Department for
Digital, Culture
Media & Sport

Secure by Design: Improving the cyber security of consumer Internet of Things Report

Contents

Foreword

Margot James
Minister for Digital and Creative Industries

As we deliver our vision for the UK to be the safest place to live and do business online, it is critical that we make sure the internet works for everyone. That means, as Government and industry work together to ensure we protect the UK from cyber attacks, we must also reduce the burden on end users by embedding effective cyber security practices at every stage of a connected product's life cycle.

Increased connectivity via the internet of things ("IoT") provides fantastic opportunities for the UK. A key part of this Government's ambition is to expand on the aspirations set out in our Digital Strategy through enhancing our status as an international leader in the development and uptake of IoT. However, we must ensure that individuals are able to access and benefit from connected technologies safely, confident that adequate security and privacy measures are in place to protect their online activity. The recent Mirai and WannaCry attacks, which affected core public services and used internet connected devices to breach private companies, reinforce the need for effective cyber security as part of our digital economy.

I am delighted to be publishing this report, which advocates a fundamental shift in approach to moving the burden away from consumers having to secure their internet connected devices and instead ensure strong cyber security is built into consumer IoT products and associated services by design.

By publishing this report we are kicking off a process of broader engagement with our key partners both here, and internationally, to ensure that we meet this need for effective and proportionate cyber security.

I would like to place on record my sincere thanks to everyone who has informed the findings and recommendations within this report, with particular thanks to the members of our Expert Advisory Group.

As this report makes clear, we are publishing our recommendations in draft, with a clear ask of you as readers to provide the necessary feedback and input which will help us to strengthen the proposed measures to ensure that they meet the cyber security requirements of our increasingly digital society.

This report, and the continuing work which it sets in motion, is part of a broader programme of work under our Digital Charter, as set out in the Government's manifesto. Through the Charter we will agree norms and rules for the online world and put them into practice. In some cases this will be through shifting our expectations of behaviour; in others we may need new laws or regulations.

I do hope that you will continue to work collaboratively with us in support of our ambition to make the UK the safest place to live and do business online. I would like to thank you for your input now, and over the coming months.

Executive Summary

This Government's ambition is to make the UK the safest place in the world to be online, and the best place in the world to start and grow a digital business. This Review focuses on how we can ensure that consumer internet connected products and associated services are sufficiently secure. In particular, it looks at the rights and responsibilities of consumers and industry.

The Internet of Things (IoT) brings huge opportunities for citizens as well as the UK's digital economy. This includes increasing the functionality of many features in the home, such as remotely changing the level of heating and lighting. However, many internet-connected devices sold to consumers lack even basic cyber security provisions. This, paired with the rapid proliferation of these devices, has led primarily to two risks:

(1) consumer security, privacy and safety is being undermined by the vulnerability of individual devices; and

(2) the wider economy faces an increasing threat of large scale cyber attacks launched from large volumes of insecure IoT devices.

These risks need to be addressed through joint government and industry action as a matter of urgency. This is important because the Government has a duty of care to UK citizens to help ensure that they can access and use the internet safely. Consequently, the Government has undertaken this Review into the cyber security of consumer IoT products and associated services. This report sets out the need for greater action, and proposes a range of measures to better protect citizens and the wider economy.

The report notes that protecting consumers requires a fundamental shift in industry's approach to managing cyber risks. There is a need to move away from placing the burden on consumers to securely configure their devices and instead ensure that strong security is built in by design.

The central proposal of this report is a draft Code of Practice aimed primarily at manufacturers of consumer IoT products and associated services. It has been developed through extensive engagement with industry and subject matter experts and sets out thirteen practical steps to improve the cyber security of consumer IoT.

The publication of this report, and particularly the draft Code of Practice, is intended to stimulate further dialogue with industry, academic institutions and civil society over the coming months. The Government needs to collectively balance the need to

create effective incentives for manufacturers, the supply chain and retailers, while also continuing to encourage innovation in new technologies.

The Government's preference would be for the market to solve this problem - the clear security guidelines we set out will be expected by consumers and delivered by IoT producers. But if this does not happen, and quickly, then we will look to make these guidelines compulsory through law. We will review progress throughout 2018.

Further details on how to provide input into the Review, and the proposed recommendations outlined in this report, are provided in Chapter 7.

IoT security is a global challenge requiring global collaboration. The Government is working with our international partners and through international organisations to collectively take action to secure consumer IoT products and associated services at every stage of their lifecycle.

1. The Internet of Things (IoT) - new opportunities and risks for consumers

Benefits of the IoT

1.1. The growth of IoT has already brought significant economic and social benefits. As developments continue, it is expected that there will be further benefits for consumers and companies alike, for example: new and better products and services; companies using data to better anticipate and meet people's needs; companies providing useful, tailored information to inform consumers' decision making and features to save people time and money, for example on home energy and security.

1.2. Along with consumer connected products and services, the IoT is also being put to effective use across a range of industries, such as automating industrial manufacturing processes in industry, for example within the agriculture and automotive sectors. The IoT is also being utilised in the public sector, including health, social care, urban infrastructure and services and transport.

1.3. The growth of IoT markets is providing great opportunities for UK companies. In 2016, digital sectors contributed £116.5 billion to the UK economy - almost 7% of the UK's gross value added. Additionally, the export of digital sector services amounted to just over £32 billion in 2015.[1]

1.4. The number of internet connected devices in use continues to rise. Forecasts vary, but some suggest that there will be an estimated 20 billion internet connected devices worldwide by 2020.[2] Moreover, the UK household ownership of smart devices could rise from approximately ten, to fifteen devices per household by 2020.[3] The networks and data that flow from connected devices will also support an extraordinary range of applications and economic opportunities.[4] This expected increase in IoT devices emphasises the need for a proportionate and collaborative approach to securing consumer IoT to be

[1] DCMS Sectors Economic Estimates 2017: Employment and Trade, 16 August 2017. Accessed at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/640628/DCMS_Sectors_Economic_Estimates_2017_Employment_and_Trade.pdf

[2] Gartner report on scale of connected devices by 2020, accessed at: https://www.gartner.com/newsroom/id/3598917, 2017. This figure excludes smartphones, tablets, and computers.

[3] WRAP report 'Smart Devices and Secure Data Eradication', 2016, accessed at: http://www.wrap.org.uk/sites/files/wrap/Data%20Eradication%20report%20Defra.pdf (forecasts taken from 17 smart product categories)

[4] Government Office for Science, IoT report, 2014, accessed at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf

taken by the Government and industry, to protect consumers while continuing to support and foster innovation.[5]

Risks associated with consumer IoT

1.5. While the recent growth in IoT provides opportunities, it also brings risks. With one in ten adults now falling victim to cyber crime, it is clear that the uptake of connected products and services will only increase the attack surface.[6] Cyber criminals could exploit vulnerabilities in IoT devices and associated services to access, damage and destroy data and hardware or cause physical, or other types of harm. Where these vulnerabilities can be exploited at scale, impact could be felt by multiple victims across geographic boundaries.

