3LG

T 02890 234343
jenny.irwin@rsmuk.com

Matt Rooke
Associate Director

2nd Floor, North Wing East,
City House,
Hills Road,
Cambridge,
CB2 1AB

T 01223 455715
matt.rooke@rsmuk.com

rsmuk.com

The UK group of companies and LLPs trading as RSM is a member of the RSM network. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm each of which practises in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction. The RSM network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 50 Cannon Street, London EC4N 6JJ. The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made.

Recommendations for improvements should be assessed by you for their full impact before they are implemented. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

This report is supplied on the understanding that it is solely for the use of the persons to whom it is addressed and for the purposes set out herein. Our work has been undertaken solely to prepare this report and state those matters that we have agreed to state to them. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM UK Consulting LLP for any purpose or in any context. Any party other than the Board which obtains access to this report or a copy and chooses to rely on this report (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM UK Consulting LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to our Client on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report. RSM UK Consulting LLP is a limited liability partnership registered in England and Wales no.OC397475 at 6th floor, 25 Farringdon Street, London EC4A 4AB