HOUSES OF PARLIAMENT
PARLIAMENTARY OFFICE OF SCIENCE & TECHNOLOGY

POSTNOTE

Number 593 February 2019

Cyber Security of Consumer Devices

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.

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.

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).[1] Although forecasting the growth of the IoT is difficult,[2,3] analysis firm Gartner suggests that over 13 billion (bn) connected devices could be in use by consumers globally by 2020.[4] 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.[5] However, stakeholders have expressed concerns about the poor security of many devices.[6-10]

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.[11,12] 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.[13] This code was published in October 2018.[14]

Device Adoption

A 2018 survey of 3,750 consumers by Ofcom found that the most common connected devices in the UK include:[15]

- 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%).[16]

Box 1: Features of Connected Devices

Connected devices (sometimes referred to as smart devices) use software and hardware to process data, and typically include:

- **Sensors**, such as cameras, microphones or temperature sensors that enable data to be collected from the environment or user
- **Actuators**, which control a mechanism in response to a signal, such as turning on a radiator or unlocking a door[17]
- **A network connection**, to a network like the internet, often via wireless technology such as Wi-Fi, 4G, Bluetooth, or Zigbee (a low-power radio wave network). This enables data to be communicated between devices, as well as to data centres and cloud platforms where data are often remotely processed or stored.

Many devices are controlled via software on another device, such as a smartphone. Some devices, such as smart home systems, can be used to control multiple other devices.[18] This enables devices to operate together, for example lightbulbs may be switched on when a sensor detects movement (POSTnote 423).

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.[19,20] 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.[21] Attacks can also exploit software vulnerabilities resulting from programming errors or insecure software design.[22] 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.[23-27]

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).[28] These include attacks on personal computers, as well as connected devices.[29] 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.[30]

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.[31,32] 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.[33] Such vulnerabilities have been reported for smart TVs and thermostats.[34,35] 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.[39-43] 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.[44,45] Furthermore, concerns have been raised by academics and victim support services that connected devices could enable domestic abuse.[46-49] For instance, spyware may facilitate controlling or stalking behaviour (POSTnote 592).

Box 2: Computer Misuse Offences

Computer misuse covers any unauthorised access to computer material, including spreading malicious software.[36] The Office for National Statistics has suggested that incidents are under-reported.[37] According to the annual Crime Survey for England and Wales, there were an estimated 1.4 million computer misuse offences against adults in 2017.[28,37] In comparison, Action Fraud (the UK's reporting service for fraud and cybercrime) received 22,154 reports of cyber offences against individuals and businesses. In 2017, there were 47 convictions under the Computer Misuse Act.[38]

Physical damage or harm might also result from a cyber-attack. For example, a compromised device might be manipulated to operate dangerously or inappropriately.[13,50] Although there is no evidence to date of a malicious attack of this kind on an individual, attacks have occurred on industrial systems. An attack on the control system of a steel mill in Germany in 2014 prevented a blast furnace from being shut down, resulting in physical damage.[51,52]

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.[53,54] Devices on a network may also be vulnerable to malware or unauthorised use if visitors connect their own devices to the network.[55,56] 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).[57,58] 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.[59] This temporarily blocked access to Twitter, Spotify and many other websites and services.[60] Large-scale attacks may put critical national infrastructure at risk, including the provision of utilities and healthcare (POSTnote 554). 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.[61]

Box 3: Botnets

A 'botnet' is an automated network of compromised internet-connected devices that can be externally controlled, without the knowledge of the devices' users. For example, botnets of compromised consumer devices can be used for:

- **Distributed denial of service attacks (DDoS)** – blocking access to websites and internet-connected services by flooding them with requests for data.[62,63]
- **Cryptocurrency mining** – allowing the attacker to generate digital currency (POSTbrief 23).[64] This type of attack has become more common in the past year, according to security firm Symantec.[30]

Connected consumer devices most commonly recruited into botnets include Wi-Fi routers, cameras, and digital video recorders. Devices with default passwords, as well as out-of-date devices with known vulnerabilities, are common targets.[65-68]