1.6. This Review has been conducted primarily in light of two key risks associated with consumer IoT. Firstly, poorly secured IoT products and associated services threaten individuals' online security, privacy and safety. Secondly, devices with weak security can become part of large-scale cyber attacks, such as Distributed Denial of Service (DDoS) attacks. The impact of such attacks are predominantly felt by third parties and can reverberate across the wider UK, and indeed global, economy.

1.7. When security flaws of devices in the home are exploited, compromised services can cause significant problems. A device with a microphone or camera could be used to record individuals within their home, or information about their daily routine could be used without their knowledge, to exploit, harass or blackmail. Some IoT products designed for children have had security issues that left voice recordings and imagery, (that families believed were private), open to the public, or easily accessible for those wishing to access it.[7]

1.8. A compromised device connected to home heating or appliances may also cause safety risks - for example an attacker may be able to disable safety controls or deny usage, such as disrupting heating systems during winter. Alternatively, if smart locks or connected physical access control systems are compromised, criminals could get into homes without needing to force entry.[8]

1.9. The nature of the internet is such that any attack could be at a local, national or even international scale. If home routers are targeted, an attack could leave

[5] Definition of consumer IoT: *This includes consumer purchased 'off the shelf' IoT devices; IoT devices used and installed 'in the home' and the associated services linked to these devices.*
[6] Crime Survey of England and Wales for year ending June 2017, accessed at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/june2017
[7] BBC News report, Connected Toys cyber breach, 2017, accessed at: http://www.bbc.co.uk/news/technology-39115001
[8] Engadget report on flaws in bluetooth locks, 2016, accessed at: https://www.engadget.com/2016/08/10/researcher-finds-huge-security-flaws-in-bluetooth-locks/

many people without internet connectivity. If a vulnerability is found in a home assistant product, a breach in consumer privacy could be significantly more catastrophic - criminals could gain a live audio feed into large numbers of households.

1.10. Widespread attacks on IoT devices are not a theoretical concept – they have already happened. This is illustrated by the Mirai malware which was discovered in 2016 which targeted devices such as internet-enabled cameras (IP cameras) and other IoT products and ultimately disrupted the service of many news and media websites. These attacks were successful because the Mirai malware used common default credentials (such as a username and password being set by the manufacturer as 'admin') and poor configuration of devices. These weaknesses are frequently identified in IoT products. In the case of Mirai, compromised devices were grouped together as a network (known as a botnet), controlled by an attacker and used to launch DDoS attacks against other internet-connected devices and services.[9] The malware was used in several high-profile attacks, including against the French cloud computing company OVH, and internet services company Dyn – temporarily preventing users worldwide accessing popular platforms such as Netflix, GitHub, and Twitter.

1.11. Mirai provides an example of IoT devices being both specifically targeted and used for potential adverse end-goals by an attacker, such as causing wide-scale disruption to internet services worldwide. In October 2017 an evolution of Mirai, called Reaper,[10] was discovered which unlike Mirai uses publicly and easily available exploits.[11] Reaper highlights the weaknesses within the IoT industry around patching known security vulnerabilities, allowing attackers to utilise them to cause harm. Often patching has relied on manual intervention by a user - sometimes requiring an update file to be copied directly onto the device. Other cases have involved updates being delivered via insecure means with no guarantee of integrity - leaving the device open to attacks where a criminal could manipulate the download.

1.12. The security flaws utilised by both Mirai and Reaper are not the only ones that are commonly found in consumer IoT products. There have been several cases where security vulnerabilities have been found within the web service or mobile application that supports the product.

[9] (DDoS) Distributed Denial of Service – where many coordinated networked devices try to communicate with a target device at the same time, causing it to be significantly slower to respond or cease to function.
[10] Wired report on Reaper IOT botnet, 2017, accessed at: https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/
[11] Exploits: Software code or a mechanism that allows them to gain access to a device.

Rationale for Government & Industry Intervention

1.13. As part of this review, the Government explored current industry incentives and disincentives for implementing cyber security in consumer IoT. The Government's evidence suggests that the main disincentives centre around cost and the challenge of justifying investing time and money when a business's focus is to get their product to market as soon as possible. Additionally, manufacturers are unlikely to face immediate economic costs borne by a DDoS attack conducted through their devices, and, therefore, they do not face sufficient commercial incentive to invest in a secure by design approach.

1.14. Moreover, consumers are struggling to distinguish between good and bad security in devices on sale, primarily due to a lack of information about built-in device security. Additionally at present, consumers are not prioritising good security as a preference over other features included within a product. This further limits the incentives for manufacturers and suppliers to develop products with sufficient security built-in from the start.

1.15. The Government can help create the right incentives for industry to improve the security of consumer IoT products and associated services and so facilitate a shift in behaviour across supply chains. In light of the increasing risk of IoT-associated attacks, the Government will take the necessary steps to put these incentives in place.

2. Context of the Review

The cyber security context

2.1. The Government is developing a Digital Charter to respond to the opportunities and challenges brought about by new technologies. The Government is committed to making the UK the safest place to live and work online while also driving innovation and growth across the economy. Alongside this, there is a need to ensure that the right rules and frameworks are in place to govern our increasingly digital world.

2.2. To do this, the Government needs to develop a shared understanding of the rights and responsibilities of citizens and businesses alongside a programme of work to put them into practice. This will be a collaborative process between the Government, public, industry, academia and other like-minded countries to develop and implement a set of principles to guide our behaviour in the digital age. As an important piece of work linked to the Charter, this Review moves the conversation forward on the respective rights and responsibilities of consumers and manufacturers for consumer IoT products and associated services.

2.3. This work is being taken forward as part of the Government's National Cyber Security Strategy (2016-2021) which outlines the Government's cyber security ambition over a five year period.[12] A centrepiece of this strategy was the creation of the National Cyber Security Centre (NCSC) in 2016 as a single, central body for cyber security at a national level.[13] The NCSC, whose role includes protecting nationally critical services from cyber attacks, managing major incidents and providing advice to citizens and organisations, has contributed to this review and provided technical input into the draft Code of Practice.

2.4. This work builds on NCSC's existing technical guidance to industry, including a set of principles that describe a secure by default approach in the context of cyber security, published in May 2017.[14]

Supporting Government Activity

2.5. The conclusions and recommendations of this Review should not be looked at in isolation, but as part of a much broader set of activity across the Government. This includes encouraging innovation with the IoT and other digital

[12] UK National Cyber Security Strategy, 2016, accessed at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
[13] UK National Cyber Security Centre, accessed at: www.ncsc.gov.uk
[14] National Cyber Security Centre website on secure by default, 2017, accessed at: https://www.ncsc.gov.uk/articles/secure-default

technologies whilst ensuring that citizens and organisations can continue to safely and confidently embrace the opportunities that a thriving digital economy can bring. The following paragraphs outline the main supporting activities across the Government.

2.6. The Government's recent Industrial Strategy White Paper highlighted the importance of new technologies for innovation and productivity, and outlined the Government's commitment to respond to global challenges and opportunities.[15] The strategy focuses on boosting productivity across the UK, for example through raising UK investment in research and development.

