Rethinking the cybersecurity of consumer Internet of Things (IoT): how to incentivise companies to produce cyber-secure consumer IoT products

Joo Ng

Technical Report

RHUL–ISG–2019–2

27 March 2019

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

Student Number: 100873794

Joo Ng

Rethinking the cybersecurity of consumer Internet of Things (IoT): how to incentivise companies to produce cyber-secure consumer IoT products.

(Supervisor: Robert Coles)

Submitted as part of the requirements for the award of the
MSc in Information Security
at Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledged all quotations from published or unpublished work of other people. I also declare that I have read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences, and in accordance with these regulations I submit this project report as my own work.

Signature:

Date: 22 August 2018

ACKNOWLEDGEMENT

I would like to express my appreciation to Robert Coles for his time, support, guidance, suggestions, and encouragement. His contributions helped to make this project a successful one.

TABLE OF CONTENT

LIST OF FIGURES AND TABLES

LIST OF ABBREVIATIONS

ACAA	Assessment and Acceptance of Industrial Products
Auto-ISAC	Automotive Information Sharing and Analysis Center
BSI	British Standards Institution
CAN	Controller Area Network
CCC	China Compulsory Certificate
CE	European Conformity
CERT	Computer Emergency Readiness Teams
CISP	Cyber Security Information Sharing Partnership
CSA	Canadian Standards Association
CSA	Cloud Security Alliance
CSIRT	Cyber Security Incident Response Teams
CSP	Cloud Service Provider
DCMS	Department for Digital, Culture, Media and Sport
DDoS	Distributed Denial of Service
DMCA	Digital Millennium Copyright Act
EEA	European Economic Area
EFTA	European Free Trade Association

ENISA	European Union Agency for Network and Information Security
EU	European Union
FCA	Fiat Chrysler Automotive
FSC	Forestry Stewardship Council
FTC	US Federal Trade Commission
FTP	File Transfer Protocol
GPS	Global Positioning System
GSMA	GSM Association
HVAC	Heating, ventilation, and air-conditioning
IASB	International Accounting Standards Board
ICPSC	International Consumer Product Safety Caucus
IEC	International Electrotechnical Commission
IGO	Inter-Governmental Organisations
IoT	Internet of Things
IoTSF	Internet of Things Security Foundation
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ISP	Internet Service Provider

ITU	International Telecommunication Union
JAS-ANZ	Joint Accreditation System of Australia and New Zealand
JIS	Japanese Industrial Standards
MRA	Mutual Recognition Agreement
MSC	Marine Stewardship Council
NCC	Norwegian Consumer Council
NGOs	Non-Governmental Organisations
NIST	National Institute of Standards and Technology
ODM	Original Design Manufacturer
OECD	Organization for Economic Cooperation and Development
OEM	Original Design Manufacturer
OMB	Office of Management and Budget
PAS	Publicly Available Specification
SSH	Secure Shell
SSID	Service Set Identifier
SSO	Standard setting organisation
UART	Universal Asynchronous Receiver-Transmitter
UN	United Nations

WTO	World Trade Organisation

EXECUTIVE SUMMARY

The current widespread use of poorly secured consumer IoT products has been causing menace to the overall security of the Internet (or cybersecurity). This project contributes to the exploration for an alternative and more plausible solution by rethinking the problem from a different and more fundamental perspective. This project report investigates and analyses how innate psychological factors influence consumers' thinking process when making judgement about the cybersecurity risk of IoT, and how this perception eventually leads to economic externalities that cause market failures in the provision of cybersecurity. The insights gained are then applied to formulate a plausible solution model that would incentivise enterprises to design and make consumer IoT products that are more cyber-secure.

Based on these insights, I advocate and recommend a self-regulatory model that incorporates supervision from national governments to ensure robust governance and strict compliance. The model incorporates mandatory and universal adherence to well-founded baseline cybersecurity principles for IoT products traded in the global consumer market. It entails imposing mandatory cybersecurity certification on all IoT products traded in the global consumer market. A global framework for internationally recognised certifications and cybersecurity markings that are based on international standards would provide information transparency about the security quality of IoT products. This would reduce information asymmetry about the cybersecurity of IoT products in the market and enhance consumer trust. This approach would also provide a level playing field for competition and eliminate the economic reason for free-riding in the first place.

The proposed model should also include a more global, standardised, and integrated eco-system for the responsible disclosure and sharing of vulnerability information, and for promptly repairing known IoT defects. The timely availability of accurate, consistent, and relevant information to decision makers in the global market is necessary to fundamentally address the problem regarding inadequate public information about cybersecurity vulnerabilities and incidents. The improved quality and availability of cybersecurity information enables more accurate management and allocation of security risk, as well as better decision-making and policy-making.

[Word count from Introduction to Conclusion: 19,987]

SECTION 1

1.1 Introduction

The Oxford English Dictionary succinctly defines Internet of things (IoT) as "*a proposed development of the Internet in which many everyday objects are embedded with microchips giving them network connectivity, allowing them to send and receive data.*" [OXF18].

For brevity and readability, the terms 'IoT' and 'IoT product' are used interchangeably in this report to refer to: *a combination of the IoT hardware, its associated software and services, and the underlying infrastructure required to provide and maintain these software and services*.

The Internet and its security (also known as cybersecurity) are not random manifestations. The Internet may be viewed as an organised platform where its users make decisions and act on (using computers) these decisions by interacting with each other, as well as by sharing and trading resources. Hence the state of cybersecurity reflects the collective, deliberate decisions and actions of the Internet users.

The exploitation by malicious actors of consumer IoT products connected to the Internet has been increasingly prevalent, intrusive, and damaging. The underlying knowledge and technology that are necessary to design and implement secure IoT products are already well-known and widely available. Conventional wisdom to resolving this problem has been largely technical, reactive, and inconsequential. Many organisations representing industry groups and government agencies have recommended a plethora of at least 30 cybersecurity frameworks and technical guidelines (listed in the Appendix) to address the menace. Generally, these guidelines are recommended 'best practices' and not mandatory.

Although such technical solutions are helpful and necessary, they are insufficient and reactive. It is not due to the unavailability of technological knowledge and its application that manufacturers are still designing and producing consumer IoT products with inadequate cybersecurity features. To prevent the problem from arising in the first place, we need to fundamentally understand why manufacturers of consumer IoT products are not motivated to produce cyber-secure IoT products in the first place.

This project contributes to the exploration for an alternative and more plausible solution by rethinking the problem from a different and more fundamental perspective. The study involved uncovering, evaluating, and analysing the fundamental causes that underlie the menace to cybersecurity due to the widespread use of insecure consumer IoT products. The insight gained are then applied to formulate a plausible solution model that would incentivise enterprises to design and make consumer IoT that are more secure.

This report consists of four main sections. Section 1 defines the study objectives and introduces three mini-cases that exemplify cybersecurity failures caused by insecure consumer IoT. These cases are then used to inform and stimulate the exploration of cybersecurity challenges posed by consumer IoT products in the real-world. Section 2 examines and analyses how innate psychological factors influence the average consumer's thinking process when making judgement about cybersecurity risk. It also analyses how consumers' perception and expectation about their IoT products can eventually lead to economic externalities that cause market failures in the provision of cybersecurity. Section 3 examines and analyses the justification for regulation and the potential regulatory approaches that could be brought to bear on the problem on hand. There is also a brief examination on some recent regulatory initiatives to regulate consumer IoT. Section 4 draws on the learnings and insight gained from this study to critically discuss and derive a plausible theoretical model of regulation that fundamentally addresses the underlying externalities, and hence encouraging manufacturers to make secure IoT products for the global consumer market.

1.2 Project Objectives and Methodology

This inquiry posits that the current problem of widespread availability of consumer IoT products possessing inadequate cybersecurity controls is a manifestation of an underlying and more fundamental phenomenon. A solution that addresses the fundamental causes is more successful than one that technically addresses the symptoms of the problem. Hence it is necessary to uncover and analyse the theoretical principles that fundamentally underlie the problem, before an appropriate solution model could be formulated to fundamentally address the problem.

This project aims to uncover and analyse from a behavioural, socio-economic, and policy-making perspective: what are the fundamental factors that lead to the widespread practice by manufacturers to design and make insecure consumer IoT products; why these factors have arisen in the first place; how these factors lead to the problem; and why existing solutions have been inconsequential. The findings and insight are then applied to inform the formulation of an alternative policy proposal that could effectively incentivise manufacturers to produce safer consumer IoT products.

These objectives are achieved based on the multiple-case study approach as advocated by Yin [YIN14]. This is because the method is well-founded and widely regarded to be particularly suited to extracting a holistic insight to problems in their operational and socio-economic context needed for scrutiny and analysis. This research is aided by considering three representative cases which demonstrate real-life cybersecurity failures involving a smart toy, common smart homes devices such as web-enabled surveillance cameras, and a smart car. These cases help to provide insight to: the set of decisions that led to these failures, why the decisions were taken, and how they were implemented. Observations of common patterns among the three cases would substantiate the ubiquity of cybersecurity problems among consumer IoT products and would also suggest the phenomenon shares common fundamental causes. Similarities among the cases would also strengthen the theoretical validity of generalising the analysis, findings, and proposed solution to encompass other consumer IoT products in the market.

1.3 Case Examples of IoT Vulnerabilities

This research uses three mini-cases to stimulate the exploration of human behaviour and decisions that underlie the IoT security problem. These cases describe real-life demonstrations of cybersecurity failures involving: a smart toy, popular smart homes devices, and a smart car.

1.3.1 Vulnerable Smart Toys

Genesis is a start-up company incorporated in Hong Kong. According to its website, the company describes itself as a designer, developer, and marketer of innovative hi-tech children's entertainment products. Among the products are the interactive doll 'My Friend Carla' and the interactive model robot 'iQue Intelligent Robot', both of which can converse with their users via a Bluetooth connection to an iOS or Android mobile device that is running an accompanying speech recognition application. The Bluetooth technology typically has a working range of about 10 metres.

When the mobile device is connected to the Internet, the toy can answer factual questions by using the speech recognition application to transform verbal questions into textual queries which are sent to websites such as Wikipedia, and then dictating the answers found back to the user. The speech recognition technology is provided by Nuance Communications and all voices within the working range of the toy's internal microphone are recorded and sent via the Internet connection to Nuance Communications' remote servers. These recordings could include any background conversations or any secret that a child user confides to his or her toy. When not connected to the Internet, the toys can still simulate simple conversations by using a local database of common questions and answers that is contained in the application.

In January 2015, a British information security consultancy reported [MUN15] that these toys have been proven to be effectively Bluetooth headsets dressed up as dolls, with no authentication when pairing the toy with another Bluetooth device. Consequently, any mobile device with the ubiquitous Bluetooth capability and within the working range of about 10 metres can communicate with the toy. This means by using two basic smartphones it is potentially possible for anyone to both converse

with and eavesdrop on children using these toys. The blog also illustrated how it is possible to readily edit the answer phrases that are pre-installed in the application's database so that the toy could "swear like a docker". The discovery was subsequently covered by mainstream news media including the BBC World Service [BBC15] and the Wall Street Journal [FOW15].

In June 2015, the same security consultancy reported [LOD15] that Genesis had responded by claiming "we immediately developed a patch and upgraded the software". Nevertheless, the patch was found to be inconsequential because the fix merely encrypted the local database and conveniently stored the encryption key locally in the mobile application.

In November 2016, the Norwegian Consumer Council (NCC) [FOR16, pp. 30] reported that it was still possible to connect a smart phone to the toy through unsecured Bluetooth, and then call that phone with another phone to both speak and listen through the toy. This report explicitly confirmed that, despite being made aware of the vulnerabilities as disclosed by the security consultancy since early 2015, Genesis has not yet fixed the problems. And the NCC regards this inaction as a breach of trust [FOR16, pp. 31]. Watchdog organisations in the USA, France, and Germany have also banned the sales of these toys and launched formal complaints against the manufacturer Genesis for violating privacy laws.

1.3.2 Vulnerable Surveillance Cameras and Smart Home IoT

In the paper [SHW17], a team of researchers from Ben-Gurion University of Negev provided a detailed analysis on the practical security level of 16 popular consumer IoT devices from high-end and low-end manufacturers. They investigated the Operating Systems embedded in these IoT devices, which are 11 IP cameras, 2 baby monitors, 2 smart doorbells, and a smart thermostat.

The doorbells are capable of Voice over Internet Protocol sessions, opening entry doors, and streaming video and audio. The smart thermostat can control an entire domestic heating, ventilation, and air-conditioning (HVAC) system. Like many other consumer IoT devices, all these devices run on embedded Linux operating system.

Table 1 contains a summary of the investigation findings. The investigation revealed the following vulnerabilities:

- *Vulnerable Unix root account passwords.* Using conventional brute force techniques, the login credentials for 11 of the devices have been recovered, with one device not even requiring password. These recovered passwords are common among devices of the same model. The remaining passwords were expected to be recovered in the following few weeks.

- *Exposed private keys.* Three of the devices were found to contain hard-coded private keys, which are used for encrypting communications using asymmetric cryptography. Hence, the encrypted communications can be readily compromised using a straight-forward man-in-the-middle attack and the exposed key.

- *Open ports for remote access.* It was possible to gain administrative access to 6 of the devices remotely through open Telnet service. Two devices allowed access through open File Transfer Protocol (FTP) ports and one device through open Secure Shell (SSH) port. Using these open accesses and the recovered login credentials, outsiders or malwares can readily and remotely commandeer the devices. With physical access to the remaining devices, it is still possible to establish network services through their physical universal asynchronous receiver-transmitter (UART) interfaces.

- *Exposed Wi-Fi Credentials.* To recover wireless connection after any re-boot or power outage, all the devices maintain a configuration file containing Wi-Fi settings, Wi-Fi login credentials, Service Set Identifier (SSID), and passwords in cleartext. These files can be located by simply searching for the relevant keywords in the source code.

- *Similar products with different brands.* It is a widespread practice for consumer IoT vendors to procure similar devices from original equipment manufacturers and then packaging and marketing these devices using the vendors' own brands and models. Hence the vulnerabilities uncovered by this investigation may also exist in other similar products marketed under different brands.

Using simple web searches with the recovered login credentials, the researchers found similar products for 4 of the investigated models.

- *Potential to Infect the devices with Mirai malware.* The recovered credentials could be incorporated to the existing list used by the Mirai malware, and this enhanced malware could then be used to infect these vulnerable models of devices connected to the Internet. The researchers have successfully proven this potential by conducting such an attack under controlled conditions in their laboratory.