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.[80] 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.[30]

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.[70,73,103] 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).[70,73] 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.[104] 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.[103,105] The Royal Academy of Engineering has recommended that skills development initiatives be expanded, with a focus on secure design and technical skills.[99] It has also highlighted the role of schools in ensuring that future consumers are well informed.[106] The Government published an Initial National Cyber Security Skills Strategy in December 2018.[107]

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.[108] 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.[12] An agreement on the Act was reached in December 2018.[109]

The Commonwealth

The 2018 Commonwealth Cyber Declaration committed member states to cooperate on cyber security and to promote security by default for connected devices.[110]

DCMS is developing a global standard based on the Code of Practice through the European Telecommunications Standards Institute.[89,111] The British Standards Institution 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.[112-114] 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.[115]

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.[99,116-122] 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.[123] 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.[124] 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.[125,126] 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.[127]

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.[89] 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.[128-130] 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.[131]

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.[132] DCMS is also developing a consumer IoT security labelling scheme to help inform consumers' purchasing decisions.[13]

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.[98] 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.[101] It is difficult to verify that a device is secure due to complex global supply chains (Box 6) 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.[133,134] 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.[117,133]

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.[99] 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.[123] Furthermore, attackers may exploit this supply chain,[135] for example, by implanting malware into a software update or third-party application.[30] 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.[106]

POST is an office of both Houses of Parliament, charged with providing independent and balanced analysis of policy issues that have a basis in science and technology. POST is grateful to Clare West for researching this briefing, to the Engineering and Physical Sciences Research Council for funding her parliamentary fellowship, and to all contributors and reviewers. For further information, please contact the co-author, Dr Lydia Harriss.