2.7. The Government's Digital Strategy includes the aspiration for the UK to remain an international leader in the development and uptake of IoT.[16] The Government's actions include the funding of research and innovation in IoT, including through the three year £30 million IoT UK Programme.[17] This includes:

- The Cityverve smart cities demonstrator in Manchester, showing how IoT technologies and services can improve local services;
- NHS projects to help people with dementia in Surrey and people with diabetes in the West of England;
- Academic research by the PETRAS IoT Research Hub; and
- Work with a range of partners, including Catapult's where appropriate.

2.8. The Government's Smart Energy Team is working to remove barriers to a smart, flexible UK energy system, which includes smart appliances. The Government and Ofgem published the Smart Systems and Flexibility Plan in July 2017 which outlined a range of actions to achieve this.[18] The Government has commissioned work to assess the magnitude of the smart cyber security risk up to 2030, which includes consideration of the impact of increased use of IoT devices across the electricity system on the stability of the grid. This work is already informing the Government's work to address cyber security risks in a smart energy system, for example on technical standards for smart appliances.

2.9. This work to ensure that the UK embraces the opportunities connected technologies provide in a growing digital economy, sits side by side with work to protect consumers from the risks that arise from an increasingly online

[15] HM Government (2017), *Industrial Strategy: Building a Britain Fit for the Future*, accessed at https://www.gov.uk/government/publications/industrial-strategy-building-a-britain-fit-for-the-future
[16] HM Government (2017), *Government Digital Strategy,* accessed at: https://www.gov.uk/government/publications/uk-digital-strategy
[17] Internet of Things UK, 2017, accessed at: https://iotuk.org.uk/
[18] UK Government report 'upgrading our energy system', 2017, accessed at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/633442/upgrading-our-energy-system-july-2017.pdf

environment. Alongside this Review, and within the parameters of the work on the Digital Charter, the Government published the Internet Safety Strategy Green Paper in October 2017. This sets out the UK Government's ambition to tackle online harms, by not only working with technology companies, but also supporting users.[19] It details a number of activities to enhance online safety for users, including the use of technical solutions to reduce and prevent online harms. The Strategy sets out the Government's desire for technology companies and developers to 'think safety first' and build safety features into their products and platforms from the beginning.[20] Critical to getting the required shift in industry's approach to the security and safety of connected technologies will be taking a coherent and consistent approach to both safety and security at the design phase and indeed throughout the lifecycle of the product or service.

2.10. The UK's consumer protection regime is world-leading, and it is important that we remain at the forefront by reviewing current protections to ensure they keep pace with the technology now in use. The Review has considered how consumer protection structures and legislation can protect users from the threats posed by connected products and services. This is part of the Government's much broader review of consumer markets that will lead to the publication of a Consumer Green Paper.

2.11. Protecting the rights of individuals is also a key focus of the Government's existing data protection legislation. In September 2017, the Government introduced a Data Protection Bill in the House of Lords. The Bill will make the UK's data protection laws fit for a digital age, and apply the General Data Protection Regime in the UK. These new laws will provide a comprehensive and modern framework for data protection in the UK, with stronger sanctions for malpractice. Organisations that handle personal data will need to evaluate the risks of processing such data and implement appropriate measures to mitigate those risks. For many organisations, such measures will need to include effective cyber security controls.

[19]UK Government Internet Safety Strategy Green Paper, 2017, accessed at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/650949/Internet_Safety_Strategy_green_paper.pdf

[20]UK Government Internet Safety Strategy Green Paper, 2017, accessed at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/650949/Internet_Safety_Strategy_green_paper.pdf

3. Promoting a Secure by Design Approach to Consumer IoT Security

Process of conducting the Review

3.1. The Review commenced in early 2017. Over the course of the Review, the Government has sought input from a range of stakeholders, including industry, academia, consumer bodies, other Government departments and international governments. In support of a multi-stakeholder advisory approach, the Government set up an independently chaired Expert Advisory Group which included a wide range of external stakeholders, including industry representatives, to support the review by advising and commenting on proposals for further action.

3.2. The Review comprised of three key strands of work, focusing on:

- Understanding the burden currently placed on consumers (ie. the expected behaviours when buying, installing, maintaining and disposing of a consumer IoT product);
- Developing guidelines for a secure by design approach in the form of a Code of Practice; and
- Broader Government incentives and levers to gain traction with industry.

3.3. This report is intended as the start of a much more extensive dialogue with industry and partners, to ensure that any action taken balances the need to address current security concerns and preventing unnecessary stifling of IoT innovation and enterprise.

3.4. In addition to the establishment of an Expert Advisory Group and as part of the Government's broader engagement, we have drawn extensively on the resources of the PETRAS IoT Hub, funded out of the IoT UK programme.[21] Alongside this Review, the Government is publishing a literature review of industry recommendations for the Government and an overview of international activity on IoT security which was compiled by PETRAS.[22]

3.5. There will be an opportunity for stakeholders to submit views on the report's proposals (further details are outlined in Chapter 7). This feedback mechanism has been put in place to ensure that a wide variety of organisations and

[21] PETRAS IoT Research Hub, 2017, accessed at: https://www.petrashub.org/

[22] Summary literature review of industry recommendations for the Government and an overview of international activity on IoT security, PETRAS. Accessed at: www.gov.uk/government/publications/secure-by-design

interested parties are able to provide specific comments on the Review's findings.

Guiding Principles of the Review

3.6. Throughout the course of conducting the Review, the Government's approach and engagement with industry and key stakeholders has been informed by five key principles which we view as critical in informing future action by industry and the Government to improve the security of connected devices and services. Specific options for intervention, which are set out in subsequent chapters, have been designed with these principles in mind.

One: Reducing burden (on consumers and others in the supply chain)

3.7. Many consumers struggle to understand what is required of them, or conducted on their behalf, to keep their products secure. Currently there is a large amount of uncertainty because of a lack of information, varying advice on password strength and how often to change passwords, different expectations on what the user needs to do to keep their product up to date, and a lack of clarity on what data is being collected and what happens to it.

3.8. Uncertainty is not confined to consumers. Companies designing and assembling IoT products and solutions often find it difficult to obtain information about the security of the component parts they are intending to use.

3.9. Reducing the burden on consumers will likely require everyone in the supply chain to pay more attention to security. As part of building security into their components, products and services, companies should reduce the burden currently placed upon consumers, and consider how they might make it easier for others in the supply chain to also implement a secure by design approach.

Two: Transparency

3.10. Greater transparency is an essential part of a secure by design approach. Being open and explicit about security mechanisms that have been put in place to secure a product or service, allows for accountability and scrutiny, thereby enabling others in the supply chain to make informed choices.

3.11. Being transparent means explaining clearly to customers what security measures have been taken, which will reduce uncertainty and increase consumer confidence when purchasing products. This need for transparency extends to all stakeholders within the IoT production supply chain, which ensures shared accountability.

