Internet-connected consumer devices can provide economic and social benefits. Weaknesses in the cyber security of these devices can undermine the privacy and safety of individual users, and can be used for large-scale cyber-attacks. This briefing looks at the cyber threats associated with consumer devices, their causes, and initiatives to improve device security and related challenges.

Background
An increasing number of consumer devices, including toys, TVs and washing machines, can be connected to networks such as the internet. Connected devices, together with the networks and services they connect to, are often referred to as the Internet of Things (IoT). Although forecasting the growth of the IoT is difficult, analysis firm Gartner suggests that over 13 billion (bn) connected devices could be in use by consumers globally by 2020. Connected consumer devices (Box 1) may offer consumers lower costs, greater convenience, and improved quality of life. McKinsey estimate that by 2025, consumer IoT systems could contribute $200-350 bn (roughly £155-270 bn) per year to the global economy via more efficient energy management, labour savings due to the automation of household chores, and the avoidance of injuries and deaths due to better home security. However, stakeholders have expressed concerns about the poor security of many devices.

Insecure devices can compromise consumers’ privacy and security or be hijacked and used to disrupt others’ use of the internet. In 2016, the UK Government committed £1.9 bn to cyber security over five years, as part of its National Cyber Security Strategy. This included an objective for most new online products and services to be cyber secure by default by 2021. In March 2018, the Department for Digital, Culture, Media and Sport (DCMS) proposed a voluntary Code of Practice for industry to ensure that devices are “secure by design”, with strong security built in, reducing the onus on consumers to securely configure their own devices. This code was published in October 2018.

Device Adoption
A 2018 survey of 3,750 consumers by Ofcom found that the most common connected devices in the UK include: Smartphones – used by 78% of respondents. Smart TVs – in 42% of households surveyed. Wearable devices – in 20% of households, including fitness trackers that monitor factors such as physical activity and location. Smart speakers – in 13% of households, which can react to voice commands and be used to control other devices. Other applications for connected devices include home monitoring systems (such as those for heating systems, lighting systems, burglar alarms and cameras) and smart appliances such as kettles and fridges. These can often be remotely monitored or controlled by users for greater convenience or security. A 2018 survey of 1,000 consumers by the trade body techUK found that ownership of these products is growing more slowly than for the most prevalent devices (above). Consumers most often cited cost as the main barrier to purchasing devices (41%), followed by privacy (21%) and cyber security concerns (16%).

Overview
- There is a growing UK market for internet-connected devices such as smart home appliances and home monitoring systems.
- The poor cyber security of these devices can lead to data loss, privacy infringements, risks to physical safety and security, and the widespread disruption of online services.
- A lack of economic incentives, fragmented industry standards, and some user behaviours contribute to poor cyber security.
- The UK Government has produced a voluntary Code of Practice for industry, which it may decide to enforce through regulation. It is also developing a labelling scheme to help inform consumers.
- Challenges include the complexity of supply chains, difficulties assessing security, and a shortage of cyber security expertise.
Cyber Threats for Consumer Devices

Security researchers and malicious attackers have demonstrated that many connected consumer devices are vulnerable to exploitation. Attackers may gain access to systems or sensitive data, which can lead to infringement of privacy, economic losses, and physical safety and security being put at risk. Individuals, companies and other network users may all be affected.

Cyber-attacks often use basic techniques, such as gaining access to a device by trying common or default usernames and passwords. Attacks can also exploit software vulnerabilities resulting from programming errors or insecure software design. Hardware may also be vulnerable. In 2018, hardware design flaws that could be exploited to gain unauthorised access to security-critical data were found in processors used in most personal computers and mobile devices, although there is little evidence to date of these hardware vulnerabilities being used maliciously.

Threats to Device Users

Cyber-attacks are one of the most common types of crime experienced by individuals in the UK according to national crime statistics, affecting an estimated 2.4% of adults in 2017 (Box 2). These include attacks on personal computers, as well as connected devices. Cyber-attacks typically involve the use of malicious software (or ‘malware’). Types of malware include ‘ransomware’, which encrypts files and demands a ransom for making them usable again, and ‘spyware’, which secretly monitors computer activity or provides access to unauthorised people.

Cyber-attacks on consumer devices can cause harm to individuals in different ways, potentially undermining their security, safety and privacy. For example, vulnerabilities in some connected locks may allow attackers to discover their physical location and unlock them without the consumer’s permission. Ransomware may be used to deny an individual access to physical assets and services, for instance by locking the screen through which a device is controlled. Such vulnerabilities have been reported for smart TVs and thermostats. Insecure connected devices can expose private data. For example, video and audio data may be accessed without permission from certain home security cameras, baby monitors, and toys. Connected devices also raise challenges for obtaining informed consent from users, who may not be fully aware of how their data are used, or may be unable to configure devices according to their privacy preferences.