Type	Manufacturer and Model Video	Video recording	Price (US$)	Additional capabilities	Password hash type	Remote access service	Password complexity	Contains private key	Similar product
IP camera	Simple home XCS7 1001	Yes	54	None	md5crypt	Telnet	Very low		-
IP camera	TP-Link NC250	Yes	70	None	md5crypt	-	Very low	-	-
Doorbell	Danmini WiFi Doorbell	Yes	80	Open	descrypt	Telnet	Very low	-	-
Doorbell	Ennio SYWIFI002	Yes	119	Open	descrypt	Telnet	Very low	-	-
IP camera	Simple home XCS7 1002	Yes	47	None	descrypt	Telnet	Low		-
IP camera	Simple home XCS7 1003	Yes	142	None	md5crypt	Telnet	Low	-	Tenvis TH692
IP camera	Provision PT-838	Yes	163	None	descrypt	-	Low	-	VStarcam D38
IP camera	Provision PT-737E	Yes	102	None	descrypt	Telnet	Low	-	VStarcam C23S
Thermostat	Ecobee 3	No	170	HVAC control	descrypt	-	Low	-	-
IP camera	Xtreamer Cloud camera	Yes	84	None	descrypt	-	Medium	Yes	Closeli
Baby monitor	Phillips B120N	Yes	46	None	descrypt	SSH	Medium	Yes	-
IP camera	Xiaomi YI Dome	Yes	40	None	md5crypt	-	None	-	-
IP camera	Foscam FI9816P	Yes	70	None	md5crypt	FTP	Unknown	Yes	-
IP camera	Foscam C1	Yes	58	None	md5crypt	FTP	Unknown	-	-
IP camera	Samsung SNH-1011N	Yes	68	None	md5crypt	-	Unknown		-
Baby monitor	Motorola FOCUS86T	Yes	145	None	md5crypt	-	Unknown	-	-

Table 1. Summary of findings of devices investigated in [SHW17].

1.3.3 Vulnerable Smart Car

After more than 3 years of research, automotive security experts Miller and Valasek managed to discover and successfully exploit vulnerabilities in the controller area network (CAN) and the Uconnect Access infotainment system commonly used in Chrysler, Dodge, Jeep, Ram, and Fiat brands of vehicles [MIL15]. By using a laptop to perform a few relatively straight-forward steps, the researchers succeeded in remotely exploiting vulnerabilities in: a cellular communications service to the Uconnect system; the Uconnect's in-car Wi-Fi implementation; and Uconnect's direct connection to the two CANs of a 2014 Jeep Cherokee vehicle.

The researchers disclosed the Uconnect vulnerability to the manufacturer Fiat Chrysler Automotive (FCA) in October 2014. They subsequently disclosed the CAN processor vulnerability in March 2015 and informed FCA that they intended to present the findings during the Black Hat and DEFCON conferences in August of 2015. In May 2015, the cellular communication vulnerability was also disclosed. FCA released patches for the issue on 16 July 2015.

On 21 July 2015, an article [GRE15] and a video was published on a popular technology magazine's website Wired.com featuring both researchers executing the attack, from 10 miles away, on a Jeep Cherokee driven at 70 miles per hour by a Wired.com journalist.

Three days later on 24 July 2015, Chrysler announced a recall for 1.4 million vehicles because of the vulnerabilities. The cellular service provider Sprint blocked the vulnerable communication connection to the Uconnect system. The U.S. National Highway Traffic Safety Administration launched a recall query to assess FCA's response and the proposed fixes for the security vulnerabilities [SPE15].

1.4 Mirai Botnet and Distributed Denial of Service Attacks

Mirai is a malware that spreads like worm by seeking out poorly configured IoT devices that are connected to the Internet and then commandeer these devices to form a malicious botnet. The malware is designed to infect and control popular consumer IoT devices, such as home routers, digital video recorders, close-circuit TV cameras. Figure 1 shows an overview of a Mirai botnet system. Mirai runs on a range of CPU architectures commonly used by IoT devices and it uses a dictionary attack to gain control of vulnerable devices. Once exploited, the devices are reported to a control server in order to be used as part of a large-scale Agent-Handler botnet [MAN16].

Mirai botnets were responsible for several high-profile and massive distributed denial of service (DDoS) attacks in the last quarter of 2016 [AKA18, pp. 15], [UNI17]. Unfortunately, it is extremely easy for malicious actors to use these botnets to launch DDoS attacks, including UDP, GRE, ACK, SYN, DNS, HTTP, and Valve Engine flooding. For a nominal fee, anyone could hire one of the many DDoS-for-hire

platforms available online to launch an attack. Such services lower the barrier of entry for attackers by offering them ready access to massive botnets without having to create or maintain any botnet by themselves.

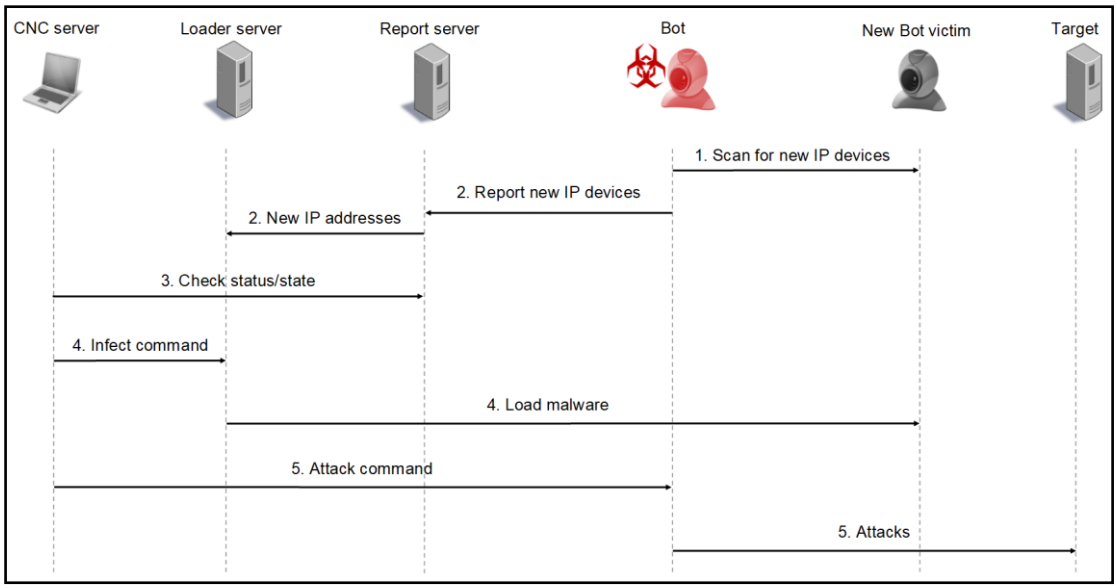

Figure 1. Overview of Mirai botnet system (source: [KOL17]).

In September 2016, a Mirai botnet directed a series of DDoS attacks at the French web host OVH. The attack peaked at least 1.1 terabits per second, making it the largest DDoS attack ever recorded at the time [GOO16]. In the same month, a Mirai botnet of IoT devices launched another massive DDoS attack exceeding 620 gigabits per second that disrupted a popular security blogging website (krebsonsecurity.com) run by Brian Krebs. On 21 October 2016, a separate series of DDoS attacks believed to be launched using Mirai botnets were directed at systems operated by Domain Name System provider Dyn [ETH16], [MAN16]. The attacks caused major Internet platforms and services to be unavailable to large swathes of the Internet in Europe and North America. Popular websites such as Twitter, Amazon, AirBnB, Spotify, GitHub, SoundCloud, Spotify, Shopify, and others had been inaccessible to many users throughout that day.

The Mirai source codes were made public in September 2016 by its author in a hacker's online forum [ANN16]. The program has since been widely analysed and adapted into many variants [AKA18, pp. 15], hence making the malware even more

menacing. Several recent detailed academic analyses of Mirai include [ANT17], [DON18] and [KOL17].

1.5 Security Challenges Created by Consumer IoT

The case examples illustrate the key threats posed by the widespread use of insecure IoT products in the consumer market. These threats are also perturbing enough to be scrutinised in a recent UK government report [DEP18], which guides the government's strategy to address the cybersecurity problem facing consumer IoT.

1.5.1 Security Threats Posed by Insecure Consumer IoT

Within a household, many insecure consumer IoT products are easy targets for malicious physical and online attacks. Malicious actors could covertly exploit the vulnerabilities of these IoT products to access and manipulate the relevant software to: steal confidential information, commandeer the devices for malicious uses, and propagate malware to other computers connected to the same or other accessible network. Hence the use of these vulnerable products in the home potentially harm the privacy, identity, and physical security of individuals and organisations. For example, besides stealing personal data from a compromised IoT system, the attacker could potentially commandeer any camera, microphone, or Global Positioning System (GPS) function available to covertly locate and monitor activities of household members, including the vulnerable ones. Vulnerable IoT devices that control actuators (such as thermostat) could be maliciously manipulated to cause physical harm, such disabling heating equipment during winter. On a wider public scale, vulnerabilities of IoT products have also been covertly exploited and commandeered to form extensive botnets that are used to launch large-scale DDoS attacks, resulting in enormous economic loss.

An independent survey [PON15] revealed that denial of service attacks account for the highest proportion (24-26%) of cyber-crime cost to UK companies, with an average annualised cost of £167,788 per attack in 2015. Another survey revealed that data centres paid an average of US$255,470 per denial of service attack [PON16].

The case examples demonstrated that successful exploitations of IoT vulnerabilities are not dubious or just theoretical possibilities. The attacks have been realistically demonstrated in the real-world using skills and resources that are relatively accessible by the public. Hence the barrier of entry to conduct these abuses is low for computer-savvy members of the public, and even lower for professional and organised criminals.

The UK government identified a variety of cyber-criminals in its national cybersecurity strategy policy paper [HMG16]. They include: organised criminal groups, states and state-sponsored groups, hacktivists, terrorists, individual ‘script kiddies’, and insiders. This suggests cyber-crimes are conducted for a wide variety of motives, ranging from financial gain, commercial or state espionage, political gain, to personal disgruntlement. The document singled out Russian-language organised criminal groups hosted in Eastern Europe as the principal culprits of increasingly advanced malware attacks on computers and networks in the UK. These attacks are becoming increasingly aggressive and confrontational, with the increasing use of ransomware and threats of DDoS for extortion. Organised cyber-crime supports a large underground industry and black-market. Apart perpetrating large-scale financial fraud on individuals and organisations, organised criminal groups also provide botnets for hire to other nefarious actors to conduct large-scale DDoS and spamming phishing emails [LUI12], [SMI15].

Even when the most serious criminals could be identified, it is often difficult for governments and international law enforcement agencies to prosecute them if they are in jurisdictions with limited or no extradition arrangements. Hence in addition to improving law enforcement cooperation internationally, other viable counter-measures include increasing the cost and effort for potential criminals to launch attacks, as well as reducing the attractiveness and vulnerabilities of potential targets. An obvious approach would be to improve the security level of consumer IoT. These measures should involve international cooperation to improve the overall cybersecurity and resilience of information and communications technology (ICT) systems and their support infrastructures.

To implement these measures effectively, it is necessary to consider the fundamental reasons that undermine cybersecurity. The case examples demonstrate that consumer IoT products are part of the problem. We need to uncover and analyse the fundamental reasons that underlie the IoT security problem before an appropriate theoretical model could be proposed to address the problem effectively. This means evaluating and considering the basic factors that influence the decisions and actions of consumers, enterprises, malicious actors, and policymakers, as well as how these activities interact collectively within their social, economic, and political milieu.

SECTION 2

2.1 Consumer Perception of Cybersecurity

This section evaluates why consumers tend to be indifferent to cybersecurity and are unwilling to pay for more-secure IoT products. It explores how individuals perceive risk, make decisions under uncertainty, and how this process differs with those adopted by organisations, including governments.

2.1.1 Bounded Rationality in Decision-Making

As humans, we must make decision on all sorts of fleeting and uncertain situations that we encounter in our daily activities. It is infeasible to methodically research, analyse and compute in detail the underlying risk probabilities before pursuing each situation. Even assuming this is possible, the underlying risk factors may already have changed by the time one finishes the calculation and assessment.

Mainstream neo-classical economists assume that the consumer is a perfectly rational actor who always compute and choose the benefit-maximising solution. However, this assumption is inconsistent with common empirical experience. Simon [SIM55], [SIM90] called this phenomenon ‘bounded rationality’ because actual decisions are influenced and bounded by various cognitive and environmental factors. These factors include lack of complete knowledge, cognitive limitations, and time constrains. He maintained that individuals do not seek to maximise benefit during decision making as it is cognitively infeasible to obtain, assimilate, and process all information to derive the optimal solution. Instead, individuals decide by

instinctively going through a simplified mental process that is adaptive, partly rational, and partly cognitive to seek an option that is sufficiently satisfying and good enough to meet our aspiration at that moment. Psychologists refer to such mental shortcut which facilitate decision making as a *heuristic process*.

Simon's argument is consistent with Tversky and Kahneman's observation [TVE74] that when making risk judgement, people rely on a limited number of crude heuristic principles to simplify the complex tasks of assessing probabilities and predicting outcomes. These crude heuristic processes are generally useful in avoiding danger and ensuring survival in a primitive environment, but they could lead to severe and systematic errors when managing certain situations in the modern society. The rest of section 2.1 attempts to establish that the current cybersecurity problem caused by consumer IoT is in fact a manifestation of one of these situations.

2.1.2 Human Perception, Intuition and Reasoning

Psychologists traditionally use the dual-process theory to explain how humans process thoughts and decisions in two different cognitive processes, namely: intuition and reasoning [KAH02], [SLO96]. Like the process of perception, the intuition process is quick, effortless, emotionally charged, and it uses association to interpret meanings. Intuition is acquired by habit and difficult to modify and control. In contrast, the reasoning process is slow, deliberate, and rule-based, as well as sequential, effortful, and emotionally neutral [KAH02], [KAH03].

According to Professor Kahneman [KAH03], reasoning occurs deliberately and effortfully by consciously searching the memory for matching concepts and performing mathematical computations. For example, this process is widely utilised within organisations during formal security risk management. In stark contrast, intuitive thinking is simplistic and occurs automatically and effortlessly; individuals tend to think intuitively when judging their personal security risks. Common experience and researches indicate that most thoughts and actions occur intuitively. Unfortunately, experiments have also shown that intuitive thoughts are prone to errors, and people (being unaccustomed to thinking hard) are often content to trust a plausible judgment that comes quickly to mind [KAH03, pp. 1450]. Hence, the principle of bounded theory and our imperfect intuitive heuristics for decision-making

suggest that individuals systematically make biased judgements and therefore do not behave rationally.