Three: Measurability

3.12. A secure by design approach should not just be about putting in place good security mechanisms, but also being able to measure the effectiveness of those mechanisms. It is difficult to consider individual security mechanisms in isolation. For example, decisions on access permissions for software have to be seen in the context of other security measures that have been put in place, for example multi-factor authentication (MFA) and Single Sign-On (SSO), and have implications for functionality of the products and services.

3.13. Even when the context is fully understood, it is difficult to analyse the incremental benefit of implementing an additional security feature. In order to avoid sacrificing essential security functions in favour of functionality requirements, clear metrics should be in place that enable the assessment of the effectiveness of security measures.

Four: Facilitating dialogue

3.14. Facilitating dialogue means maintaining effective communication between all parties across the supply chain and with consumers. It is important that companies in each sector seek to share best practice and known vulnerabilities, and, ultimately, avoid customer confusion. As different industry sectors develop their own approaches to security, underlying assumptions, models of how security is perceived, guidelines, codes of practice and regulations should all be shared widely.

3.15. A secure by design approach takes advantage of best practice in other sectors, enables effective communication across the supply chain and across sectors and establishes common approaches to what is expected from consumers.

Five: Resilience

3.16. A secure by design approach should further have provisions to increase the resilience of critical functions and services. This includes conducting business continuity planning, establishing a “fall-back framework” and undertaking regular risk assessments to anticipate and mitigate future problems.

3.17. Additionally, incident response procedures should be in place to ensure timely action if products or systems are compromised due to cyber attacks or accidental incidents. A clear incident response process, including plans, defined roles, training, communication and management, increases resilience by enabling organisations to quickly discover an attack, effectively containing any incurred damage, and restoring the integrity of networks and systems.

4. Code of Practice for Industry on Consumer IoT

4.1. The focus of the Review, in close collaboration with industry, has been the development of a 'Code of Practice' for those developing, operating and selling IoT services and solutions, including device manufacturers. The Code of Practice sets out practical steps to improve the cyber security of consumer IoT products and connected services. It brings together what is widely considered good practice and applies it to the area of consumer IoT in the form of thirteen guidelines. The Government is seeking input from industry and other key stakeholders to further refine the Code of Practice ahead of publication of a final version in Summer 2018.

4.2. The guidelines contained within the Code of Practice are not a silver bullet - only by shifting to a security mind-set and investing in a secure development lifecycle can an organisation succeed at creating secure IoT products and services. Put simply, companies should design products and services with security in mind, from product development through to the entire product lifecycle. Organisations should also regularly assess cyber security risks pertaining to their products and services and implement appropriate measures to address these.

4.3. It is important to note that a number of industry bodies and international fora are developing security recommendations and standards for IoT.[23] This Code of Practice is designed to be complementary to and supportive of those efforts, and relevant published cyber security standards.[24] The Code of Practice has been constructed directly with industry with the hope that any future trustmark scheme related to consumer IoT will align with the Code of Practice.

4.4. In 2018, following publication of the final Code of Practice, the Government will continue to work with industry, academia and civil society to produce supporting documentation to aid implementation. This will include a compliance framework which sets out the practical measures needed to adhere to the principles within the Code of Practice for every part of the product lifecycle.

[23] Summary literature review of industry recommendations for the Government and an overview of international activity on IoT security, PETRAS. Accessed at: www.gov.uk/government/publications/secure-by-design

[24] It is noted that there are specific definitions of the word "standard" in relation to what are termed "technical standards" (including legal definitions). For convenience this report uses the word standard in an everyday language sense to refer to descriptions of characteristics (largely of a technical nature for the IoT). Such technical standards may also be called specifications by their publishers.

4.5. As part of this work, the Government will consider how the uptake and impact of the Code of Practice can be measured once a final version has been published. The UK Government will also explore whether retailers can play a greater role in helping to reduce the burden on consumers. Additionally, in 2018 the Government will conduct work to map the finalised Code of Practice against the main standards on IoT security to help contextualise the Code for companies.

Proposed Code of Practice for Security in Consumer IoT Products and Associated Services

This Code of Practice is designed to improve the security of consumer IoT products and associated services. Many severe cyber security issues stem from poor security design and bad practice in products sold to consumers.

The guidance is listed in order of importance and the top three should be addressed as a matter of priority. An indication is given as to which stakeholder the responsibility primarily rests upon. These stakeholders are defined as:

Device Manufacturer: The entity that creates an assembled final internet-connected product. A final product may contain the products of many other different manufacturers.
IoT Service Providers: Companies that provide services such as networks, cloud storage and data transfer which are packaged as part of IoT solutions. Internet-connected devices may be offered as part of the service.
Mobile Application Developers: Entities that develop and provide applications which run on mobile devices. These are often offered as a way of interacting with devices as part of an IoT solution.
Retailers: The sellers of internet-connected products and associated services to consumers.

1) No default passwords
All IoT device passwords must be unique and not resettable to any universal factory default value.

Many IoT devices are being sold with universal default usernames and passwords (such as “admin, admin”) which are expected to be changed by the consumer. This has been the source of many security issues in IoT and the practice needs to be eliminated. Best practice on passwords and other authentication methods should be followed. Further details are available on the NCSC website.[25]

[25] National Cyber Security Centre, guidance, 2017, accessed at: https://www.ncsc.gov.uk/guidance

Primarily applies to: Device Manufacturers

2) Implement a vulnerability disclosure policy
All companies that provide internet-connected devices and services must provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues. Disclosed vulnerabilities should be acted on in a timely manner.

Knowing about a security vulnerability allows companies to respond. Companies should also continually monitor for, identify and rectify security vulnerabilities within their own products and services as part of the product security lifecycle. Reports of vulnerabilities can be sent to: security@ncsc.gov.uk. Companies are also encouraged to share information with competent industry bodies.[26]

Primarily applies to: Device Manufacturers, IoT Service Providers and Mobile Application Developers

3) Keep software updated
All software components in internet-connected devices should be securely updateable. *Updates must be timely and not impact on the functioning of the device*. *An end-of-life policy must be published for end-point devices which explicitly states the minimum length of time for which a device will receive software updates and the reasons why. The need for each update should be made clear to consumers and an update should be easy to implement. For constrained devices that cannot physically be updated, the product should be isolatable and replaceable.*

Software updates should be provided after the sale of a device and pushed to devices for a period appropriate to the device. This period of software update support must be made clear to a consumer when purchasing the product. For constrained devices with no possibility of a software update, the conditions for and period of replacement support should be clear.

Primarily applies to: Device Manufacturers, IoT Service Providers and Mobile Application Developers

4) Securely store credentials and security-sensitive data
Any credentials must be stored securely within services and on devices. Hard-coded credentials in device software are not acceptable.

[26] Competent industry bodies include the GSMA and the IoT Security Foundation. Guidance on Coordinated Vulnerability Disclosure is available from the IoT Security Foundation which references the ISO/IEC 29147 standard on vulnerability disclosure. The GSMA's industry level Coordinated Vulnerability Disclosure programme is located at: https://www.gsma.com/cvd.