Endnotes

1 Government Office for Science (2014). *The Internet of Things: Making the Most of the Second Digital Revolution*.
2 IoTUK (2018). *Beyond the Economic Value of IoT Report*.
3 Maple (2017). *Security and Privacy in the Internet of Things*, Journal of Cyber Policy, Vol 2(2), pgs 155-184.
4 Gartner. *Gartner Says 8.4 Billion Connected "Things" Will be in Use in 2017, Up 31 Percent from 2016*. Accessed 28/11/2018.
5 Manyika et al. (2015). *Unlocking the Potential of the Internet of Things*. McKinsey Global Institute.
6 techUK. *Government and Tech Industry Collaborate to Improve Cyber Security*. Accessed 28/11/2018.
7 Capgemini. *Consumer Security and the Internet of Things*. Accessed 28/11/2018.
8 Schneier (2018). *Click Here to Kill Everybody*. W. W. Norton & Company.
9 Commonwealth (2018). *Commonwealth Cyber Declaration*.
10 Which?. *Could your Smart Home be Hacked?*. Accessed 28/11/2018
11 Cabinet Office (2016). *National Cyber Security Strategy 2016 to 2021*.
12 Cabinet Office (2018). *National Security Capability Review (NSCR)*.
13 Department for Digital, Culture, Media and Sport (2018). *Secure by Design Report*.
14 Department for Digital, Culture, Media and Sport (2018). *Code of Practice for Consumer IoT*.
15 Ofcom (2018). *The Communications Market 2018*.
16 TechUK (2018). *The State of the Connected Home*.
17 POSTnote 263 (2006) *Pervasive Computing*.
18 Which?. *How to Buy the Best Smart Home Hub*. Accessed 28/11/2018.
19 Loukas (2015). *Cyber-Physical Attacks: A Growing Invisible Threat*. Butterworth-Heinemann.
20 Heartfield et al. (2018). *A Taxonomy of Cyber-Physical Threats and Impact in the Smart Home*. Computers & Security, Vol 78, pgs 398–428.
21 PenTestPartners. *The Most Common IoT Device Security Failings of 2017*. Accessed 28/11/2018.
22 prpl Foundation (2016). *Security Guidance for Critical Areas of Embedded Computing*.
23 *Meltdown and Spectre*. Accessed 28/11/2018.
24 Lipp et al. (2018). *Meltdown*. arXiv.
25 Kocker et al. (2018). *Spectre Attacks: Exploiting Speculative Execution*. arXiv.
26 BBC News. *Meltdown and Spectre: All Macs, iPhones and iPads Affected*. Accessed 28/11/2018.
27 NCSC. *NCSC Response to Reports about Flaws in Processors*. Accessed 22/11/2018.
28 Office for National Statistics (2018). *Crime in England and Wales: Year Ending December 2017*.
29 Metropolitan Police (2018). Freedom of Information Request.
30 Symantec (2018). *Internet Security Threat Report (ISTR) 2018*.
31 Pen Test Partners. *Totally Pwning the Tapplock Smart Lock (the API way)*. Accessed 28/11/2018.
32 Pen Test Partners. *Totally Pwning the Tapplock Smart Lock*. Accessed 28/11/2018.
33 Carr et al. (2018). *Emerging Risks in the IoT Ecosystem: Who's Afraid of the Big Bad Smart Fridge?*. Living in the Internet of Things: Cybersecurity of the IoT - 2018
34 PC World. *Ransomware on Smart TVs is Here and Removing it can be a Pain*. Accessed 28/11/2018.
35 Pen Test Partners. *Thermostat Ransomware: a Lesson in IoT Security*. Accessed 28/11/2018.
36 Computer Misuse Act 1990
37 Office for National Statistics (2018). *Overview of Fraud and Computer Misuse Statistics for England and Wales*.
38 Ministry of Justice (2018). *Criminal Justice System Statistics Quarterly: December 2017*.
39 Federal Trade Commission. *Marketer of Internet-connected Home Security Video Cameras Settles FTC Charges it Failed to Protect Consumers' Privacy*. Accessed 28/11/2018.
40 Pen Test Partners. *Hacking Swann & FLIR/Lorex Home Security Camera Video*. Accessed 28/11/2018.
41 SEC Consult. *Internet of Babies – When Baby Monitors Fail to be Smart*. Accessed 28/11/2018.
42 BBC News. *Children's Messages in CloudPets Data Breach*. Accessed 28/11/2018.
43 Forbrukerradet. *Connected Toys Violate European Consumer Law*. Accessed 28/1/2019.
44 Schraefel et al. (2017). *The Internet of Things: Interaction Challenges to Meaningful Consent at Scale*. Interactions, Volume 24 Issue 6.
45 ENISA (2015). *Threat Landscape for Smart Home and Media Convergence*.
46 The New York Times. *Thermostats, Locks and Lights: Digital Tools of Domestic Abuse*. Accessed 28/11/2018.