2.1.3 Cognitive Biases in Judgement under Uncertainty

Kahneman identified the most prominent explanations for our bias as the: availability and affect; representativeness; and 'anchoring and adjustment' of information during the process of intuitive judgement [KAH03]. An understanding of these concepts could enhance our insight into how consumers perceive cybersecurity risk when using IoT products.

Availability and affect bias. When assessing the probability of an event, various empirical studies have revealed that people tend to emphasise experiences and memories that are more strongly associated to the event, as well as those that can be recalled more vividly or easily [CAR78], [SHE85], [TVE74, pp. 1127-1128]. Moreover, other studies [MOR05], [SUN03] have shown that people tend to better remember their experience of highly emotional and atypical events, and hence intuitively exaggerate the probability of occurrences to these events.

The affective feeling towards a matter also influences how people decide and judge issues [SLO04]. For example, studies [FIN00] have shown that participants tend to believe technologies that they feel as beneficial would pose less risk. While technologies that they dislike and perceive as disadvantageous would pose high risk. Moreover, this affective feeling could be manipulated. After being provided with information that stress the benefits or low risks of a technology, the participants significantly reversed their initial negative bias.

Representativeness bias. When assessing the probability question involving two dependent events, people tend to assign more weight to both events if they seem more representative or resemblant of each other. For example, when A is highly representative of B, the probability that A originates from B is judged to be high. This bias causes serious misjudgements such as: base-rate error, sample size error, insensitivity to predictability, illusion of validity, and misconception of regression [TVE74, pp. 1124-1127], [TVE83].

Anchoring and adjustment bias. This bias occurs when people are given a value (anchor) to ponder before being asked to estimate an unknown quantity. Experiments have revealed that the estimated quantity remains close to the anchor value. For example, if a house is advertised with a high asking price, potential buyers will value the house more than if it were advertised at low asking price [KAH11, Ch. 11].

Unrealistic optimism bias. Psychological studies [ROS66], [WEI80] have consistently shown that when predicting outcomes of personal events, people tend to believe good outcomes are more likely than bad ones. This is consistent with Adams' [ADA97] observation that people have an innate individualised 'risk thermometer', which intuitively reconciles the potential satisfaction of undertaking a risk against a limited number of subjective cognitive factors, such as danger, risk propensity, and previous experience of loss. This helps to explain why people still choose to pursue dangerous activities such as smoking and extreme sport despite knowing the potential danger.

Mental accounting/Framing bias. Studies have revealed that when subjected to different circumstances, people assign different reference prices to the same item. For example, Kahneman and Tversky [TVE81] showed that people are unlikely to buy a replacement theatre ticket after losing the original one. But they are more likely to still buy a new ticket after losing the same amount of money just before purchasing the ticket. In fact, the same amount of money has been lost in both scenarios. But in the subject's mind, buying a second ticket is more aversive because it is included in the mental account for theatre-going, but the loss of the money is not.

A related heuristic model that accommodates the existing understanding of human cognitive bias when making risky decisions is the prospect theory [KAH79]. It embodies empirical observations of people's willingness or reluctance to take risks, depending on whether the stakes are perceived as relative gains or losses. More specifically, the prospect theory postulates that people:

- tend to evaluate the expectation of gain and loss relative to a chosen reference point, e.g. the status quo.

- are risk averse. When deciding on gains, people prefer certainty and hence tend to accept a sure gain over a probable but significantly bigger gain. For example: option A is a 50% chance of gaining $1,000 and a 50% chance of gaining nothing. And option B is a sure gain of $500. Experiments has shown that most participants will choose option B.

- are risk seeking. People do not perceive gains and losses equally. When deciding on losses, people tend to protect what they already have. A loss is perceived as more averse than a gain of the same amount. Hence, people prefer to accept a gamble that could prevent a loss over a sure but smaller loss. For example, option A is a 50% chance of losing $1,000, and a 50% chance of losing nothing. And option B is a sure loss of $500. Experiments has revealed that most participants will choose option A.

A corollary of the prospect theory is that people could make contradicting decisions to two effectively equivalent questions depending on whether the question is expressed (or framed) as gain or a loss. This is illustrated by the well-known Asian Disease problem [TVE81]. An Asian Disease is expected to kill 600 people. Two independent sets of participants were asked to select between two alternative programs to combat the disease.

The first set of participants were asked to choose between programs that were framed positively by focusing on lives saved. More specifically: if program A is adopted, 200 people will be saved. If program B is adopted, there is a 33% chance that 600 people will be saved and a 67% chance that nobody will be saved. In this case, 72% of participants chose A.

The second set of participants were asked to choose between programs that were framed negatively by focusing on lives lost. More specifically: If program A is adopted, 400 people will die. Or if program B is adopted, there is a 33% chance that nobody will die and a 67% chance that 600 will die. In this case, 78% of participants chose B.

In fact, both are statistically similar. However, the choices reflected the participants' risk-averse preference for 'sure gain' (i.e. lives saved) in the first case, and risk-seeking preference to take extraordinary risk in order to prevent the sure loss of lives in the second case.

As Schneier [SCH08] has observed, security risk is both a subjective feeling and an objective reality. One might feel secure when it is not secure in reality. Conversely one might feel insecure when it is in fact secure. A security risk judgement involves a trade-off between the cost of preventing perceived harm and cost of actual harm. An understanding of people's irrational cognitive biases could enhance our insight into how consumers tend to make security judgements based on perceived rather than actual risk. It demystifies how the divergence between the perceived and actual security risk of IoT products could (mis)lead individual consumers to make decisions that collectively cause market failures and undesirable social outcome.

2.1.4 Linking Cognitive Bias and Consumer's Perception of Cybersecurity Risk

Understanding both the fact that the average consumer has not personally experienced a cybersecurity incident, and the insight to the shortcomings of our intuitive heuristic processes when judging risks could help us to fundamentally explain why IoT consumers are generally apathetic about cybersecurity.

The average Internet users are generally apathetic about others hacking into their computers and they are unlikely to have personally experienced any hacking incident. This is substantiated by figures from recent global surveys. As shown in Figure 2, only 4% and 6% of Internet users worldwide had their online accounts or devices, respectively, hacked into in the second half of 2017 [KAS18]. Other consumer surveys [ISA15a], [ISA15b], [ISA15c] conducted in 2015 by Information Systems Audit and Control Association (ISACA) suggest only that about 37% of Internet users in the USA, UK, and Australia are seriously concerned about someone hacking in their IoT devices (see Table 2). In England and Wales, less than 3% of adults reported crimes in computer misuse (which include virus, unauthorised access to personal information, and hacking incidence) during the year ending March 2018 [ELK18].

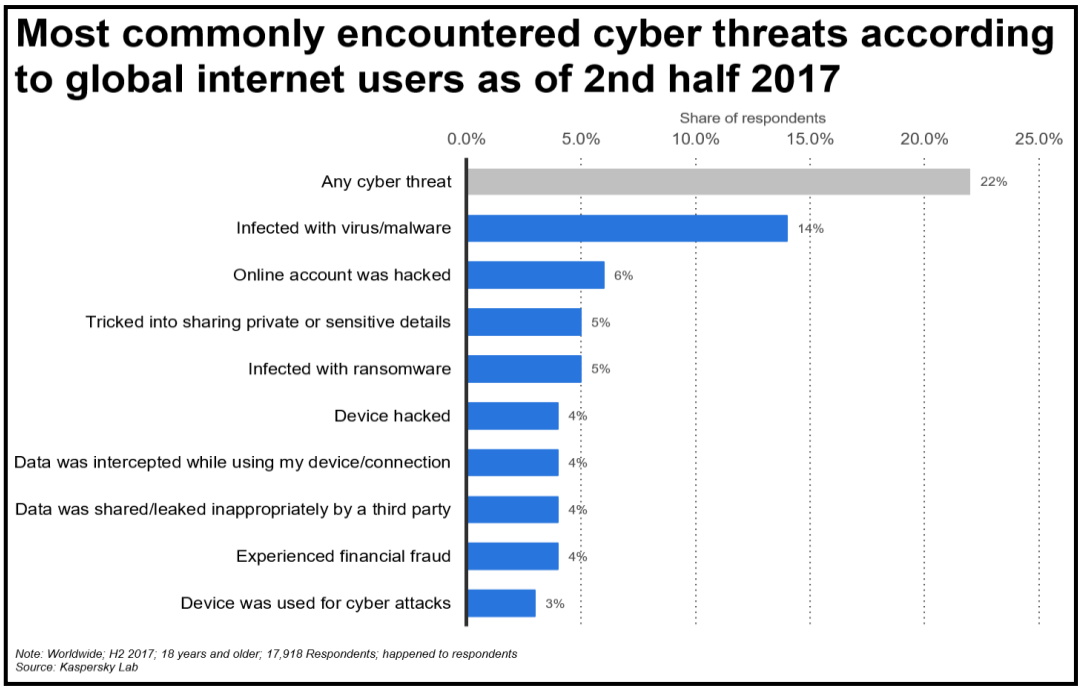

Figure 2. Cyber threats encountered by Internet users worldwide 2017 (source: [KAS18]).

These evidences indicate that the average consumer is unlikely to have personal memory or affective feeling associated with real-life cyberattacks. Without these unpleasant feelings and as adopters of IoT technology, the average IoT consumer is likely to have positive feeling about the advantage of IoT technology. Our understanding of the heuristics of availability and affect bias suggests that such positive emotion would further reinforce the consumer's feeling of security associated with IoT products.

Without any personal experience and memory of cyberattack as mental reference, average consumers of IoT products are unlikely to distinguish the cybersecurity quality of IoT products from the health and safety quality which they are accustomed to in other consumer products. The principle of representativeness bias suggests that it would be quite natural for average consumers to intuitively associate IoT products with any other consumer products. For example, consumers expect their smart car to be safe when they purchase the car from the dealer. They do not need to know how the emission system, braking system, CAN Bus, authentication, or encryption work to expect their car to be safe.

As illustrated by the botnet DDoS attacks narrated in section 1.4, exploiting a small percentage of vulnerable IoT devices is enough to cause overwhelming disruption to organisations in large swathes of the Internet. Nevertheless, the revelations from this analysis suggest that the perception of average consumers is probably insulated from this reality, as their personal experience would lead them to intuitively conclude that the Internet is in fact a safe service. If a DDoS attack severely disrupts the consumer's Internet service, the consumer would regard the problem as the incompetence of the Internet Service Provider (ISP). Because consumers are paying for the service, they expect their ISP to deliver the service and sort out its internal technical problems. The principle of mental accounting or framing suggests that the average consumers would intuitively believe they have already paid for cybersecurity as part of their product purchases. Like any other consumer products, the product price implicitly includes reasonable product safety and security. That is why they rarely experienced any cyberattack in the first place. Nevertheless, this expectation is unlikely to be acceptable to the numerous enterprises and organisations, such as Dyn, that bore the brunt of costly DDoS attacks from botnets of commandeered consumer IoT devices.

Which of the following, if any, concerns you most about the information delivered to connected/"Internet of Things" devices. (i.e., devices that connect with each other or to the Internet)? (Please select ONE.)

	USA	UK	Australia	Average
(Total Respondents)	1227	1025	1060	
Someone will hack into the device and do something malicious.	*39%*	*36%*	*36%*	*37%*
You don't know how the information that is collected by these device(s) will be used.	21%	20%	23%	21%
Companies/organizations will sell your personal information to other companies/organizations.	12%	18%	15%	15%
Companies/organizations will be able to track your life (e.g., actions, whereabouts, etc.).	11%	10%	11%	11%
Companies/organizations will use your personal information to market to you.	6%	9%	9%	8%
Other.	1%	--	1%	1%
You have no concerns.	10%	2%	7%	6%

Note:
- Due to rounding, percentages may not add up to 100.
- At a 95% confidence level, the margin of error for each individual country sample is +/- 3.1%.
Source: ISACA IT Risk/Reward Barometer.

Table 2. Concern about information delivered to IoT devices (sources: [ISA15a], [ISA15b], [ISA15c]).

Manufacturers of consumer IoT are unlikely to convince their consumers to pay extra for more-secure IoT products. Firstly, the heuristics of unrealistic optimism bias would intuitively nudge the consumers to assume that unfortunate events such as

cyberattacks are unlikely to happen to them. Secondly, the heuristics process of anchor and adjustments bias would intuitively compel the consumers to reference (or anchor) any additional security from their personal experience, which intuitively is already secure enough for their purpose.

Moreover, the principles of prospect theory suggest that the consumers are likely to prefer the sure gain of low product price to any uncertain but bigger gain of more-secure IoT products. In fact, there is no 'bigger gain' to be had in the first place since the consumers already feel relatively safe intuitively from their existing perspective or frame. Framing the problem to the consumers as a potential loss of cybersecurity would not help the manufacturer's quandary either. The evidence from the prospect theory suggest that the consumers would be more willing to gamble a bigger but uncertain loss in order to preserve the sure gain of low product price that they have been enjoying. This suggests that while manufacturers may regard the extra cost of security controls as affordable to consumers, the consumers intuitively perceive this potential loss as worse than any perceived gain in security.

As suggested by the Bounded Rationality theory, when deciding to purchase an IoT product, average consumers are likely to seek a product that is sufficiently satisfying and good enough to meet their aspiration at that time. Unlike organisations, individual customers are unlikely to perform a risk assessment to identify, analyse, and compute the probabilities of potential cybersecurity risks, and then evaluate these risks against some policy-based criteria that would optimise the overall cybersecurity of the entire Internet. Moreover, the innate biases of intuitive judgement which we have discussed reinforce the consumers' objection to paying more for IoT products in order to improve the overall cybersecurity of the Internet.

2.2 Commercial Challenges of the Consumer IoT Market

The global market for consumer IoT is a substantial one. Surveys have claimed that consumers spent US$532 billion worldwide on IoT endpoints in 2016 [GAR17] and the product price is an important consideration for customer. For example, a British consumer survey in 2016 [THO16] on connected smart home IoT revealed that high price is the main reason (48%) preventing consumers from buying smart home IoT

devices. Another survey [BAU17] revealed that although IoT consumers and producers expect cybersecurity with IoT products, they are unwilling to pay a premium for it.