Reverse engineering of devices and applications can easily discover credentials such as hard-coded usernames and passwords in software. Simple obfuscation methods also used to obscure or encrypt this hard-coded information can be trivially broken. Security-sensitive data that should be stored securely includes, for example, cryptographic keys and initialisation vectors. Secure, trusted storage mechanisms should be used such as those provided by a Trusted Execution Environment and associated trusted, secure storage. Stored credentials in services should follow best practices.[27]

Primarily applies to: Device Manufacturers, IoT Service Providers, Mobile Application Developers

5) Communicate securely
Security-sensitive data, including any remote management and control, should be encrypted when transiting the internet, appropriate to the properties of the technology and usage. *All keys should be managed securely.*

The use of open, peer-reviewed internet standards is strongly encouraged.

Primarily applies to: Device Manufacturers, IoT Service Providers, Mobile Application Developers

6) Minimise exposed attack surfaces
All devices and services should operate on the "principle of least privilege"; unused ports must be closed, hardware should not unnecessarily expose access, services should not be available if they are not used and code should be minimised to the functionality necessary for the service to operate. Software should run with appropriate privileges, taking account of both security and functionality.

The principle of least privilege is a foundation stone of good security engineering, applicable to IoT as much as in any other field of application.

Primarily applies to: Device Manufacturers, IoT Service Providers

7) Ensure software integrity
Software on IoT devices must be verified using secure boot mechanisms. If an unauthorised change is detected, the device should alert the consumer/administrator to an issue and should not connect to wider networks than those necessary to perform the alerting function.

[27] NIST Special Publication 800-63B: Digital Identity Guidelines, Authentication and Lifecycle Management, 2017. Accessed at: https://pages.nist.gov/800-63-3/sp800-63b.html#sec5

Primarily applies to: Device Manufacturers

8) Ensure that personal data is protected
Where devices and/or services process personal data, they should do so in accordance with data protection law. Device manufacturers and IoT service providers must provide consumers with clear and transparent information about how their data is being used, by whom, and for what purposes, for each device and service. This also applies to any third parties that may be involved (including advertisers). Where personal data is processed on the basis of consumers' consent, this must be validly and lawfully obtained, with those consumers being given the opportunity to withdraw it at any time. Consumers should also be provided with guidance on how to securely set up their device, as well as how they may eventually securely dispose of it.

This ensures that IoT manufacturers, service providers and application developers adhere to data protection obligations when developing products and services; that personal data is processed in accordance with data protection law; that users are assisted in assuring that the data processing operations of their products are consistent and that they are functioning as specified; and that users are provided with means to preserve their privacy by configuring device and service functionality appropriately.

Primarily applies to: Device Manufacturers, IoT Service Providers, Mobile Application Developers, Retailers

9) Make systems resilient to outages
Resilience must be built in to IoT services where required by the usage or other relying systems, such that the IoT services remain operating and functional.

IoT systems and devices are relied upon by consumers for increasingly important use cases that may be safety relevant or life-impacting. This may include building redundancy into services as well as mitigations against DDoS attacks.

Primarily applies to: Device Manufacturers, IoT Service Providers

10) Monitor system telemetry data
If collected, all telemetry such as usage and measurement data from IoT devices and services should be monitored for security anomalies within it.

Any unusual circumstances can be identified early and dealt with, minimising security risk and allowing quick mitigation of problems that do emerge.

Primarily applies to: IoT Service Providers

11) Make it easy for consumers to delete personal data
Devices and services should be configured such that personal data can easily be removed when there is a transfer of ownership, when the consumer wishes to delete it and/or when the consumer wishes to dispose of the device. Consumers should be given clear instructions on how to delete their personal data.

Primarily applies to: Device Manufacturers, IoT Service Providers, Mobile Application Developers

12) Make installation and maintenance of devices easy
Installation and maintenance of IoT devices should employ minimal steps and should follow security best practice on usability.

This is in order to prevent security issues caused by consumer confusion or misconfiguration, sometimes caused by complexity and poor or unclear design in user interfaces.

Primarily applies to: Device Manufacturers, IoT Service Providers, Mobile Application Developers

13) Validate input data
Data input via user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices must be validated.

This ensures that systems are not easily subverted by incorrectly formatted data or code.

Primarily Applies to: Device Manufacturers, IoT Service Providers, Mobile Application Developers

Code of Practice: Additional explanatory notes on specific guidelines

4.6. *How should the Code of Practice be read?* The Code of Practice is written in priority order, with an indication provided as to which parties each guideline primarily applies to. The first three guidelines are of particular importance because action in these areas will bring about the largest improvement in security in the short term. The term “consumer” is used throughout for consistency; consumers can generally be considered the end users of IoT products and services.

4.7. *Guideline 1 on default passwords:* Whilst much work has been done to eliminate reliance on passwords and providing alternative methods of authenticating users and systems, some IoT products are still being brought to market with default usernames and passwords from user interfaces through to network protocols. This is not an acceptable practice and it should be discontinued.

4.8. *Guideline 2 on a Coordinated Vulnerability Disclosure (CVD):* CVD is now standardised by the International Organization for Standardization (ISO), is simple to implement and has been proven to be successful in some large software companies around the world.[28] CVD is however still not established in the IoT industry and some companies may be reticent about dealing with security researchers. CVD provides a way for security researchers to contact companies to inform them of security issues putting the company ahead of the threat of malicious exploitation and giving them an opportunity to resolve vulnerabilities in advance of a public disclosure. Additionally, companies that share this information through industry bodies can assist others who may be suffering from the same problem.

4.9. Disclosures may require different approaches depending on the circumstances:

- Vulnerabilities related to single products or services: the problem should be reported directly to the affected stakeholder (e.g. Device Manufacturer, IoT Service Provider or Mobile Application Developer). The source of these reports may be security researchers or industry peers. It is also possible to report an issue directly to the NCSC.
- Systemic vulnerabilities: It may be the case that a stakeholder, such as a Device Manufacturer, discovers a problem that is potentially systemic. Whilst fixing it in the Device Manufacturer's own product is crucial, there is significant benefit to industry and consumers from sharing this information and to work with the NCSC and / or a relevant competent industry body to coordinate a wider scale response. Similarly security researchers may also seek to report such systemic vulnerabilities via the same approach.

4.10. *Guideline 3 on software updates:* Software security updates are one of the most important things a company can do to protect its customers and the wider technical ecosystem. Vulnerabilities often stem from software components that are not considered to be security related. Therefore as a general principle, all software should be kept updated and well maintained. Fixes can be pushed out

[28] International Organisation for Standardisation, Vulnerability Disclosure, accessed at: https://www.iso.org/standard/45170.html

to devices in a preventative manner, often as part of automatic updates, which can remove security vulnerabilities before it is exploited. Managing this can be complex, especially if there are cloud updates, device updates and other service updates to deal with, therefore a clear management and deployment plan is essential, as is transparency to consumers about the current state of update support.