47 Tanczer et al. (2018). *Tech Abuse Guide: How Internet-connected Devices Can Affect Victims of Gender-based Domestic and Sexual Violence and Abuse*. University College London.
48 Tanczer et al. (2018). *The Implications of the Internet of Things (IoT) on Victims of Gender-Based Domestic Violence and Abuse (G-IoT)*. University College London.
49 Tanczer et al. (2018). *Gender and IoT (G-IoT) Resource List*. University College London.
50 NCC Group. *Security of the Internet of Things in the Home*. Accessed 28/11/2018.
51 BBC News. *Hack Attack Causes 'Massive Damage' at Steel Works*. Accessed 28/11/2018.
52 Federal Office for Information Security in Germany (BSI) (2014). *Die Lage der IT-Sicherheit in Deutschland 2014*.
53 Pen Test Partners. *Steal your Wi-Fi Key from your Doorbell? IoT WTF!*. Accessed 28/11/2018.
54 BBC News. *Smart LED Light Bulbs Leak Wi-Fi Passwords*. Accessed 28/11/2018.
55 Broadband Internet Technical Advisory Group (2016). *Internet of Things (IoT) Security and Privacy Recommendations*.
56 Symantec (2015). *Insecurity in the Internet of Things*.
57 NCSC. *Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed*. Accessed 28/11/2018.
58 NCSC (2018). *Joint Technical Alert, Advisory: Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices*.
59 Oracle Dyn. *Dyn Analysis Summary of Friday October 21 Attack*. Company News. Accessed 28/1/2019
60 The Guardian. *DDoS Attack that Disrupted Internet was Largest of its Kind in History, Experts say*. Accessed 22/11/2018.
61 Soltan et al. (2018). *BlackIoT: IoT Botnet of High Wattage Devices can Disrupt the Power Grid*. SEC'18 Proceedings of the 27th USENIX Conference on Security Symposium, pgs 15-31.
62 NCSC (2018). *Understanding Denial of Service (DoS) Attacks*.
63 NCSC & NCA (2018). *The Cyber Threat to UK Business 2016/2017 Report*.
64 POSTbrief 28 (2018) *Distributed Ledger Technology*.
65 NCSC (2016). *Weekly Threat Report 2nd December 2016*.
66 NCSC (2016). *Weekly Threat Report 10th October 2016*.
67 NCSC (2018). *Weekly Threat Report 31st August 2018*.
68 NCSC (2017). *Weekly Threat Report 217th October 2017*.
69 ENISA et al. (2016). *Common Position on Cybersecurity*.
70 ENISA (2015). *Security and Resilience of Smart Home Environments.*
71 Joint Committee on the National Security Strategy (2016-17). Cyber Security: UK National Security in a Digital World Inquiry. Written Evidence Martyn Thomas.
72 Morgner & Benenson (2018). *Exploring Security Economics in IoT Standardization Efforts*. Proceedings 2018 NDSS Workshop on Decentralized IoT Security and Standards (DISS).
73 Internet Society (2018). *IoT Security for Policymakers*.
74 Bauer et al. (2017). *Security in the Internet of Things*. McKinsey & Company.
75 Anderson & Moore (2006). *The Economics of Information Security*. Science, Volume 314, pgs 610-613.
76 Akerlof (1970). *The Market for "Lemons": Quality Uncertainty and the Market Mechanism.* The Quarterly Journal of Economics, Volume 84, pgs. 488-500.
77 BBC News. *Amazon and eBay Pull CloudPets Smart Toys from Sale*. Accessed 28/11/2018.
78 NCSC (2017). *Secure Development and Deployment*.
79 The Conversation. *What are Software Vulnerabilities, and Why are There so Many of Them?*. Accessed 28/11/2018.
80 Black et al. (2016). *Dramatically Reducing Software Vulnerabilities*. National Institute of Standards and Technology.
81 DCMS (2018). *Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT*.
82 ENISA (2017). *Baseline Security Recommendations for IoT*.
83 U.S. Department of Homeland Security (2016). *Strategic Principles for Securing the Internet of Things (IoT)*.
84 IoT Security Foundation (2018). *Understanding the Contemporary Use of Vulnerability Disclosure in Consumer Internet of Things Product Companies*.
85 Microsoft. *Windows Lifecycle Fact Sheet*. Accessed 28/11/2018.
86 Google. *Learn When You'll Get Android Updates on Pixel & Nexus Devices*. Accessed 28/11/2018.
87 Canonical (2017). *Taking Charge of the IoT's Security Vulnerabilities*.
88 Stiftung Neue Verantwortung (2017). *Internet of Insecure Things*.