The current cybersecurity problem involving consumer IoT products can be viewed as a manifestation of the collective market arrangement which reflects the behaviour and decisions of consumers, as well as the responses by enterprises. Consequently, the market outcome is that many, if not most, IoT products are likely to be much less secure than conventional computers. In the commercial interest of minimising cost, such devices tend to be equipped with just enough computational capability to perform their advertised functions and not enough to provide adequate cybersecurity.

The consumer product market is an intensely competitive one. The profitability and viability of manufacturers hinges on their ability to minimise cost and market their products expeditiously, as well as on a sustainable level product pricing and market demand. In this context, focusing on the cybersecurity of products is counterproductive as it does not generate profit, increases cost, and increases time-to-market. This is especially so for the many start-ups in the consumer IoT market, which typically operate with extremely limited resources. If an enterprise cannot generate enough sales at a price level to at least recover its cost, then the business is not viable in the first place, let alone the cybersecurity of products.

This reality was illustrated in an analysis by CB Insights [CBI17], which tracked 382 consumer hardware start-ups based in the USA. It found that 74% of these start-ups failed to obtain investment beyond the initial round and 97% of them eventually failed or became zombie companies (companies generating just about enough cash to service their debt). Of these zombie companies, 57% are dormant. The report identified the top 3 for reasons for the failure of these start-up enterprises as: lack of consumer demand, high cash burn-rate, and lack of interest after the initial round of funding.

Start-ups selling consumer hardware such as IoT devices typically need to manufacture and stock up the hardware before going to market, and thus incur manufacturing and logistics cost in addition to marketing cost and other overheads.

Hence for these start-ups, the typically small seed round of funding would only finance their projects up to a limited product launch before more funding is needed. In many cases, there is little market demand for these typically over-priced products to convince any venture capital investor to provide a more substantial round of fund to scale up production. Among the many casualties of this brutally competitive market is Jawbone, a prominent manufacturer of wearable IoT which was once valued at US$3 billion [BRA17]. Jawbone went into liquidation in July 2017 after defaulting on a US$1 million debt with a supplier, despite having received more than US$900 million of funding from venture capital investors during its 17-years history [ALB17].

Through the years, competing enterprises in the IoT industry have created a plethora of proprietary ecosystems of devices, services, service platforms, and communication protocols in their hope to dominate or capture a slice of the market. These assortment of disparate IoT ecosystems and their underlying technologies not only defeat the potential of the IoT concept but also annoy consumers by forcing them to keep different applications in their smart phone or tablets for different makes of products. This in turn imposes additional complexity and cost to incorporating cybersecurity to the IoT products.

2.2.1 State of Supply Chain for Consumer IoT Products

From the production perspective, consumer decisions and their reactions by enterprises are also reflected in the current market arrangement of the IoT supply chain. This status quo in turn contributes to the cybersecurity problem inherent in consumer IoT products.

Globalisation and technology advances, especially in the fields of ICT technology and logistics, during the last 30 years or so has enabled a very advanced degree of division of labour in the guise of global supply chains in the manufacturing industry. To optimise economic efficiency, the modern supply chain operates with a high degree of specialisation by exploiting the benefits of modern globalisation and technology. A typical supply chain for consumer goods consists of highly specialised partners whose operations and activities are tightly integrated using commercial contracts and ICT. Among the primary partners are: component manufacturers,

original design manufacturers, original design manufacturers, and cloud service providers.

Component Manufacturer. The main IoT hardware components such as the processor and memories chips, as well as the firmware embedded in them are typically standard products made by specialised semi-conductor manufacturers such as Samsung, Texas Instruments, Broadcom, and ARM. The low-cost, miniature, and low-power requirements of IoT usage entail these components to be inherently low-powered with minimal computing capacity.

Original design manufacturer (ODM) and *original design manufacturer (OEM)*. An ODM is typically an enterprise that designs, develops, and makes both the hardware and software of a product on the behalf of the ODM's clients. In contrast, an OEM typically manufactures a product on the behalf of its clients using design specifications provided by the clients. Both the OEM and ODM assemble the product using standard components procured from component manufacturers. The application software that provides the services accompanying IoT devices could be developed by an ODM or another third-party software contractor. Such a software could be a smart phone application that communicates directly with the IoT devices, as well as remotely with a remote cloud service. To maximise efficiency and minimise cost where possible, applications are usually developed by reusing existing software components, open-source codes, and a variety of communication protocols.

Cloud Service Provider (CSP). The CSP provides the backend cloud services that remotely store and process data collected by IoT devices. These cloud services are typically provided by third-party CSPs such as Amazon and many others. Some ODMs also provide their own cloud services to their clients.

It is worthwhile to consider the process of developing modern application software in order to appreciate the constant struggle to balance software quality with commercial pressure to monetise the product. The development of modern software solution is typically managed using a variant of the Agile methodology. This technique is designed to deliver software quickly in order to keep abreast with the increasing pace of technological change and time-to-market of the product. The methodology aims to

accelerate software production by prioritising and limiting the scope and requirements of each version of the software to commensurate with the desired time-to-market. Hence a version of a software is released for production as soon as it is deemed to be fit for purpose. Improvements and enhancements are gradually added in subsequent iterations of version. This enables an enterprise to monetise its product design quickly and to maximise the product's fleeting foothold in the market before becoming undercut by competitors.

The Agile methodology is merely a management tool and its principles, in theory, do not entail any sacrifice of security over speed. It is up to the practitioners to define what 'fit for purpose' encompasses and to decide how they want to use the tool. Unfortunately, in realty the combination of limited financial resource, bounded rationality of decision makers, and overwhelming commercial pressure often culminate in unrealistic requirements to be built into a product using insufficient resources and timeframe. Consequently, products are often compelled to be released pre-maturely for production after it has been hastily tested to fulfil the most basic user functions. The inherent flexibility of Agile could be easily misused as an easy excuse to perpetually sweep any non-user defects, including security-related ones, aside to the next iteration of development.

All these means of division of labour has enabled enterprises in a modern supply chain to adapt to business models and operations that exploit competitive advantages provided by labour, resources, and capital worldwide to minimise cost. Such arrangement is double-edged because it escalates cost competition to a global scale, and this race to the bottom in order to quote the lowest price inevitably overlook the cybersecurity of IoT products because security incurs cost. And as we have learnt, consumers expect security but they are unwilling to pay for it anyway.

2.2.2 Market Competition and its Effect on Cybersecurity

Like most other consumer electronic products, consumer IoT products are either close imitations made by enterprises trying to capture a slice of the existing market, or novel products from start-ups or existing manufacturers hoping to create and dominate a new market before other imitators join the competition. The combination of low entry barrier to market, fierce competition, and low price point as discussed

earlier ensures minimum room to realise profit from the hardware and software alone. Any meaningful profit must come from additional value realised from the product's novelty and utility.

It is a common practice among consumer electronic product manufacturers (including IoT manufacturers) not to have in-house expertise and resource for designing or building their own end products. Instead, it is more economical to provide the product requirements and specifications to a third-party OEM or ODM, which will design and develop the product (in the case of ODM) and build the hardware using components procured from component suppliers. The IoT manufacturer merely adds its brand, name, and packaging to the end products and focuses on marketing them.

The security vulnerabilities revealed in the case examples are outlined in Table 3. Some of the IoT products examined in these cases do not even include any ability to update the embedded firmware. Hence these devices stay exposed to all vulnerabilities discovered during their lifespan. Although other IoT manufacturers may provide update facilities for their firmware and software, the update mechanism and its infrastructure may not function securely. In addition to fixing program bugs and vulnerabilities, program updates need to be delivered securely as well as applied promptly and correctly without causing any undesirable side-effect.

Table 4 contains a summary of some basic security control principles which are often taken for granted in conventional computing systems. Unsurprisingly, all the attacks identified in the case examples would had been forestalled had those underlying IoT products implemented these basic control principles. However, the adoption of these controls would also require IoT manufacturers to implement the underlying technical, physical, and administrative infrastructures, as well as the resources needed to sustain them in order to support the product lifecycle of the entire product range. The technologies that need to be implemented would have to include: identifying and authenticating the correct target programs; signing and verifying the update programs; encryption of data in transit; as well as a robust regime to securely maintain encryption keys. These implementations would entail the manufacturers to use more advance hardware components and more sophisticated programs for their products, as well as to hire more highly skilled professionals to do the work. Not only

do all this additional effort generate no revenue, it may also quickly escalate production and maintenance cost substantially to an unsustainable level for low-value IoT products.

Case	Vulnerabilities
Smart toy	▪ Communicating programs were not subjected to adequate identification, authentication, and authorisation before exchanging data with each other. ▪ Data and programs were not encrypted or protected from modification. ▪ Details of collection and processing of personal data were not fully and clearly disclosed to users. ▪ Cryptographic keys were stored locally and in cleartext. ▪ Sensitive data in transit were not encrypted.
Smart car	▪ Communicating programs were not subjected to adequate identification, authentication, and authorisation before exchanging data with each other. ▪ Critical data and programs were not encrypted or protected from modification.
Smart home devices	▪ Communicating programs were not subjected to adequate identification, authentication, and authorisation before exchanging data with each other. ▪ Application software uses well-known default passwords. ▪ Program interfaces were not secured.

Table 3. Security vulnerabilities revealed in the case examples.

We have examined how the choices and behaviour of both consumers and manufacturers have collectively led to fundamental design and implementation flaws in consumer IoT products, which in turn are causing menace to the overall cybersecurity of the Internet.

2.3 Analysis of Some Existing IoT Best Practice Guidelines

An IoT eco-system is essentially an information processing system connected to a network and hence it shares the same fundamental information security requirements as those of any other networked computer. These requirements are the protection of confidentiality, integrity, and availability of information that are stored, processed, and transmitted by the system. Nevertheless, the usage model as well as technical constraints inherent in the hardware and software architecture of consumer IoT systems present unique vulnerabilities that increases the attack surface. The three

case examples illustrated how these vulnerabilities could be realistically exploited to cause widespread physical and economic harm to the public and the society.

Process	Control	Control Description
Entity identification, authentication, and authorisation	▪ Identification, authentication, and authorisation (IAA)	▪ Before exchanging data, the communicating software and hardware entities must be identified, authenticated using appropriate cryptographic protocols. ▪ The permission of authenticated entities must be verified to ensure that they are authorised to perform the transaction.
Secure password	▪ No default password ▪ Secure default configuration	▪ The system should enforce compulsory password change upon first use, as well as a strong password regime.
Data in transit	▪ Encryption ▪ Data protection	▪ Data transmitted between devices, service apps, and backend cloud servers through unsecured channels must be encrypted with an appropriate encryption technology. ▪ Data transmitted must be signed at the source and then verified at the destination to ensure the data's integrity.
Data at rest	▪ Data protection ▪ Encryption	▪ Program source codes, and user and personal data stored in end-point devices, applications on smart phones or tablets, and remote servers must be encrypted with an appropriate encryption technology. ▪ Passwords and encryption keys must be hashed and randomised with salt values using with an appropriate encryption technology and then stored using appropriate technology, such as in Trusted Platform Modules.
Data processing	▪ Privacy ▪ Secure default configuration ▪ Hardening ▪ Secure API ▪ Physical security	▪ Manufacturers must provide a privacy policy written in clear and unambiguous language to disclose what personal are collected and how they are processed, stored, and shared. ▪ Both hardware and software must be hardened to remove or disable all unnecessary functionalities, codes, interface to minimise attack surface. ▪ Interfaces must validate and sanitise all input data before the data are used for processing. ▪ Hardware need to include seals or temper-resistance technology to detect and deter tempering.
Program update	▪ Over-the-air update	▪ Manufacturers must provide automated update mechanism for implementing fixes to program bugs and vulnerabilities. ▪ All update program updates must be delivered securely as well as applied promptly, correctly without causing any side-effect, and securely.

Table 4. Summary of some basic security control principles.

There is no shortage of advice available to the public for best practices of IoT security. Currently, there are at least thirty guidelines (listed in the Appendix) that recommend security best practices for IoT and their associated infrastructures. These guidelines are freely available to the public and collectively they address a broad range of security controls for IoT systems, including: risk assessment of threats, security frameworks and models, secure-design principles, and security controls for IoT endpoint, service and infrastructure. These voluntary guidelines are

provided by organisations representing a wide range of industrial and governmental interests, including: International Telecommunication Union (ITU), European Union Agency for Network and Information Security (ENISA), US Federal Trade Commission (FTC), UK Department for Digital, Culture, Media and Sport (DCMS), Cloud Security Alliance (CSA), Internet of Things Security Foundation (IoTSF), Automotive Information Sharing and Analysis Center (Auto-ISAC), and GSM Association (GSMA), just to mention a few. The coverage and details of these documents vary widely. For example, the 'I Am The Calvary's Automotive Cyber Safety Framework' contains only high-level framework principles for the automotive industry. In contrast, the GSMA's IoT Security Guidelines consist of a suite of four documents that cover IoT device, service, and infrastructure in significant details.

The bar chart in Figure 3 summarises security controls that have been addressed by the thirty IoT security guidelines identified in the Appendix. The 13 black bars in the chart indicate security controls that are addressed in the majority (i.e. at least 50%) of these guidelines. These security controls are by no means novel. In their 1975 tutorial paper [SAL75], Saltzer and Schroeder had already identified (amongst other security control principles) the importance of: secure design; identification, authentication, and authorisation; encryption; secure default configuration; data protection; privacy; and secure password as controls that can guide the design and implementation of information security in computer systems.

The principles and practices for securing computing systems are also not recent conceptions. In 1992, the Organization for Economic Cooperation and Development (OECD) published its first Guidelines for the Security of Information Systems [ORG92], which are adopted by OECD member countries. An objective of the guideline is to "raise awareness about the risk to information systems and networks; the policies, practices, measures and procedures available to address those risks; and the need for their adoption and implementation." This guideline formed the basis of National Institute of Standards and Technology's Generally Accepted Principles and Practices for Securing Information Technology Systems [SWA96], which was first published in 1996.

It is also worth clarifying that ‘secure by design’, which according to Figure 3 is the second most frequently cited security control among the guidelines, is not a technology but a conceptual approach to software and hardware development. Instead of the common practice of treating security reactively as an after-thought, the secure by design concept advocates a proactive approach that focuses on designing computing systems that are holistically secure using well-proven principles and technical measures. Such as: authentication safeguards, adherence to best programming practices, secure configuration by default, and continuous testing. Hence, the other technical controls identified can be viewed as tools which are available to realise the secure by design approach.