4.11. In many cases publishing software updates will involve multiple dependencies on other organisations such as manufacturers of sub-components. This is not a reason to withhold updates - the aim of the Code of Practice is to instigate positive security change throughout the entire software supply chain. There are also some situations where devices cannot be patched. Some ultra-constrained devices will fit in this category and for these a replacement plan needs to be in place which should be clearly communicated to the consumer. This plan should detail a schedule for when technologies will need to be replaced and, where applicable, when support for hardware and software ends.

4.12. It may be critical for consumers that a device continues to function. This is why an update should “not impact the functioning of a device”. Devices should not turn completely off in the case of an update; there should be some minimal system functional capability, for example maintaining the operation of a heating system or a burglar alarm.

4.13. *Guideline 7 on software integrity: what does the ‘administrator’ mean?* If an IoT device detects something unusual has happened with its software, it needs to be able to inform the right person. In some cases, devices may have the ability to be in administration mode - for example, there may be a user mode for a thermostat in a room that prevents other settings being changed. In these cases, an alert to the administrator is appropriate as that person has the ability to act on the alert.

4.14. *Guideline 9 on resilience: what is meant by life-impacting?* The aim is to ensure that IoT services are kept up and running as the adoption of IoT devices across all aspects of a consumer's life increases. The impact on people’s lives could be prevalent if for example, an internet connection is lost to a connected door and someone is locked outside. Another example is a home heating system that turns off because of a DDoS attack against a cloud service. It is important to note that other safety-related regulations may apply, but the key is to avoid making outages the cause of these problems and to design products and services ready for these challenges.

5. Supporting Actions by the Government and Industry

5.1. Mainstreaming cyber security into the design, development and deployment of consumer IoT devices and associated services requires a broad set of government and industry interventions. This chapter outlines proposed measures in support of the Code of Practice that the Government will take forward throughout 2018. A longer list of additional measures under consideration are outlined in Annex B.

Consumer information and enablement

5.2. Currently, there are high expectations placed on consumers to proactively protect their devices and their privacy. These expectations include changing default passwords, updating devices and “opting out” of sharing their personal information. This causes excessive consumer burden and can lead consumers to disregard security in favour of convenience. Additionally at present, consumers have limited access to clear and relevant information to enable them to make informed purchasing decisions.

5.3. The Government’s aim is to ensure that consumers have access to sufficient information on the security of IoT products to make informed purchasing decisions and that manufacturers put in place the necessary conditions for consumers to securely use their devices. As part of achieving this, the Government proposes that:

- The packaging and information provided with any device should use clear language, particularly around guidance on installation and maintenance of devices.
- Consumers should be provided with sufficient information regarding the context in which the device has been designed for use, so that their behavioural responses and interactions with devices enhance rather than reduce the security of the device.
- Device manufacturers should follow the NCSC Secure by Default paradigm to ensure security is built in while facilitating usable security best practices.[29]
- Additionally, there is a clear role for manufacturers and providers of consumer IoT products in educating the rest of the value chain (such as app developers, firmware producers and consumers).

[29] Secure by Default Platforms, NCSC, 22nd September 2016. Accessed at: https://www.ncsc.gov.uk/articles/secure-default-platforms

5.4. These recommendations would significantly improve the relationship between companies and their customers and the broader climate for helping consumers to make informed decisions when buying consumer IoT products. It is important to note that these changes should not offset the need for consumers to keep aware and be considerate of their personal cyber security.

Voluntary labelling scheme

5.5. A proposal currently under development as part of the Review is a voluntary labelling scheme for consumer IoT products to aid consumer purchasing decisions and to facilitate consumer trust in companies.

5.6. A labelling scheme offers advantages to consumers, manufacturers and retailers. It provides consumers with basic yet essential information on IoT products to help them make informed purchasing decisions. This can be facilitated by retailers which will in turn help boost consumer trust with retailers and manufacturers. Additionally, retailers will be able to select products with security features when deciding what should be available for consumers to buy. Manufacturers can use labels to demonstrate their commitment to protecting consumers' privacy, safety and data and, in doing so, the label can act as a market differentiator. Labels can also provide an opportunity for industry to champion good practice in IoT security.

5.7. Currently, consumers are concerned about the security and privacy of their internet connected products which is an inhibiting factor in the adoption of IoT. It is widely understood that many consumers want greater transparency from manufacturers and control over how organisation collect, use and share their data.[30] Research has shown that a lack of transparency impacts on consumer trust in organisations and that consumers would trust organisations more if they were transparent about their data collection practices.[31]

5.8. Through specific engagements and workshops with industry, consumer bodies and academia, as well as via a survey with consumers, the Government has identified that there are a number of areas where consumers could benefit from information within a product label, such as:

- Stating that the product is internet connected
- Stating the product's minimum support period

[30] Gigya. (2014). 2014 state of consumer privacy and personalization. Retrieved from http://info.gigya.com/rs/gigya/images/Gigya_2014_State_of_Consumer_Privacy_and_Personalization_032015_US_F_WEB.pdf

[31] Walker, K.L. (2016). Surrendering information through the looking glass: transparency, trust, and protection. Journal of Public Policy & Marketing, 35 (1), 144-158.

- Providing consistent and transparent privacy-related information (e.g. type of personal data collected, whether it's shared with third parties and if users can opt out of sharing)

5.9. Further development of a labelling scheme will be undertaken in collaboration with academic researchers from the PETRAS IoT Research Hub - Consumer Security Index Project.[32] It will be open to further public and industry consultation. As part of this work, the Government will consider the areas listed above alongside how we could convey security language within a labelling scheme. We will seek to align our work with existing industry and international efforts where possible. Before adopting a labelling scheme, the Government will engage widely with stakeholders to explore how any labelling scheme could monitored and responsibly used.

Information sharing and guidance

5.10. Consumer organisations, such as Which?, are increasingly reviewing the security of consumer IoT and highlighting good and bad practice. Over the coming months, the Government will seek to support the efforts of these consumer-facing organisations, promoting the Code of Practice as a means of differentiating those products with strong security measures throughout the lifecycle of the device.

5.11. Consumers need clear, consistent and accessible advice at the point of product purchase, during set-up, maintenance and ultimately, disposal. The UK benefits from consumer associations that champion and advocate for greater IoT security and consumer rights. For example in 2018, Which? will be expanding their consumer facing work to help consumers identify secure products and inferior products with poor inbuilt security. The Government will seek to align messages and advice provided by Government departments, industry and from independent public-facing organisations. The Government will seek to establish a working group with consumer associations, the Information Commissioner's Office, industry representatives and academics to develop consistent guidance for consumers.

5.12. The Information Commissioner's Office has recently published guidance for consumers who are considering buying IoT products. This guidance will help

[32] The Consumer Security Index (CSI) project aims to develop a CSI for consumer IoT devices to aid consumer decision making and encourage its use to incentivise manufacturers to improve IoT device security. The index will be co-designed with consumers, manufacturers and retailers. Further information about the project is available at: https://www.petrashub.org/portfolio-item/developing-a-consumer-security-index-for-domestic-iot-devices-csi/

raise awareness among consumers on the main actions that they should consider when buying, installing and maintaining IoT devices.[33]

5.13. The Government also recognise that the effectiveness of cyber security messages differ depending on the target group. The Government will be working with the EPSRC project 'Cyber Security Across the LifeSpan' (cSALSA) which is exploring how cyber security is understood and talked about across the lifespan (e.g. across young children, working age population, and older adults). The findings from this project will help the Government to design more effective cyber security advice and educational materials that are tailored for different audiences.