89 DCMS (2018). *Government Response to the Secure by Design Informal Consultation*.
90 Maple (2017). *Security and Privacy in the Internet of Things*. Journal of Cyber Policy, Vol 2 pgs 155-184.
91 The Internet Engineering Task Force (IETF) (2014). *Terminology for Constrained-Node Networks*.
92 Arm Ltd. *Introducing Arm TrustZone*. Accessed 28/11/2018.
93 Arm Ltd. *Platform Security Architecture*. Accessed 28/11/2018.
94 BullGuard. *Despite Fast Adoption of the Internet of Things, a Shocking 72 Percent of Consumers Don't Know How to Secure their Connected Devices*. Accessed 28/11/2018.
95 Norton (2017). *2017 Norton Cyber Security Insights Report*.
96 Cyber Aware (2018). *A Call to Action: the Cyber Aware Perception Gap*.
97 IoTUK (2017). *Cyberhygiene Insight Report*.
98 Blythe & Johnson (2018). *Rapid Evidence Assessment on Labelling Schemes and Implications for Consumer IoT Security*. PETRAS IoT Hub.
99 Royal Academy of Engineering (2018). *Cyber Safety and Resilience: Strengthening the Digital Systems that Support the Modern Economy*.
100 Coventry et al. (2014). *Using Behavioural Insights to Improve the Public's Use of Cyber Security Best Practices*. Government Office for Science.
101 Tanczer et al. (2018). *Summary Literature Review of Industry Recommendations and International Developments on IoT Security*. PETRAS IoT Hub.
102 Brass et al. (2018). *Regulating IoT: Enabling or Disabling the Capacity of the Internet of Things*. Risk & Regulation, pgs 12-15.
103 Joint Committee on the National Security Strategy (2018). *Cyber Security Skills and the UK's Critical National Infrastructure*.
104 DCMS (2018). *Government Response to Consultation on Developing the UK Cyber Security Profession*.
105 Joint Committee on the National Security Strategy (2018). *Letter to the Minister for Digital and the Creative Industries, Regarding the Cyber Security Skills Strategy, Dated 28 January 2019*.
106 Royal Academy of Engineering & PETRAS (2018). *Internet of Things: Realising the Potential of a Trusted Smart World*.
107 DCMS (2018). *Initial National Cyber Security Skills Strategy: Increasing the UK's Cyber Security Capability - a Call for Views.*
108 European Commission. *The EU Cybersecurity Certification Framework*. Accessed 22/11/2018.
109 European Commission (2018). *EU Negotiators Agree on Strengthening Europe's Cybersecurity*. Accessed 09/01/2019.
110 Commonwealth (2018). *Commonwealth Cyber Declaration*.
111 The European Telecommunications Standards Institute online portal, ETSI. DTS/CYBER-0039. Accessed 20/12/2018.
112 BSI Group. *BSI First to Provide Verification to Government's IoT Code of Practice*. Accessed 29/11/2018.
113 BSI Group. *BSI Internet of Things Assurance Services*. Accessed 28/11/2018.
114 BSI Group. *The BSI Kitemark for the Internet of Things*. Accessed 28/11/2018.
115 ANEC & BEUC (2018). *Cybersecurity for Connected Product Position Paper*.
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)
117 Anderson et al. (2008). *Security Economics and the Internal Market*. ENISA
118 General Product Safety Regulations 2005.
119 House of Commons Library (2018). *Product Safety and Recall*.
120 Consumer Protection from Unfair Trading Regulations 2008.
121 Consumer rights Act 2015.
122 BEIS (2012). *CE marking*.
123 Lloyd's (2018). *Networked world*.
124 ANEC, BEUC, Consumers International & ICRT (2017). *Securing Consumer Trust in the Internet of Things*.
125 European Commission (2017). *Brief Factual Summary on the Results of the Public Consultation on the Rules on Producer Liability for Damage Caused by a Defective Product*.
126 European Commission (2017). *Public Consultation on the Rules on Liability of the Producer for Damage Caused by a Defective Product*.
127 SB-327 (2018)
128 BEIS (2018). *Government Response to Consultation on Proposals Regarding Smart Appliances*.
129 BEIS & Ofgem (2018). *Smart Systems and Flexibility Plan: Progress Update*.
130 BEIS & Ofgem (2017). *Upgrading our Energy System: Smart Systems and Flexibility Plan*.
131 Department for Transport (2017). *The Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles*.
132 DCMS (2018). *Consumer Guidance for Smart Devices in the Home*.
133 Morgner et al. (2018). *Opinion: Security Lifetime Labels – Overcoming Information Asymmetry in Security of IoT Consumer Products*. WiSec '18 Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks, pgs 208-211.
134 Leverett et al. (2017). *Standardisation and Certification in the 'Internet of Things'*.
135 NCSC (2018). *The Principles of Supply Chain Security*.