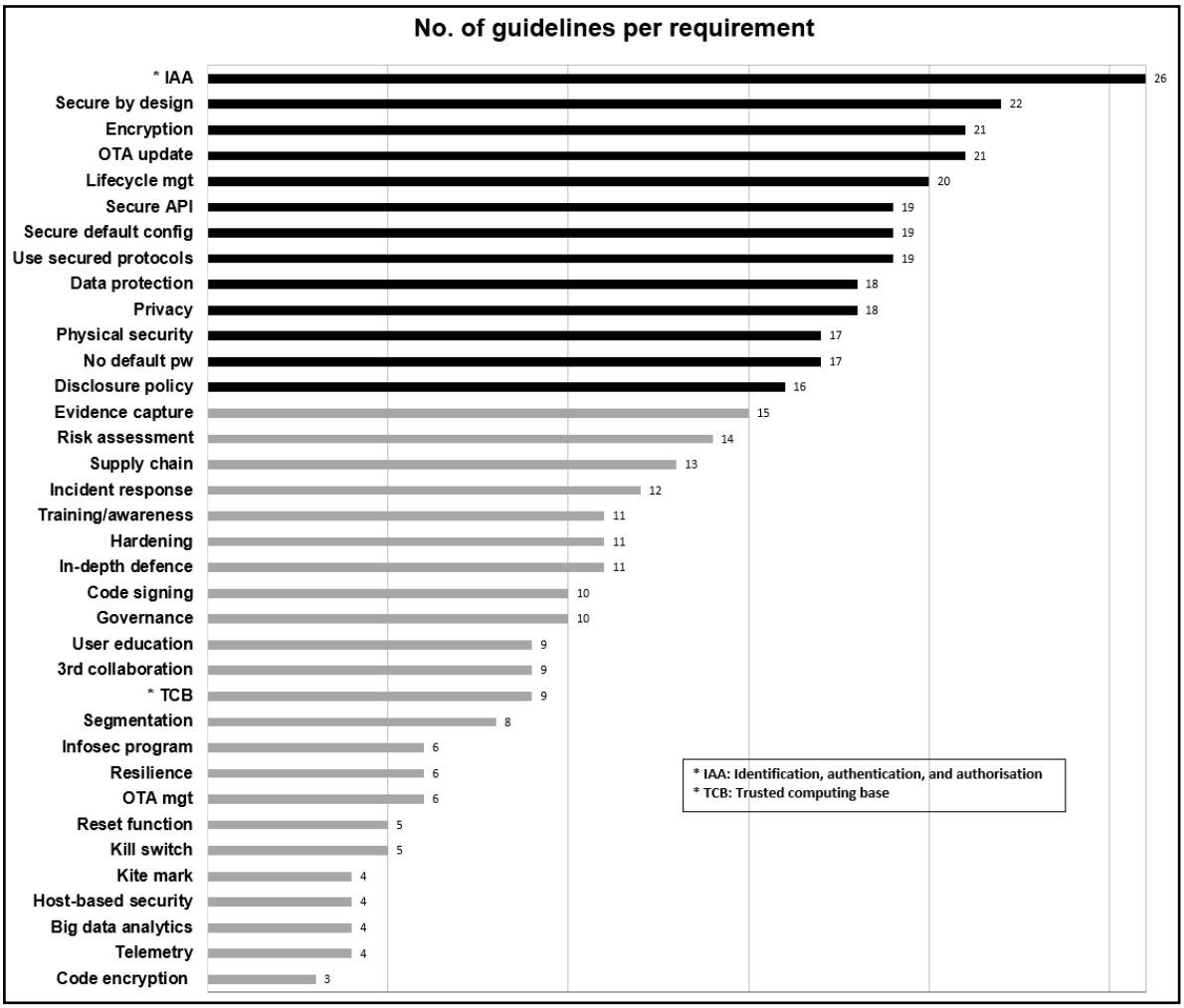

Figure 3. Frequency of requirements mentioned in IoT security guidelines.

Unsurprisingly, the basic IoT security controls (which are outlined in Table 4) necessary to prevent all attacks described in the three case examples are also

encompassed amongst the thirteen most cited controls (the black bars in Figure 3) identified in this analysis. This revelation inevitably raises the questions:

- Why were all these basic and time-honoured controls overlooked in practice when they are included in at least sixteen publicly available IoT security guidelines?

- Could the society rely on the industry's voluntary initiatives to provide the cybersecurity of consumer IoT system?

2.4 Economics of Cybersecurity

Market failure occurs when participants in a free market are motivated to make economic decisions that are collectively undesirable to the society. The current cybersecurity problem involving consumer IoT seems to resemble manifestations of market failure caused by a combination of the nature of cybersecurity and the adverse economic decisions made by both consumers and enterprises. Hence an analysis of the problem from a socio-economic perspective could provide useful alternative insight to inform the formulation of a suitable theoretical model for intervention.

2.4.1 Cybersecurity as a Public Good and the Free Rider Problem

Samuelson [SAM54] first formalised the concept of a public good, which is one that is non-rivalrous and non-excludable. Non-rivalry refers to the property that consuming the good normally does not reduce its supply available to others. Non-exclusion refers to the property that, while providing the good, it is not practical to exclude other people from consuming the same good. In contrast, a private good is rivalrous and excludable because it is sold to those who can afford to pay its market price, and hence excluding those who cannot afford the price.

These inherent properties of the public good poses a 'free rider' problem [KIM84]. Because somebody can free-ride and freely enjoy the benefit of a public good provided by others, there is no natural incentive in a free market for someone to pay for the supply of the good. Consequenty, the problem of free riding causes market

failure in the form of shortage of public goods in the free market. This is because the rational but selfish decisions of individuals will collectively result in the over-consumption and under-supply of the public goods, and hence to the detriment of overall social well-being [COR96]. Economists refer to this moral hazard as tragedy of the commons [HAR68], [LLO80].

Cybersecurity resembles public good as it is non-rivalrous and non-excludable. An enterprise which builds IoT products that resist exploitation by botnets will intrinsically contribute to the overall security of the Internet by raising the cost of attack. This positive externality will be enjoyed by all Internet users as it is not practical to restrict this enjoyment only to users who have paid for these devices. Unfortunately, this desirable externality is unsustainable in practice as it encourages competitors as well as other Internet users to free-ride on the benefit. This prevents manufacturers of secure IoT products from getting adequately rewarded for their extra cost of providing cybersecurity service. Consequently, as demonstrated by the three case examples, the supply and use of vulnerable IoT products have large undesirable effects on other innocent Internet users by putting them at risk of cyberattacks.

Like all commercial enterprises, the primary aim of IoT manufacturers is to maximise profit. This objective necessitates minimising cost and maximising revenue. Unfortunately, it costs significant time, money, and resources to design and incorporate robust cybersecurity features into the already low-budget and miniature IoT products. Unless these cybersecurity features are mandated by the law or strong social norm, which in turn could hinder profit generation, it is not in the manufacturers' best interest to voluntarily build robust security into the consumer IoT products.

2.4.2 Market Failure due to Economic Externality

The problem of tragedy of the commons is in fact an instance of a wider concept called economic externality. In 1920, Pigou [PIG32] introduced the concept of externality by expounding on the lack of incentive for private firms to pay for (or internalise) certain cost imposed on the wider society because of their pursuit for maximum profit.

Externality is the economic cost or benefit that is imposed on external parties who are not involved in an economic transaction. Externality can be either positive (beneficial) or negative (harmful). If left uncontrolled, negative externalities cause inefficiencies in the market and the over-consumption of economic resources. For example, the failure by enterprises to pay for anti-pollution measures of their industrial activities and consequently causing damages the environment, human health, and social well-being. Hence these enterprises have not internalized all the costs of their undesirable actions. In the case of positive externality, an enterprise has not internalized all benefits caused by its action. For example, results of an enterprise's research and development activities may benefit other parties in the society beyond the enterprise, because the findings add to the general body of knowledge that contributes to other discoveries and developments.

Theoretically, positive externalities will be under-supplied in the market due to the free-rider problem. While negative externalities will be over-supplied because producers will internalize all benefits of their activities but not all the costs. The conventional wisdom is that government should align the social costs and benefits by penalising or regulating those activities responsible for negative externalities, and supporting activities that cause positive negativities through subsidies or other incentives. Pigou suggested that government intervene by levying a tax on the producer of negative externality to cover the social cost that is not privately borne by the producer. This tax, also known as Pigouvian tax, is set equal to the social cost of the negative externality. Alternatively, the government may impose regulation such as private law or quality standards to internalise the true cost. If the society widely relies heavily on a public good, such as cybersecurity, then there may also be a justification to impose public quality standard on the good. Nevertheless, such interventions may not be worthwhile when the administrative cost to re-allocate the social cost outweighs the desired social benefit.

Besides the problem of tragedy of the commons, various other negative externalities could be identified to explain the failure of cybersecurity in the market for consumer IoT. These externalities include: information asymmetry, and network effect (or network externality), and misaligned economic incentives.

2.4.3 Information Asymmetry in the Market

In a wider context of cybersecurity, a form of market failure due to information asymmetry occurs when organisations do not disclose information or accurate information on losses due to security breaches. For example, because it serves their commercial interest to do so, security consultancies tend to exaggerate risks involving newly discovered security breaches, security threats, or vulnerabilities. In contrast, other enterprises that have suffered security breaches might be reticent in disclosing information about the breaches for various reasons. Such as the fear of: attracting further attacks due to the publicity of disclosure; the consequences of bad publicity; or inviting costly litigations. The lack of reliable information and data about cybersecurity vulnerabilities and incidents is undesirable to the society. This is because it impedes the ability of consumers and enterprises to manage cybersecurity risk accurately, and consequently to misallocate resources in the society. Ignorance and misinformation during risk assessment causes wrong risk decisions and investments to be made. On the one hand, enterprises might deploy the wrong technology to address the wrong security problem. On the other hand, decision makers in enterprises and governments might overlook critical security risks because there is insufficient data available to provide insight to the nature and potential severity of the risks. Consequently, the society's welfare is worse off as a whole.

In the context of consumer IoT products, inadequate information disclosure and consumer awareness in the market also hinder the average consumer's ability to discern between products that offer better cybersecurity and those that do not. The fact that cybersecurity technology is embedded in the IoT products makes the technology unobservable to the average consumer. And this adds another incentive for unscrupulous enterprises to exploit the information asymmetry by marketing and pricing insecure IoT products as 'secure' ones.

Using the example of used car market, where it is common for unscrupulous dealers to market and price faulty cars (also known as 'lemons') disguised as good cars, Akerlof [AKE70] illustrated how inaccessibility to accurate information on product quality can distort prices and consequently drive down the overall quality of products traded in the market. In this context of asymmetric information, a 'hidden-action' problem occurs when the more well-informed parties in a market exploit their position

and cheat by acting unfairly to influence economic transactions, while this deception remain unobservable to others [AND01]. This problem prevents responsible manufacturers from selling their genuinely secure products at a commercially viable price, while bogus products are mis-sold at an inflated price. This consequently depresses the overall quality of products in the market [MOO11].

This problem of information asymmetry adds another disincentive that obstructs enterprises from introducing genuinely secure IoT products to the consumer market. Manufacturers could not charge a fair price for these products unless consumers could feel confident that they are presented with fair and trustworthy information necessary to differentiate these products from inferior ones. A potential solution is a product certification scheme that is independently monitored and governed by a trustworthy authority. Such schemes in the context of consumer IoT are explored and analysed in more detail in sections 3 and 4 of this report.

2.4.4 Network Effect (or Network Externality)

Network effect or network externality occurs when the perceived value of an innovation increases as more consumers adopt that innovation. For example, the usefulness of the Facebook website as a forum for social interaction and networking increases as more people uses the network.

Network externality has three properties [SHA98] that are important to understanding the economics underlying information security, namely:

1. *Positive feedback.* A technology that is subjected to network externality tends to exhibit long lead times followed by explosive growth. As the installed base grows, the eco-system or network becomes increasingly useful and this attracts even more users to the network. With this virtuous cycle of positive feedback, the technology or product eventually reaches a critical mass and takes over the market, while eliminating its rivals and forestalling new ones during the process.

2. *Diminishing average cost.* An information technology good tends to involve high sunk cost to develop. But after the first copy of the good has been

produced, the cost to replicate each subsequent copy tends to be relatively cheap and constant, with no natural limit for producing copies. This condition allows enterprises to price the good based on its proposed value rather than its cost.

3. *Cost of switching (lock-in effect).* The cost for users to switch from one technology to another could be prohibitive. This is because the user's information is already stored and processed using an eco-system of hardware and software. It could require considerable effort, time, and money to acquire new hardware and software, learn a new technology, and then convert and transfer the information based on one technology to another.

Shapiro and Varian [SHA98, pp. 24-27] observed that a market for goods with high sunk cost and diminishing average cost is sustainable only with two market structures, which are a market with:

1. a dominant firm in terms of sales volume. This enables the dominant firm to minimise its average cost through economy of scale and hence undercut its smaller competitors; and/or

2. different firms that differentiate themselves by producing different varieties of the same 'kind' of goods. This is the most common structure in markets for goods based on intellectual property, which include the market for IoT products.

These characteristics of network externalities offer an additional perspective to analysing why manufacturers of consumer IoT products have a strong incentive to neglect the cybersecurity of their products. IoT products exhibit network externality because an IoT solution becomes more useful to its users as more compatible devices from the same manufacturer are connected to form an integrated eco-system. For example, a smart home IoT solution would be more useful when its user could use a single application to centrally control and monitor multiple IoT devices (such as lightings, audio and video systems, closed-circuit televisions, household appliances, HVAC systems, door locks, etc) as an integrated eco-system. Hence

consumer IoT manufacturers have a strong interest in offering a large variety of compatible IoT devices with proprietary technology and to sell them in large volumes at low prices. This is necessary to: rapidly generate positive feedback and a critical mass of installed base before competitors do so; impose maximum switching cost on users to discourage switching technology; and lock in customers by entrenching them in an ecosystem of integrated products, services, and data. This business strategy inherently motivates business decision makers to hastily release sub-optimal designs into production to pre-empt competition, as well as to maximise the product lifecycle duration and revenue stream. There is always a next version or model in future to accommodate any residual design flaws.

From the perspective of a consumer IoT supply chain, we could also view the status quo of the supply chain as outcomes of network externality. The business model relies on component suppliers, OEMs, and ODMs working in collaboration to integrate their hardware and software components together to mass-produce a variety of consumer IoT goods. These components are essentially goods embedded with relatively expensive intellectual properties such as designs for semi-conductor chip, software, and hardware. The principle of diminishing average cost ensures that despite the high sunk cost to create the first unit of a component, the average cost per unit diminishes continuously with mass production. These dynamics incentivise incumbent enterprises in the supply chain to minimise development cost, maximise production volume, and to recycle existing designs for as long as possible. Hence there is little financial incentive in this business model to incorporate security technology into existing design unless it is inevitable.