5.14. Preliminary work was conducted to explore the barriers and advantages people see arising as a result of the expansion of the Internet of Things. The UK Government will seek to gain a deeper understanding of how underserved communities interact with the Internet of Things and will ensure that future work on supportive measures take their needs into consideration.[34]

Training and professional development

5.15. The UK faces a significant shortage of skills to meet the cyber security needs of citizens and businesses. This extends to IoT where technology has evolved so rapidly that professionals in hardware and software development have had little opportunity to gain the skills needed to protect IoT products and services from increasingly complex cyber security threats.

5.16. As part of its wider strategic approach to tackle the cyber skills shortage, the Government will conduct work to explore avenues for including cyber security within further education and university courses - and in professional development programmes - for the future generation of IoT developers. IoT has already been a key area of learning for students and teachers attending the Government's CyberFirst summer courses.[35]

5.17. The Government must also ensure that experienced professionals who develop, install and maintain IoT products possess an appropriate cyber security skill-set. We are working jointly with professional bodies to include

[33] Wood, S. (Deputy Commissioner (Policy) 'The 12 ways that Christmas shoppers can keep children and data safe when buying smart toys and devices', 24 November 2017. Access at: https://iconewsblog.org.uk/2017/11/23/the-12-ways-that-christmas-shoppers-can-keep-children-and-data-safe-when-buying-smart-toys-and-devices/

[34] Heath, C. P. and Coles-Kemp, L. 'The Internet of Things: Creating the necessary conditions for secure by default', Information Security Group, Royal Holloway, University of London, 2017.

[35] CyberFirst Courses, NCSC, 2017, accessed at: https://www.ncsc.gov.uk/information/cyberfirst-courses

cyber security in professional accreditation schemes and make it an integral part of continual professional development.

5.18. The Government is working with Trustmark (a Government endorsed scheme to marginalise unscrupulous traders undertaking repair, maintenance and improvement works in and around the home) to create online training and provide guidance to local tradesman and installers on IoT security.

Regulatory Options

5.19. As part of the Review, the Government has begun exploring where we can further leverage existing legislative measures to place selected guidelines from the Code of Practice on a regulatory footing. Parts of the Code of Practice (guideline 8) are already legally enforceable based on the legal requirements set out in the Data Protection Bill. The Government will continue this work throughout 2018 in consultation with stakeholders, such as industry and consumer organisations.

5.20. The Government is also monitoring regulatory action taken by other countries, such as Germany, who recently banned several children's smart watches.[36] This will help to ensure that the UK's approach to improving the cyber security of consumer IoT is taken in conjunction with efforts by our international partners.

Consumer Protection and Product Safety Legislation

5.21. The Government will, in due course, publish a green paper that will closely examine markets, especially those which are not working fairly for consumers, and is prepared to act where necessary. The Consumer Green Paper will look across industries, covering energy and other utilities as well, in order to consider whether the existing regulatory arrangements are sufficient. DCMS have been closely engaged in the development of the Government's Consumer Green Paper which will note the impact of the IoT within a consumer setting.

5.22. The fast pace of technological development and innovation in relation to IoT and web-enabled appliances pose specific challenges. The Government recognises that ongoing work is needed to better understand how the safety of products and consumer rights would be affected by IoT to ensure we maintain high levels of consumer protection and safety.

[36] Germany bans children's smartwatches, 17 November 2017. accessed at: http://www.bbc.co.uk/news/technology-42030109

Protecting citizens' data through the Data Protection Bill

5.23. Organisations supplying IoT products and services that collect and process personal data will be subject to the requirements of the Data Protection Bill which is currently going through Parliament. They will need to consider data protection requirements carefully and take steps to address the risks posed to individuals' privacy.

5.24. The supply chains of IoT products and associated services can be complex, with many different organisations involved, including manufacturers, software and application developers, hardware and data centre providers, retailers, and data aggregation platform providers. With specific reference to security and data protection, IoT manufacturers in particular need to be mindful of:

- Providing clear and transparent information to consumers about what personal data devices and services process, the organisations that process this data, and the lawful basis on which the processing takes place.
- Building privacy and security into the product lifecycle from the design phase, and ensure these are continued throughout.
- Ensuring that appropriate technical and organisational measures are in place to protect any personal data, including processes to ensure the confidentiality, integrity, availability and resilience of processing systems and services, and regular testing to ensure the effectiveness of such measures. Organisations can consider such requirements as part of a Data Protection Impact Assessment (DPIA) where it is appropriate to do so.

5.25. The Information Commissioner's Office is the UK's data protection regulator, providing advice and guidance to organisations and consumers and, where necessary, undertaking appropriate and proportionate enforcement action. The Information Commissioner's Office has published guidance for consumers on the security and privacy features of devices.[37][38] The Information Commissioner's Office will be producing further guidance on the data protection aspects of IoT in due course. The Government will continue to collaborate with the Information Commissioner's Office on producing simplified guidance for citizens on consumer IoT security to ensure consistency of messaging to all audiences.

[37] ICO Consumer Devices Guidance, accessed at: https://ico.org.uk/for-the-public/online/consumer-devices/

[38] ICO Blog, Accessed at: https://iconewsblog.org.uk/2016/07/15/public-must-act-to-protect-themselves-when-using-internet-of-things-devices/

6. Building an International Consensus

6.1. The development of internet connected products and associated services often involves an extensive international supply chain. Additionally, the impact of security flaws in these connected products and services are not confined to domestic boundaries. The Government recognises that, to be truly effective, work to improve IoT security cannot be taken forward in isolation. IoT security is a global challenge and requires industry, academia, civil society and governments across the world to find and implement solutions to address security concerns.

6.2. As part of this Review, and as part of the UK's broader National Cyber Security Strategy, the Government's focus has been on leading and influencing discussions on the global stage to, as far as possible, align standards, guidance and practical measures intended to improve IoT security. This activity has formed part of the Government's broader efforts for creating a free, open, peaceful and secure cyberspace. This work is also being conducted with the ambition to initiate fundamental and lasting improvement to the security of connected products and services on the market, and to positively impact on the growth of a global digital economy.

6.3. The Government's participation in relevant international fora includes extensive work within global standards bodies to highlight existing activity and to maintain awareness of the broader standards landscape. The discussions in these standard setting fora are predominantly led by industry or multi stakeholder bodies including governments and complement the more policy-focussed discussions underway with both other governments and international organisations.

6.4. A literature review of industry recommendations and international developments on IoT security is published alongside this report.[39] The Government is committed to establishing sustained and consistent engagement with international partners to develop a shared approach and an implementation plan to improve IoT security.