Threats to Other Network Users

Insecure devices can expose a network, and all the devices on it, to potential attack. For example, some connected devices, such as doorbells and lightbulbs, can reveal unencrypted names and passwords for home Wi-Fi networks. Devices on a network may also be vulnerable to malware or unauthorised use if visitors connect their own devices to the network. Internet routers (used to connect the devices in a home or organisation to each other and the internet) can also be targeted directly. In October 2017, thousands of routers in homes and small businesses were infected with malware that has been attributed to Russian state-sponsored actors, according to the National Cyber Security Centre (the UK technical authority for cyber security). This potentially enabled the attackers to intercept or block data passing through the routers.

Cyber-attacks can affect networks on a national or international scale if many devices are exploited at once, for instance in a ‘botnet’ attack (Box 3). In 2016, ‘Mirai’ malware recruited hundreds of thousands of devices with common or default passwords for a distributed denial of service attack on the internet services company, Dyn. This temporarily blocked access to Twitter, Spotify and many other websites and services. Large-scale attacks may put critical national infrastructure at risk, including the provision of utilities and healthcare. Simulations suggest that a large-scale botnet attack on multiple smart homes might be used to manipulate the electricity demands of devices with high energy usage (e.g. heaters) causing power cuts.
Causes of Poor Cyber Security

A range of economic and technical drivers have contributed to the poor cyber security of many consumer devices. User behaviour is also an important factor for device security.

Economic Drivers

The UK Government’s 2018 Secure by Design Report concluded that manufacturers lack sufficient economic incentive to incorporate security features into devices.13 Bodies such as the EU Agency for Network and Information Security have raised concerns that producers place security below other priorities, such as performance, costs and time-to-market.45,69-73 A 2017 survey reported that over 40% of companies said their customers are either unwilling to pay a premium for security, or expect security costs to decline over time.74 Consumers may be unwilling to pay for attributes that they cannot measure, which might discourage investment in security features.75,76 Investment may be further disincentivised as, for some attacks (e.g. DDoS attacks, Box 3), the majority of economic costs may fall on third parties (such as online service providers) rather than device manufacturers or users.13 In addition, while retailers sometimes remove insecure devices from sale, many devices with known vulnerabilities remain on the market.77

Technical Drivers

Software flaws cannot be entirely avoided and some flaws will be vulnerable to exploitation.22,78,79 The US National Institute of Standards and Technology suggests that vulnerabilities are often difficult to discover and correct, and more should be done during software development to prevent, identify and mitigate them.90 Best practice guidelines recommend that device producers establish a vulnerability disclosure policy, including providing a public point of contact to which vulnerabilities can be reported when they are discovered, and a process for remediation.81-83 Such policies are not widely adopted.84 Firms routinely release security updates for devices such as laptops and smartphones to address known software vulnerabilities.85,86 Some updates are automatic, but many require users to install them. A 2016 survey of 2,000 connected device owners found that 40% had never knowingly updated their devices.87 A device may rely on pieces of software from multiple companies, each of which may need updating.88 Updates may be unavailable if the device is no longer supported by the software producer or cannot be updated (e.g. due to hardware constraints). Manufacturers do not always state whether updates will be issued for a particular device, or for how long this support will continue.89 In addition, if updates are not delivered securely, they may be imitated or hijacked by an attacker to compromise a device.90

Security may also be affected by the choice of hardware. Due to physical, technological or cost constraints, many small internet-connected devices have limited processing power, battery life, data storage, and capacity to transfer data.90,91 Such devices may have limited capacity for security features such as encryption and secure updates (unlike more sophisticated devices such as smartphones). Technological developments in device efficiency and software are addressing some of these limitations.92,93

User Behaviour

Consumer surveys by the cyber security industry report that poor cyber security practices are common.94,95 These include using default, weak, or reused passwords. Focus groups suggest that consumers may underestimate the risk and severity of cybercrime that targets devices and believe that security is not their responsibility.96 Users and security experts say that cyber security advice is often complex, inconsistent, or difficult to use.96,97 In addition, assessing the cyber security of a device and setting it up securely often requires technical knowledge not readily available to all consumers.13,98-100 The Government has also highlighted that consumers lack the information needed to assess security when buying devices, saying that cyber security should not rely on users and that devices should be designed to be secure and easy to manage.13,89,100

Approaches to Improving Cyber Security

Efforts to improve the cyber security of consumer products have focused on establishing good practice in industry, informing consumers, and developing the cyber security skills of consumers and those involved in producing and supplying devices (Box 4). Steps are also being taken internationally to address cyber security challenges (Box 5).

Establishing Good Practice in Industry

The international landscape of cyber security standards and guidance for connected devices is fragmented; almost 50 different organisations have published good practice principles.81,101,102 In 2018, DCMS consulted with industry and academia to produce the Code of Practice for Consumer IoT Security, which outlines good practices for the development, manufacturing and retail of connected consumer devices.14 The guidelines aim to encourage the integration of cyber security into products, reducing the burden on consumers to ensure that their devices are secure. The top three guidelines are:

- Eliminate non-unique default passwords
- Adopt a vulnerability disclosure policy (Technical Drivers)
- Make secure software updates available for an explicitly stated length of time.
Box 4: Developing Cyber Security Skills
There is a shortage of people with cyber security skills, and device producers may not always recognise the need to access such expertise. Accessing cyber security expertise may be particularly challenging for small manufacturers or those that focus on the primary function of a device (such as refrigeration or sensing). The Government is investing in training, research and other initiatives to develop the UK’s cyber security capabilities as part of the National Cyber Security Strategy. The Joint Committee on the National Security Strategy has welcomed these initiatives but concluded that efforts did not “match the scale of demand” for cyber security expertise. The Royal Academy of Engineering has recommended that skills development initiatives be expanded, with a focus on secure design and technical skills. It has also highlighted the role of schools in ensuring that future consumers are well informed. The Government published an Initial National Cyber Security Skills Strategy in December 2018.