Evidence of negative impact created by this widespread practice can be observed in both the Mirai botnet and the smart home IoT case examples. These cases revealed numerous existing consumer IoT devices inheriting similar security vulnerabilities because these devices are basically assembled using similar hardware and software components. This widespread practice not only entrenches the inherent security problems in the supply chain model but also discourages the adoption of new alternatives that are potentially more secure. Because these alternatives would lack economy of scale to be commercially viable in the first place.

2.4.5 Effects of Misaligned Incentives and Externalities on Cybersecurity

Human factors, poor design, and poor implementation are well-known causes of information security failure. These factors can be fundamentally attributed to a misalignment between the cause and the resulting harm. More specifically, the people who neglected security are often not the same ones who bear the brunt of security failures due to the negligence.

In his discourse [AND94], Anderson narrated a good example of misaligned incentives between those responsible for security and those who benefit from the protection. The courts in the UK traditionally regard banks as more trustworthy than bank customers. Hence, the burden of proof lies on bank customers should they become victims of banking fraud. Consequently, British banks could generally get away scot free from allegations of ATM fraud as it is almost impossible for a customer to prove the bank made a mistake. Anderson observed that this created a climate of moral hazard in which banks lack incentive to take systems security seriously and became complacent about assuring security. He contends that this in turn led to a long series of fraud occurrences and miscarriage of justice. Anderson examined several banking and ATM fraud cases and found that these incidents were not caused by the failure of security technology per se but by human factors. The security problems occurred due to flaws in implementation, installation, configuration, and management by the local banks.

In another example, in 2000, hackers commandeered computers connected to vulnerable university networks to attack and shut down Yahoo's website and other major web sites. The attacks materialised because the universities did not take the vulnerabilities seriously enough, as they are not legally liable for the damage caused by such attacks. Varian [VAR00] reflected on these incidents and concluded that the universities would have had a stronger incentive to improve their network security had they been required to bear some liability for the damages to third parties. This logically led him to suggest that liability for cybersecurity should be allocated to those who are best positioned to control the risks have appropriate incentives to do so.

The principle of misaligned incentive is apparent in the context leading to the DDoS attacks involving Mirai botnets. Both the manufacturers and consumers of those IoT

devices that were commandeered to launch the attack were not legally liable to the actual victims who bore the brunt of disruptions and economic loss caused by the biggest ever DDoS attack at that time. In fact, economic loss is generally not claimable in the courts of the UK, USA, and many European countries [BUS03], [GRI14], [SCO08]. Hence there is largely no legal duty to exercise reasonable care and no incentive for both manufacturers and consumers to pay attention to the cybersecurity of their IoT products. This disincentive is in addition to the other problems of network externality and information asymmetry that manufacturers and consumers of IoT products are also facing. In the case example involving smart home IoT products, the discovery of basic and simple vulnerabilities in all 16 samples of popular consumer IoT investigated by Shwartz and his team [SHW17] corroborates this argument.

The effect of misaligned incentive could also be discerned in the other two case examples involving smart toys and connected car. The IoT manufacturers in both cases would face legal sanction if their devices were exploited to invade personal privacy or to cause physical damage or injury. The less serious consequence of privacy violation may have led the toy manufacturer Genesis to accept a higher risk, which is reflected in its lukewarm response despite formal complaints and sanctions by authorities in the USA and various European countries. Genesis has since issued an inconsequential update [LOD15] to the reported vulnerability and (at the time of writing this report) has not yet revised its privacy policy on its website. This response contrasted starkly with the response from the car maker FCA, which among other measures, announced a recall of 1.4 million cars within 3 days after the vulnerability was publicly demonstrated.

This difference in behaviour seems to reflect the severity of potential liability underlying both sets of risk. The consequence of remotely disabling a car cruising along a motorway is likely to involve severe injuries and physical damages, as well as substantial legal liability and commercial damage to a reputable household brand. In contrast, hacking a US$60 talking toy to utter profanity or to eavesdrop private conversations would not cause direct physical damage or injury. The toy manufacturer has apparently regarded this risk as not severe enough justify a robust response or a product recall. The contrasting efforts made by Genesis and FCA

appear to commensurate with the perceived severity and potential liability associated with the different risks. This behaviour is logically consistent with the undesirable effect of misaligned incentive and it strongly suggests that liability for causing harm should be assigned such that those who are in a position to control the risks have appropriate incentives to do so.

It is worthwhile to recapitulate the main points uncovered so far about how failures in the current consumer market for IoT undermine cybersecurity. The status quo of the consumer IoT market imposes perverse and conflicting incentives that inhibit enterprises from investing in secure hardware or software for consumer IoT products. It is already an intrinsically complex and costly constraint to incorporate rudimentary security technology into a low-priced and miniature IoT product. Any additional complexity also tends to worsen the user experience and performance of the product. As I have evaluated earlier in section 2.2, the current market arrangement and commercial pressure on consumer IoT manufacturers is driving them to compete relentlessly on low price and on jostling to be the first to introduce novel and cheap products, never mind being compensated for the cost of embedding robust cybersecurity capabilities into the products. As Shapiro and Varian [SHA98, pp. 27] has pointed out, if it is not possible for a firm to compete on product differentiation, the next best strategy is to compete on volume and sell as many as possible to capture the market. Since the marginal cost of producing another copy of software for an IoT device is negligible, high sales volume will lower the average cost and hence also lower the selling price. While the higher sales volume will compensate for the lower profit margin per unit.

Meanwhile, consumers of IoT products are spoilt for choice in the market and they are most concerned about the price and utility of their gadgets. But this does not mean the consumers do not expect their IoT products be secure. They are already highly accustomed to their legal right to enjoy safe consumer goods and services, and hence the IoT consumers logically expect and assume that their IoT products are also safe and secure by default.

This market quandary strongly suggests that some form of extra-market intervention may be necessary to balance risk allocation in the market and to internalise the cost of cybersecurity.

2.4.6 Typical Justifications for Regulation

Apart from political motives, another main reason for governmental regulation is to remedy market failures, which produce outcomes and behaviour that are undesirable to public interest. Typical market-failure rationales for regulation are examined in discourses on regulation such as [BAL11], [BRE98], and [OGU94]. Among those justifications that are directly relevant to the context of this project include: information inadequacy (or information asymmetry), economic externality, public goods and moral hazard, and continuity and availability of service. All, except the last, of these justifications have been explored in this report. The continuity and availability of service refers to the situation where the free market could not provide adequate commercial incentive for enterprises to supply a service to the socially desired level of continuity and availability. A social policy may also require certain critical products and services (such as water, other utility supplies, and increasingly the Internet) to be generally available at least to a certain minimum standard. Although one may argue that intervention by the government to re-allocate market incentive is inefficient and unfair from the economic perspective, such regulation may still be justified in the context of ensuring desired social outcomes.

SECTION 3

3.1 Rationale for Regulating the Consumer IoT Market

The problems of free-riding and economic externalities, as evidenced by the observed market failures, indicate that the private sector alone is incapable of providing cybersecurity in the free market. Moreover, the fact that an insecure cyberspace also jeopardises the economy’s critical information infrastructure, which depends largely on the private sector to ensure connectivity, is another compelling reason for the government to intervene.

Any governmental intervention would have to address the underlying causes of market failure in order to fundamentally overcome the menace to the cybersecurity caused by consumer IoT. Nevertheless, the inherent characteristics of cyberspace poses an additional and unique set of challenges to the traditional paradigm of policy-making and enforcement. This section (section 3) examines the theoretical grounds of these issues in order to comprehend the insight necessary to formulate a plausible theoretical model of governmental intervention.

In addition to addressing market failure, the need to protect critical national infrastructure inevitably motivates modern governments to collaborate with the private sector in ensuring cybersecurity. For example, there are many organisations and companies within the UK's private and public sector that rely on the Internet to provide essential services to the country and its economy [HMG16]. Hence the UK government is duty-bound to work with the private sector to ensure that the country's critical national infrastructure and essential services are secure and resilient against cyberattack.

To successfully counteract the underlying causes that have been uncovered in this analysis, a theoretical model of regulatory intervention would need to achieve these outcomes:

- The allocation of risk to those who are able to manage the risk.
- The internalisation of the cost of intervention into IoT products.
- A global and level playing field that prevents free-riding and cheating by both consumers and manufacturers.
- The verifiable disclosure of information about security features of all consumer IoT products in the market.
- A global scheme for disclosure of information about new vulnerabilities and cyberattacks pertaining to consumer IoT products.

- The provision and enforcement of well-founded baseline cybersecurity specifications that must be met by all consumer IoT products in the market. These controls should include at least the basic security control principles (outlined in Table 4) which would prevent the common attacks exemplified by this case study.

3.2 Public Regulation and Self-Regulation

From a classic theoretical perspective, governments may remedy market externalities and information asymmetry with public regulation by mandating producers to meet minimum quality standards in order to counteract the underlying externalities. To inform consumers about the quality standard of products, a trusted agency could be tasked to award and administer quality score or quality marking that are to be disclosed alongside the products and services. Nevertheless, such schemes must also include safeguards against unintentional and counter-productive social outcomes. The schemes should include protection against abuse by influential participants to suppress competition and market entry, as well as against encouraging producers to do just enough to meet the minimum standard due to the erosion of opportunities for enterprises to seek comparative advantage through exceeding the minimum standard.

Increasingly in practice, public resources needed to negotiate and enforce these criteria in a modern globalised economy are prohibitively expensive and complex for a government to handle alone, especially in the current paradigm of lean and small governments. This is particularly so in the case of regulating IoT products, as controls must apply to a broad range of heterogeneous products and services that have different technical attributes and dependencies. Moreover, the measures must not impede the commercial viability of the products or services, and specific needs of consumers.

3.2.1 Limitations of Public Regulation

As already observed by public-policy scholars in discourses such as [BUT13] and [CAF12], there has been an impetus to privatise and internationalise governance. This is due to governments lacking the requisite technical expertise and resource, as

well as the need for flexibility to deal expeditiously with the increasing complexity and fast pace of modern regulatory tasks.

Traditional direct regulation by national policymakers has proven to be inadequate for regulating the complex and dynamic activities of a modern and globalised economy. As we have seen in section 2.2.1, advances in technology and globalisation has enabled goods, services, and information to readily transcend national borders in the modern global economy. This is problematic for the production of transnational public goods (such as deforestation, gas emission, as well as cybersecurity) for which international regulatory cooperation is needed, but lacking, to address the problems of tragedy of the commons and other economic externalities. Early examples of private initiative to fill this public policy gap created by the lack of international regulatory cooperation include the environmentally-friendly product certification schemes by the Forestry Stewardship Council (FSC) and the Marine Stewardship Council (MSC). Technology- and knowledge-based markets, including the consumer IoT market, are typically too fast-changing and knowledge-intensive for the mechanisms of traditional regulation to cope. Hence policymakers are compelled to rely on private parties, at least for defining implementation measures and technical specifications [CAF12]. These issues inevitably compel policymakers to rely on the expertise of private parties, who are better informed, skilled, resourced and positioned to manage the issues.

At the international level, these problems have exposed the inadequacy of working primarily through formal treaties and intergovernmental organisations (IGOs) to formulate, monitor and enforce mandatory public regulations on transnational economic actors. For example, the member states of ITU gathered at the World Conference on International Communications in 2012 to update and modernise the then 25-year-old 1988 International Telecommunication Regulations. The proposal included regulating Internet Protocol, spam emails, and network security. After 11 days of intensive debate and negotiation, the proposal was substantially watered down due to substantial political and ideological disagreements between member countries. Eventually, only 89 of the 193 members signed the treaty. In response to such deficiencies, there has been a global trend for governments to delegate regulatory responsibility to individual international private-sector organisations whose

areas of expertise are widely regarded as obvious forum for transnational regulation [ABB09a].

3.2.2 Characteristics of Self-regulation

Self-regulation occurs when private, regulated organisations undertake governance responsibilities that are traditionally allocated to government regulators. These responsibilities include setting standard, monitoring compliance, and enforcing compliance. Industry self-regulation typically involves a set of practices adopted voluntarily by organisations for complying with legal or normative obligations, such as internal compliance auditing, compliance management systems, and voluntary beyond-compliance commitments [SHO13]. Self-regulation and its counterpart public governmental regulation are two ends of a spectrum rather than two distinct forms of governance [PAG86]. Hence the degree of self-regulation in practice depends on its unique combination of legislative constraints, outsider participation in formulating and enforcing rules, and external control and accountability [OGU95].

Unlike traditional international treaties involving IGOs, most of these arrangements are governed by a combination of companies and industry groups whose own practices or those of supplier firms are the targets of regulation, non-governmental organisations (NGOs), and other civil society groups, including labour unions and socially responsible investors [CAF12]. In some arrangements, state governments and IGOs play a secondary or supporting role in the governance and operations of self-regulation. Other arrangements resemble public-private partnerships, with states or IGOs collaborating on roughly equal footing with private organisations. Some IGOs have also adopted principles of responsible business conduct to influence companies directly, as opposed to indirectly through the rules of governing states. For example, the United Nations (UN) through its Global Compact, and the OECD through its Guidelines for Multinational Enterprises [ORG09]. Many of these initiatives also engage private actors in the regulatory process.

Crucially, various studies [AYR95], [PAR02], [SHO08], [SHO13], [TOF11] have found that self-regulation is most likely to achieve its intended social outcome when:

- government regulators devout enough resources to monitor the scheme and sanction violators;

- government regulators refrain from using these resources to coerce companies to adopt self-regulatory measures; and

- there is consensus among regulators and regulated parties about the desired social outcome, although there may not be consensus on the method of achieving these objectives.