6.5. This engagement has been particularly important in light of the recent publication of the European Commission's European Cyber Security Strategy.[40]

[39] Summary literature review of industry recommendations for the Government and an overview of international activity on IoT security, PETRAS. Accessed at: www.gov.uk/government/publications/secure-by-design

[40] Proposal for a Regulation on ENISA, the "EU Cybersecurity Agency", and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"). Access at:

The Strategy sets out a number of strategic objectives and actions to increase the EU's resilience and preparedness, including a regulatory proposal for a pan-European cyber security certification framework. While it remains a member of the EU, the UK Government will continue to engage in negotiations relating to the regulatory proposals included, alongside other Member States. Cyber security is a global issue and it is important that we continue to work with European and other international partners to shape the global evolution of cyberspace and enhance our collective security.

http://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF

7. Conclusion

7.1. This report is the culmination of over twelve months of engagement with industry, academia, civil society more broadly, and international partners. It is intended as an interim update on an ongoing programme of activities to effect fundamental, long lasting behaviour change across industry and consumers to address the most commonly identified security vulnerabilities in consumer IoT.

7.2. Alongside a much broader set of activities in support of the emerging Digital Charter, this Review is intended to support both the UK's ambition to be a world-leading cyber security authority, and a prosperous and thriving digital economy.

7.3. Achieving this ambition requires close and sustained collaboration across industry and governments, both within the UK and internationally. As the Government's thinking evolves and as measures are implemented that are aimed at protecting consumers' privacy and safety, as well as securing the UK's digital future, the Government would like to open up this Review for comment and input.

7.4. The Government would specifically welcome comments on the draft Code of Practice included in Chapter 4, and suggestions for further areas of supporting activity beyond those outlined in Chapter 5 and in Annex B. Please send your comments to securebydesign@culture.gov.uk by the 25th April 2018. You can also submit written comments to the *Cyber Security Team, Department for Digital, Culture, Media and Sport, Level 4, 100 Parliament Street, Westminster, London, SW1A 2BQ.* The Government will also be seeking input through engagements with stakeholders over the coming months as we further develop our recommendations and support ongoing efforts across industry and on the global stage.

8. Annex A: Glossary of Terms

8.1. **Secure by Design:** A design-stage focus on ensuring that security is in-built within consumer IoT products and connected services.

8.2. **Internet of Things (IoT):** The totality of devices, vehicles, buildings and other items embedded with electronics, software and sensors that communicate and exchange data over the Internet.

8.3. **Consumer IoT:** This includes consumer purchased ‘off the shelf’ IoT devices; IoT devices used and installed ‘in the home’ and the associated services linked to these devices.

8.4. **Internet connected services:** Allowing devices to communicate with other devices over a broad network. These connections usually involve a link occurring between devices and systems and the collection of data.

8.5. **Distributed Denial of Service (DDoS) attacks:** Where many networked devices try to communicate with another at the same time, causing the targeted device to be significantly slower to respond or cease to function.

8.6. **Botnet:** Compromised devices that are grouped together as a network.

8.7. **Ransomware:** Malware that denies access to files or devices until a ransom is paid.

8.8. **Exploits:** Software code or a mechanism that allows unauthorised access to a device.

9. Annex B: Options Analysis Summary

A number of interventions were considered in support of the Review's objectives. These proposals were wide-ranging and represented ideas from a range of stakeholders, comprised of a mix of Government officials, industry experts, consumer associations and academics. The options were considered against a set of criteria including effectiveness, cost, barriers to implementation, consistency with international approaches and equity and impact (on consumers and industry). A number of options have been outlined below which will be considered further as part of the work that will be conducted in 2018.

Measure	**Conclusions**
Regulation	
Consider how to regulate to require terms and conditions for consumer IoT products to be written clearly and succinctly	The current terms and conditions provided with consumer IoT products are wordy and use language that is hard for consumers to understand. Consequently, most consumers choose not to read them. Additionally, the information that is provided with products whether that is on the maintenance, installation or use of the product is also difficult to comprehend. During the review, deep dive work was conducted to understand what barriers were faced by consumers when buying specific IoT products. To address these issues, the Government conducted a survey of consumers from diverse age groups to understand what information consumers felt was required to come with devices. Given a key market failure appears to be a lack of accessible information for consumers, the Government has focused its initial work on a voluntary labelling scheme as outlined in Chapter 5. However the issue of inconsistent and opaque language within products and services' terms and conditions remains under consideration.
Standards and Guidance	
Create specific guidance on vendor due diligence	During discussions with industry and other stakeholders, several parties noted there was a growing reliance by UK and European companies to have an extensive global supply chain to keep costs down for making consumer IoT products. As a result of this, companies could not always guarantee that third party companies had sufficient cyber

	security defence systems or had adequately factored security into the design, manufacture, deployment and disposal of devices. As we progress the Review, we will consider how we can use the Code of Practice, and the proposed accompanying compliance frameworks, to supply organisations with the necessary confidence to engage with suppliers regarding the cyber security of their goods and services.
Guidance on recycling, reuse and disposal of Consumer IoT products	Consumer IoT devices can store potentially sensitive information about users and the secure disposal of these devices is important to prevent unauthorised access. Consumers may hold onto devices that can't be wiped or securely disposed. The Government is looking at opportunities to align with other departmental activity to feed into the work that is underway on existing recycling and reuse services and initiatives for electronic equipment and e-waste. The Waste Electrical and Electronic Equipment Regulations place financial responsibilities on producers of equipment to ensure proper collection, and recovery of unwanted items. WRAP (Waste Resources Action Programme) is currently updating good practice guidance on the collection of waste electricals.
Retailer checklist for buying consumer internet connected products	UK retailers have a key role to play in advocating for a secure by design approach for consumer IoT devices because of their interaction with both IoT manufacturers and consumers. As part of this Review, the Government is considering how best to support retailers with selecting and buying secure IoT stock to sell in store.
Potential opportunity to work with the Engineering Council	DCMS are currently exploring with the Engineering Council if, when it is next reviewed, its guidance on security could be expanded to include some text that relates to IoT security and the interaction that engineers/technicians will have with internet connected devices.
Communication/Marketing	
Behaviour Change Campaign	The uptake and use of consumer IoT products and connected services is currently quite limited. As a result, it is too early to identify the common barriers to adopting secure practices in relation to connected products and services. Behaviour change is in itself difficult to achieve. During the

	review, PETRAS assisted the Government with research to analyse the perceived barriers felt by consumers towards connected products and associated services. This work indicated that behaviour change campaigns or awareness campaigns can have a limited impact on consumer behaviour without understanding what behaviours one wants to change. Additionally, some of the current identified behavioural barriers have arisen because of the vulnerabilities that exists within consumer IoT products and associated services. Therefore the Government concluded it would be more useful to address the issues at root cause and reduce burden on consumers through advocating a secure by design approach outlined in the Code of Practice and other supporting measures.
Cyber / IoT Insurance Products	The Government is working closely with the insurance industry through existing channels of dialogue, such as the Cyber Insurance Forum, to discuss how the evolving cyber insurance market might impact and support the adoption of improved security practices.