Box 5: International Initiatives
The European Union
Under the proposed EU Cybersecurity Act, the EU Agency for Network and Information Security would establish an EU-wide voluntary certification framework for ICT products and services. The Act aims to address fragmented certification schemes across member states, and to increase trust and security in these products. The UK Government has said that it will continue to cooperate with EU cyber security bodies and share information on cyber threats. An agreement on the Act was reached in December 2018.

The Commonwealth
The 2018 Commonwealth Cyber Declaration committed member states to cooperate on cyber security and to promote security by default for connected devices.

DCMS is developing a global standard based on the Code of Practice through the European Telecommunications Standards Institute. The British Standards Institute is developing a commercial voluntary assurance scheme for compliance with the Code, as well as an independently-tested IoT Kitemark certification scheme for providers of internet-connected devices used in the home. Consumer groups have recommended mandatory minimum security standards for connected devices that pose a safety risk, and the ability for market surveillance authorities to withdraw insecure devices from the market.

Academic reviews have highlighted several potential gaps in UK product safety, liability and consumer rights laws that relate to the cyber security of consumer devices. In particular, it is unclear to what extent existing product safety and liability laws apply to faulty software, and digital services are excluded. In addition, the law requires that products are safe when they reach the market, but security levels of a device may change with time as new vulnerabilities and threats are identified. Consumer groups have said that users of connected devices should have the same right to redress as for other products. They have called for updated product safety legislation to ensure connected consumer devices do not pose a safety risk. A public consultation by the European Commission in 2017 found that about half of responses favoured revising product safety and liability laws in light of technological developments. An alternative to revising existing legislation is to pass new legislation: a 2018 California State law will require manufacturers of connected devices to provide “reasonable security features” from 2020, including a ban on default passwords.

The UK Government aims to legally enforce parts of the DCMS Code of Practice and is looking at the potential impacts of possible regulatory intervention. It also plans to introduce mandatory cyber security standards for appliances that automatically control their energy usage (e.g. internet-connected washing machines) under its plan to upgrade the UK electricity system. This is to address the risk of large-scale cyber-attacks destabilising the electricity grid, as well as cyber risks to individuals. The Government issued separate principles on the cyber security of connected and automated vehicles in 2017.

Informing Consumers
Guidance for consumers on setting up, managing and improving the security of household connected devices was published by the Home Office’s Cyber Aware campaign, alongside the DCMS Code of Practice. DCMS is also developing a consumer IoT security labelling scheme to help inform consumers’ purchasing decisions.

A Government-commissioned assessment of existing labelling schemes, including energy and food labels, concluded that a labelling scheme is likely to incentivise companies to compete on security as a form of market differentiation. However, it noted that more evidence is needed on how consumers would interpret and act on a cyber security label. Some industry stakeholders have reservations about a trust label as it is not clear who would carry out any certification and how cyber security can be measured. It is difficult to verify that a device is secure due to complex global supply chains and because devices produced by following best practice may still contain vulnerabilities. Vulnerabilities may be discovered once a device is on the market, after a label has been awarded. Some academics have suggested that labels should indicate when devices will no longer be supported, and that companies be obliged to address vulnerabilities discovered during this period.

Box 6: Vulnerabilities in Device Supply Chains
Companies involved in the production and distribution of connected devices include hardware manufacturers, cloud providers, and the developers of operating systems and third-party applications. Complex global supply chains provide many opportunities for vulnerabilities to be introduced, either inadvertently or deliberately. It can be challenging for manufacturers and retailers to validate the security claims of their products, and it may be difficult to establish responsibility for security. Furthermore, attackers may exploit this supply chain, for example, by implanting malware into a software update or third-party application. The Royal Academy of Engineering has highlighted the need for governments, industry and international institutions to collaborate on developing an international baseline for security standards.
Endnotes

34. PC World. Ransomware on Smart TVs is Here and Removing it can be a Pain. Accessed 28/11/2018.
64. POSTbrief 28 (2018) *Distributed Ledger Technology*.
69. ENISA et al. (2016). *Common Position on Cybersecurity*.
111 The European Telecommunications Standards Institute online portal, ETSI.
116 Tanczer et al., The United Kingdom’s Emerging Internet of Things (IoT) Policy Landscape. In Ellis & Mohan (Eds), Rewired: Cybersecurity Governance (due for publication in 2019).
118 General Product Safety Regulations 2005.
121 Consumer rights Act 2015.