Enterprises in different industries have already been participating in self-regulatory and voluntary management schemes in their attempts to overcome information asymmetries in the market. These schemes are typically created in attempts to forestall potentially expensive regulation and legal liability due to economic externalities, or to address the inability of government to regulate a problem plaguing the industry. These schemes typically require participants to adopt specific processes and frameworks, but without imposing any performance obligation or verification of compliance by independent auditors. An example of such schemes in the IoT market is the Best Practice User Mark promoted by the IoTSF. The scheme was created to help manufacturers of IoT products to communicate publicly that they take seriously their security responsibilities as suppliers of IoT. Nevertheless, everybody can freely download the user-mark logo from the IoTSF website and use it to show that they have voluntarily implemented the latest IoT Security Compliance Framework provided by IoTSF. There is no requirement for membership or any independent governance and audit. Moreover, the IoTSF stated explicitly in their terms of use that the user-mark “is used voluntarily and offers no guarantee as to the user’s claim of using IoTSF guidance materials. Third parties should not rely on the mark as a statement of fact and are encouraged to conduct their own diligence to ensure their specific security needs are satisfied.” [IOT18]

Many studies [GUN95], [KIN00], [LEN03], [NAI97], [RIV04], [RIV06] have revealed no conclusive evidence that participants of such schemes performed better than non-participants. These studies also suggest that effective industry self-regulation is difficult to maintain without explicit governance oversight and sanctions for violators.

This argument is substantiated by Toffel's quantitative analysis [TOF05] of enterprises that have adopted the ISO 14001 (Environmental Management System) standard. The voluntary international standard is widely adopted by enterprises worldwide and it includes a robust compliance verification process by independent and certified auditors. The study revealed convincing evidence that the ISO 14001 standard not only attracts adopters with superior environmental performance, but its adoption leads to further performance improvement. This strongly implies that self-regulation schemes for addressing information asymmetries surrounding hard-to-observe management practices need to include robust independent verification mechanisms to be effective.

The findings in this section (3.2.2) indicate that there is still a relevant role, albeit a secondary one, for state governments and IGOs in ensuring successful self-government. Governments and IGOs should harness their prerogative influence and political networks to: promulgate and promote self-regulation schemes; facilitate negotiations and participation; and create rules to support the transparent governance and enforcement of the schemes. Also, Abbott and Snidal [ABB09b] observed that this secondary role could influence the balance of bargaining power between enterprises and NGOs, as well as enhance the enforcement and governance of a self-regulatory scheme; hence improving the scheme's effectiveness in achieving the desired social outcome. Moreover, the oversight and supervision of the government in the background adds another layer of safeguard against influential enterprises and NGOs from misusing private regulatory schemes as means to increase barrier to competition and capture the market. Hence, an appropriate level of governmental supervision and the use of international standards are important elements in a successful self-regulation scheme.

3.2.3 Role of International Standards in Self-Regulation

International standards play an important role in the self-regulation of a modern economy. There is already an existing range of international standards organisations, such as International Accounting Standards Board (IASB), International Organization for Standardization (ISO), and International Electrotechnical Commission (IEC), whose primary role is to standardise global business activities and processes using international norms that enterprises and other economic actors could voluntarily

adopt. These independent institutions, which do not accept governments as members, consist of thousands of international experts representing industries and other interested organisations working in hundreds of technical committees to develop and maintain technical standards. The ISO and IEC together account for about 85% of all international product and service standards [BUT13, pp. 5].

International standards are technical specifications for the design and performance characteristics of goods or services. The increased international inter-dependence due to the global integration of supply chains and product markets has intensified the need for common technical solutions to facilitate international operations and trade. Although international standards are voluntary, governments and IGOs often refer to these standards in their laws and regulations. For instance, Article 2.4 of The Agreement on Technical Barriers to Trade of the Uruguay Round trade negotiation (1987-1994) [WOR18] requires all member states of the World Trade Organisation (WTO) to use international standards as the technical basis for domestic laws and regulations, unless international standards are ineffective or inappropriate for the specified public policy objectives. The agreement (Article 2.6) also obliges member states to actively participate, within the limits of their resources, in the preparation of international standards for products for which they either have adopted, or expect to adopt, technical regulations. Consequently, the use of any standard that differs from the appropriate international standard could be challenged through the WTO dispute settlement mechanism as an unnecessary trade barrier and violation of international trade law.

3.3 Some Recent IoT Regulatory Initiatives

There are signs that governments have begun to pay attention and take regulatory actions to address failures in the consumer IoT market by enforcing minimum security requirements on IoT products. Below are some recent examples.

3.3.1 US Proposed Internet of Things (IOT) Cybersecurity Improvement Act

In 2017, the US Senate proposed the Internet of Things (IOT) Cybersecurity Improvement Act [WAR17], which seeks to impose minimum cybersecurity

requirements on federal government procurements of IoT products. The key features of bill would:

- require vendors selling IoT to federal government agencies to ensure the IoT products: do not contain any known security vulnerabilities or defects, can be patched securely from the vendors, use only industry standard protocols and technologies, and do not contain any hard-coded credentials;

- require the vendors to maintain mechanisms that disclose new vulnerabilities and promptly replace, repair, or patch the devices affected by these vulnerabilities in a secure manner;

- direct the Office of Management and Budget (OMB) to work with the National Institute of Standards and Technology (NIST) and the industry to develop alternative security requirements for IoT with exceptionally limited data processing and software functionality;

- allow alternative third-party product certification standards that provide equivalent or superior security requirements, subject verification by NIST; and

- exempt cybersecurity researchers engaging in good-faith research from liability under the Computer Fraud and Abuse Act, and the Digital Millennium Copyright Act (DMCA) when discovering vulnerabilities in accordance to certain vulnerability disclosure guidelines.

3.3.2 EU Proposed Cybersecurity Act

In May 2018, the European Council formally proposed the Cybersecurity Act [DIR17] which aims to enhance the cybersecurity capability of the European Union (EU) by harnessing national and Union efforts. The Act defines two main policies.

The first is to establish a European cybersecurity certification scheme that attest the compliance of eligible ICT products, services, and processes to pre-defined cybersecurity standards. It would involve the mutual recognition of certified products by different EU members and hence eliminate unnecessary fragmentation between

member states adopting separate standards. Consequently, the certification of a product in any member state would be recognised in all other member states. This would enable companies to reduce both the go-to-market duration and the administrative cost of certifying their products in multiple jurisdictions. The formal certification of product quality would enhance consumer confidence in ICT (including IoT) products and consequently promote the use and sale of more IoT. Technically, common standards would also ease the development of interoperable products and help to avoid the cybersecurity flaws prevalent in connecting systems with highly differentiated technologies. Recourse to the certification would be voluntary, unless otherwise provided in the EU or national legislation.

The second policy function is to strengthen and make permanent the role of the ENISA, which was originally created in 2004 as a temporary EU agency focused on network and information security. The agency's mandate has since been expanded in response to the growing challenges of cybersecurity. The ENISA currently organizes European cyber-crisis exercises to test resiliency capabilities, supports national Cyber Security Incident Response Teams (CSIRT), and provides a forum for sharing information and best practices. The new Act broadens the ENISA's mandate to play a greater role in Europe and internationally by: facilitating the implementation of the European Commission's recommendation on coordinated response to large-scale cybersecurity incidents and crises; assisting with the development of international standards; and supervising the Europe-wide cybersecurity certification framework for ICT devices.

3.3.3 UK Proposed Code of Practice for Security in Consumer IoT

In March 2018, the UK government published the 'Secure by Design: Improving the cyber security of consumer Internet of Things Report' [DEP18] after an extensive review involving the industry, academia, civil society, and international partners. The review aimed to understand the cybersecurity burden placed on consumers to buy, install, maintain, and dispose IoT products. It also investigated incentivising the consumer IoT industry to practise security-by-design principles, and using product certification to better inform consumers about the security quality of IoT products. The report also proposed a 'code of practice' targeted at IoT manufacturers, service

providers, developers, and retailers. The code consists of these 13 fundamental cybersecurity practices:

- No default passwords
- Implement a vulnerability disclosure policy
- Keep software updated
- Secure storage of sensitive data and credentials
- Communicate securely
- Minimize exposed attack surfaces
- Ensure software integrity
- Ensure personal data is protected
- Make systems resilient to outages
- Monitor system telemetry data
- Make it easy for consumers to delete personal data
- Make device installation and maintenance easy
- Validate input data

The report also revealed that the UK government is developing a proposal for a voluntary labelling scheme for consumer IoT products to aid consumer purchasing decisions and to facilitate consumer trust in companies. The UK government prefers to adopt a light-touch approach by urging the industry to self-regulate, while making clear it would not hesitate to regulate should self-regulation not happen promptly and effectively [DEP18, pp. 5].

In response to the report, UK's independent national standards body, British Standards Institution (BSI), launched a pilot BSI Kitemark Certification scheme for IoT security in May 2018. The BSI Kitemark is a British quality marking scheme for

products and services. The scheme is owned and operated by BSI. A Kitemark certification entails a stringent regime of assessment, testing, and audit by independent and certified third-parties. The Kitemark Certification for IoT security scheme attests the security level of IoT products and it incorporates the code of practice recommended in the Secure by Design report [DEP18] among its requirements for compliance [BRI18]. More specifically, the scheme requires the manufacturer to comply with the ISO 9001 (Quality management system) standards, and the IoT product to pass the:

- relevant product performance and safety tests;
- interoperability tests between devices and the Internet;
- initial penetration tests which scans for vulnerabilities and security flaws;
- regular monitoring and assessment comprising of functional/interoperability test, penetration tests; and
- regular Kitemark audit to review the penetration results in the context of the product, as well as to review what actions have been taken.

The scheme offers three types of BSI Kitemark for IoT, namely: Residential, Commercial, and Enhanced. The main difference between them being the requirement for increasing levels of penetration test as the risk of the device's application increases. The scheme will be voluntary and it is still being developed at the time of writing this report.

SECTION 4

4.1 A Plausible Model for Regulating Consumer IoT

Although these regulatory actions are positive contributions toward resolving the IoT security problem, they are insufficient because the fundamental socio-economic rationale that underlies the problem remains largely unaddressed. As evaluated in section 2.4.1, cybersecurity is a non-excludable good. Consequently, the menace of insecure IoT is omnipresent in the cyberspace due the borderless nature of the

Internet and the global ubiquity of IoT. Independent and limited regulatory actions at a national or regional level would be futile or at best yield limited success because Internet users in unregulated countries could still free-ride on the security provided by regulated countries. Moreover, hackers could readily shift their focus on easier targets among the IoT installed in the unregulated countries. Hence the success of any solution inevitably relies on the universality of its enforcement.

In fact, this rationale is also reflected in the existing European Conformity (CE) marking regulation for declaring conformance to the health, safety, and environmental protection requirements of many regulated consumer products traded in the Single Market. The CE markings required for these products are universally mandatory within the Single Market to ensure fair competition by holding all enterprises accountable to the same rules in the Single Market. Outside the Single Market, governments of many other countries also enforce similar quality-marking regulations on regulated products in their national markets to protect the environment, and the health and safety of consumers. Some examples include: China Compulsory Certificate (CCC) mark, Japanese Industrial Standards (JIS) mark, Joint Accreditation System of Australia and New Zealand (JAS-ANZ) mark, and Canadian Standards Association (CSA) mark.

Similarly, any regulation for attesting the cybersecurity of consumer IoT products should also be universally mandatory to prevent free-riding and to ensure fair competition in the globalised market. Based on this rationale, it is peculiar that the European cybersecurity certification framework proposed in the Cybersecurity Act is voluntary. A voluntary scheme is unlikely to improve cybersecurity as it still allows free-riding in the first place.

Nevertheless, in the long run, these initial regulations could still serve as a foundation for continuous improvement toward a more plausible, improved solution model that is robust and universal. This improved model should build on existing regulatory initiatives by addressing their inherent inadequacy. It inevitably entails state governments and IGOs to exploit their political partnership and governance expertise to facilitate (in partnership with the private sector) the negotiation, promulgation, and

transparent governance of a global framework for self-regulating the cybersecurity of consumer IoT.

4.1.1 International Cybersecurity Markings for Consumer IoT Products

As evaluated earlier, the international public good nature of cybersecurity inevitably entails international cooperation among governments and private sectors to bring their different expertise and capabilities to bear. To achieve this, governments could engage existing inter-governmental fora among IGOs such as the OECD, WTO, and UN Global Compact to collaborate with private sector representatives, such as NGOs, civil societies, and other interested parties to negotiate a global framework for attesting the cybersecurity of consumer IoT products. Based on this rationale and the findings from this project, I propose a more robust and improved regulatory model and framework that should (ideally) be universally mandatory and based on independent international standards or its equivalence within the rules of the WTO Agreement on Technical Barriers to Trade. The more universally the model can be enforced, the more successful the outcome will be. Because this model is mandatory, it is important that the affected private sectors play a leading role in shaping its content and in self-regulating the framework. Nevertheless, these participants must still work within the basic discipline and legal boundary that are pre-defined by governments to ensure universal compliance, fairness, and good governance.

Instead of creating from scratch, I propose that attempts should be made to use existing regulatory framework and resources that could be naturally exploited or extended to encompass IoT security. For example, regulations for declaration of consumer product safety already exist in many countries for many years and hence these regulations are already highly developed. For instance, the EU's CE marking scheme mandates many categories of consumer products traded in the European Single Market to conform with product safety standards referenced in various relevant EU directives. These products include toys, medical devices, and radio and telecommunications equipment. The scheme requires manufacturers to independently certify or self-certify conformance and to affix the CE mark to the regulated products to indicate certification. IoT security could be added to such regulations as a new category of product safety. This is in keeping with how the other product categories (such as telecommunication equipment and medical devices) had

been added to these regulations as new consumer products emerged with technological progress. For example, in the short run, the UK's BSI Kitemark for IoT scheme, as well as similar schemes in other Single Market countries, could be incorporated into the European cybersecurity certification scheme proposed in the to-be EU Cybersecurity Act. This framework could in turn be incorporated into the existing CE marking scheme with IoT as a new category of regulated product, hence enabling mandatory and mutually recognisable cybersecurity certification for all IoT products traded within the Single Market. In the long run, the different national standards that are incorporated in the European cybersecurity certification scheme could eventually be replaced with a suite of harmonised European (or international) standards and then integrated directly into the CE marking scheme.

Regarding international co-operation among governments, there are existing infrastructures, competencies, and fora among individual governments and IGOs that support the creation and running of product safety policies internationally. For example, the OECD Working Party on Consumer Product Safety has a mandate to promote the research and harmonisation of product safety policies. It already cooperates with other international bodies that do related work on product safety. These bodies include the International Consumer Product Safety Caucus (ICPSC), Organisation of American States and Asian-Pacific Economic Co-operation Forum. These resources should be exploited to negotiate and establish a consensus to extent the consumer product safety regulations in as many countries as possible to include the cybersecurity of IoT. Governments could use these existing networks and partnerships in IGOs to negotiate, agree, and promulgate the certification of IoT products to international cybersecurity standards as an integral part of their existing national regulations for consumer product safety. Legally binding instruments such as multi-lateral mutual recognition agreement (MRA) could be used to enable different jurisdictions to recognise each other's product certification.

For instance, the EU already relies on several international legal instruments that help facilitate international trading and movement of goods [EUR18]. They include:

- The full integration of the European Economic Area (EEA) and European Free Trade Association (EFTA) countries in the internal market through the EEA agreement.

- The alignment of the legislative system and infrastructure of EU candidate countries with those of the EU, as well as similar alignment of neighbouring countries through bilateral agreements on conformity assessment and acceptance of industrial products (ACAAs).

- Bilateral MRAs that enable the mutual recognition of conformity assessment, certificates, and markings with third countries without the need to harmonise legislations among participating countries. Thus, MRAs reduce the costs of testing and certification of good traded in the participating markets. The EU currently has MRAs with Australia, Canada, Israel, Japan, New Zealand, Switzerland, and USA.

- The WTO Agreement on Technical Barriers to Trade.

As revealed in section 3.3, the cybersecurity certification requirement is voluntary in the case of the proposed EU Cybersecurity Act and the forthcoming UK BSI Kitemark for IoT security scheme. Cybersecurity certification is mandatory only to IoT products purchased by the US government in the case of the proposed Internet of Things (IOT) Cybersecurity Improvement Act. The latter case assumes that the US government and consumers buy similar IoT products, and hence the enhanced security provided to government-purchased IoT products will spill over to the consumer market. This assumption is unrealistic as the IoT products purchased by government agencies are unlikely to be consumer-grade products. In any case, IoT products that fall outside these proposed requirements remain unregulated and hence contributors of market externalities. Moreover, the larger price gap between regulated and unregulated IoT products would make the potential gain from free-riding and cheating even more lucrative. This would in turn aggravate the economic externalities that these proposed regulations are hoping to overcome in the first place.

In contrast, I submit that imposing universal and mandatory cybersecurity certification on all consumer IoT in the entire global market would provide a level playing field for global competition and eliminate the economic reason for free-riding in the first place. An internationally recognised certification and cybersecurity marking scheme would provide product information transparency, which in turn reduces information asymmetry in the global market and enhances consumer trust. Obviously, the success of this improved model which I advocate relies on the universality, integrity, and truthfulness of the certification process. Hence the model needs to be primarily self-regulated by private sectors in order to foster a sense of ownership and to be responsive to market conditions, in conjunction with enough public regulation in the background to ensure transparency of policy, fair enforcement, good governance, sanction for violators, and cross-border cooperation.

4.1.2 Balancing Public Regulation with Private Self-Regulation

As I have evaluated earlier in section 3.2.2, a successful private self-regulation needs robust independent verification mechanisms. Hence individual governments and IGOs should play a secondary but essential supporting role by providing resources and competences that are the prerogative of sovereign governments. For examples: enacting national legislation to provide legal legitimacy, including power to recall products and sanction violators; negotiating and signing international legal instruments such as conventions, MRAs, and memoranda of understanding; as well as sharing resources and expertise in policy-making and good governance.

There are several rationales underlying the need for private sectors to play a leading role in defining and operating this improved framework. The private sectors are primary participations in a free market, hence they are in the best position to define or update market rules to reflect commercial needs, albeit within the policy constraints of achieving the desired social outcome. These participants would be more likely to comply with the rules which they have helped to define. Crucially, private sectors need to internalise the cost of market failures, which is the purpose of regulatory intervention in the first place. This cost will percolate through the supply chain in the form of prices, which in turn influence economic decisions made by enterprises and consumers in the market.

To ensure commercial and political neutrality, as well as wide representations from the affected private sectors, the baseline cybersecurity standards of consumer IoT should be negotiated and defined by an appropriate independent standard setting organisation (SSO), such as the ISO or the IEC. This market independence also allows free competition among the SSOs, so that any better competitor would be free to assume the role in future should an incumbent SSO's performance fall short of expectation.

4.1.3 Using International Standards to Address Market Externalities

There is currently no international standard for the cybersecurity of consumer IoT. The closest such document is the Special Publication 800-183 ('Networks of Things') [VOA16] published by the NIST. However, it is primarily a description of IoT architecture and terminology and hence more useful as a reference for architecture analysis than as a specification standard. The Common Criteria for Information Technology Security Evaluation (also known as Common Criteria) is an international standard (ISO/IEC 15408, Evaluation criteria for IT security) for certifying ICT products with security functionality. This scheme evaluates the information security of ICT products by having them tested and certified by a network of approved laboratories. The certificate is then recognised by all participating countries mainly for the purposes of government procurement. The testing and certification process for the Common Criteria is highly bureaucratic and expensive to implement. Technically and economically, it is unnecessarily excessive to apply the Common Criteria directly to low-cost consumer IoT products. Moreover, the scheme is not fool proof as it can be overly focused on the technical aspects of design and overlook human and operational aspects [AND08, pp. 877]. Anderson [AND08, pp. 876-880] also narrated how the evaluation process of the Common Criteria scheme had been manipulated and mismanaged.

As with any trust-based scheme, its success hinges on the robustness of its governance and the integrity of those who administer it. Hence, a successful product certification scheme comes with a cost because a robust infrastructure and governance system must be implemented and maintained to govern the integrity and compliance of the scheme. When added to the product price, this extra cost represents the internalised cost of providing the product security.

The appropriate international standards should provide baseline security controls for IoT based on well-founded security principles. As I have evaluated in section 2.3, most (if not all) of the best practices for IoT security are already publicly documented in a myriad of existing IoT best practice guidelines, thirty of which are listed in the Appendix. These guidelines should be used as reference during the development of the international standards to avoid duplicate work and to expediate the process. These standards should also include the six security controls in identified in Table 4 ('Summary of some basic security controls principles.'), which are the basic security principles that would forestall the attacks exemplified in the case examples.

For the international IoT security standards to be universally useful and enduring, they should concentrate on specifying the desired security outcome based on well-founded and fundamental principles of computer security, rather than defining detailed technical specifications for specific use cases of IoT. It would be absurd and infeasible to foresee and predict all potential usages of IoT, let alone to assemble the massive resources and energy needed to negotiate, agree, and prepare technical standards for every usage scenario. In contrast, the well-founded principles of security controls are time-honoured and generally agnostic to evolving technology and applications. For example, I have discussed in section 2.3 that the security control principles elucidated by Saltzer and Schroeder in 1975 [SAL75] are still largely relevant to today's computing systems, including IoT. They were relevant to mainframe computers of the 1970s, just as (if not more) relevant to modern connected computers (including IoT), and should remain relevant to the next generation of computer systems. Such as quantum computers, or an ingestible smart pill embedded with sensor, camera, tracker, and microchip for monitoring physiological status and activities within the body [MIN18].

The proposed improved model should also include international standards that define an effective and integrated eco-system for disclosing vulnerabilities responsibly and for promptly repairing defective software or hardware. Nevertheless, the aim should seek not to replace but to exploit and enhance the extensive international networks and partnerships that have already been established among public and private sectors. For example, many countries already have national Computer Emergency Readiness Teams (CERT) which, among other mandates, cooperate with each other

to receive, monitor, manage, and share reports on computer vulnerabilities and incidents. There are also public-private sector collaborations, such as the EU's ENISA, and UK's Cyber Security Information Sharing Partnership (CISP). The CISP is a partnership between the industry and the UK government to share cyber-threat information in real-time in a secure and confidential environment.

There are already two international standards, ISO/IEC 29147 (Vulnerability disclosure) and ISO/IEC 30111 (Vulnerability handling processes), that specify good vulnerability response practices for vendors. The ISO/IEC 29147 describes an outward-facing vulnerability disclosure process, and the ISO/IEC 30111 addresses the internal processes associated with vendor vulnerability response. National CERTs and manufacturers should adopt these standards, as well as create new ones via international SSOs where necessary, to globally harmonise the process and information formats of the vulnerability disclosure systems. This helps to ensure that information gathered and shared are relevant, accurate, consistent, and comparable. As I have discussed in section 2.4.3, different enterprises have different commercial motivations or reservations when disclosing information about security vulnerabilities and incidents. Consequently, these disclosures are likely to be biased, incomplete, and inconsistent if left unregulated. The universal conformance to international standards for vulnerability disclosure and handling would help improve the quality of disclosed information and make them more consistent and relevant. High-quality information not only enables effective and efficient problem resolution but serves as reliable source data for future data aggregation and analysis. The timely availability of accurate and relevant information to decision makers in the market is necessary to fundamentally address the information asymmetry problem of inadequate information about cybersecurity vulnerabilities and incidents. Accurate, timely, consistent, and relevant information enables more accurate management and allocation of security risk at all levels, from government agencies, businesses, insurers, to consumers.

Besides addressing the problem of information asymmetry by improving the quality and quantity of cybersecurity information in the market, the use of common standards in the proposed model would also reverse the existing network effect from a negative externality to a positive one. Instead of the current trend of creating many proprietary technologies in attempts by fiercely competing manufacturers to capture fragments of

the IoT market, the common standards provide a commercial incentive for manufacturers to create system components that are compatible and inter-operable with each other. The principle of network theory ensures that a large network of compatible and secure IoT eco-systems would intrinsically offer more potentially useful applications than a patchwork of independent proprietary IoT eco-systems.

Enterprises should be free to supplement this baseline with additional and stricter security feature in order to differentiate their IoT products and services. However, enterprises can only influence the content of an international standard via their official representations in the SSO and within the standard development rules of the SSO. The use of open standards-setting process by international SSOs might seem less efficient and take more time because of the need for consensus among the participants, whom may own proprietary technologies or have competing commercial interests. However, the transparent process reduces the possibility of participants misusing the process as a strategy to raise competition barrier. In addition, the oversight and involvement of the government in the background serves as an added safeguard against such policy capture. This is because the government ultimately needs to refer to these standards when formalising the regulation. A more detailed treatment regarding safeguarding standards-setting processes from anti-competitive influence is available in [LIN12].

4.1.4 Being Realistic about the Bureaucracy of Standards Setting

If the duration of developing a full-fledged international standard is too prohibitive, a Publicly Available Specification (PAS) could be developed as interim standard. The PAS is a fast-tracked standardisation document that could be developed in 9 to 12 months for a sponsoring organisation to meet an urgent market need. They are prepared by a steering group of stakeholders selected from the relevant fields and led by the SSO. A PAS published by ISO has a maximum life of six years, after which they can be transformed into an international standard or withdrawn.

Nevertheless, it is necessary to be realistic and recognise that the negotiation and preparation of formal instruments such as a treaty, international standard, or PAS entail rigorous and formal procedures for good reasons. These procedures are established not to deliberately frustrate the process but to ensure the integrity and

legality of the eventually agreed instrument, as well as to prevent undesired complications and disputes caused by an ill-prepared document. The rigor of the process is designed to reflect the importance, complexity, and scope of the underlying instrument, as well as the severity of consequences should things go wrong after its implementation. In any decision-making process that is based on the consensus of many participants, it is inevitable that significant amount of time and energy would be required to negotiate and agree on a compromise that is unanimously acceptable. The greater the divergence of views among the participants, then the more tedious the negotiation will be, and the more diluted the final compromised outcome will be from the original proposal. Hence, it is necessary to be realistic about these constraints when defining the scope, objective, and expectation of new international standards for IoT security, or any other formal instrument.

As we have already learnt, the fundamental security principles for IoT are well-founded and understood. Moreover, these principles are already included in majority of the thirty IoT security guidelines that has been identified in section 2.3. These facts suggest that consensus about the baseline requirements for IoT security already exist within the market. The problem is not so much the lack of consensus on the baseline requirements but the lack of economic incentive for the industry to implement them due to the market externalities that I have evaluated in this report. Hence, this pre-existing consensus augurs well for the expeditious agreement and inclusion of the baseline principles into a new international standard.

4.2 Conclusion

In this discourse I contend that the global menace to cybersecurity caused by the widespread use of insecure consumer IoT is a manifestation of a combination of the public good nature of cybersecurity, consumer's perception of cybersecurity, and socio-economic factors.

Because of the human's innate cognitive bias when making intuitive judgements (including judgements about cybersecurity) under uncertain conditions, consumers instinctively tend to be indifferent to cybersecurity. Consequently, they are unwilling

to pay for more-secure IoT products even though they still expect these products to be secure. Instead, the consumers tend to focus on the certainty of low price and high utility when purchasing IoT products.

The public good characteristics of cybersecurity incentivise consumers and manufacturers to cheat and free-ride on the cybersecurity provided and paid for by others. Inadequate information about the security quality and vulnerability of IoT products encourages unfair trading and mismanagement of security risk in the market. Moreover, the consumers and manufacturers who neglect cybersecurity are often not the same people who bear the brunt of security breaches caused by the negligence. These misaligned consumer expectations, economic incentives, and legal liabilities, in conjunction with modern technology and economic globalisation, has led to a supply chain model that is fiercely price-competitive and highly tuned to maximising division of labour (to minimise cost).

Securing IoT products entail the same basic computer security principles as those needed for securing conventional computers. These basic technological principles are well-founded and time-honoured. In fact, these principles have already been incorporated into many existing IoT security guidelines created by both the public and private sectors in attempts to address the IoT security problem. The outcome of these initiatives has been largely inconsequential, because these technical solutions, while necessary, are not sufficient to address the fundamental causes of the problem. A theoretical model that claims to resolve this security quandary should fundamentally address the underlying causes I have identified in this report. More specifically, a plausible solution model needs to fulfil these basic criteria:

- Allocation of risk to those who can manage the risk.
- Internalisation of the cost of cybersecurity into IoT products.
- Provision of a global and level playing field that prevents free-riding and cheating by both consumers and manufacturers.

- Global disclosure of verifiable information about security features of consumer IoT products in the global market.

- Global responsible disclosure of appropriate, consistent information about new vulnerabilities and security incidents pertaining to consumer IoT.

- Mandatory and well-founded baseline cybersecurity specifications that must be met by all consumer IoT products in the global market, including the requirement to promptly repair newly-discovered vulnerabilities.

Based on this insight, I advocate and recommend an improved solution model that incorporates mandatory and universal conformance to well-founded baseline cybersecurity principles for IoT products traded in the global consumer market. I submit that imposing universal and mandatory cybersecurity certification on all IoT products traded in the global consumer market would provide a level playing field for competition and eliminate the economic reason for free-riding in the first place. A global framework for internationally recognised certifications and cybersecurity markings that is based on international standards would provide information transparency about the security quality of IoT products. This would reduce information asymmetry about the cybersecurity of IoT products in the market and enhance consumer trust.

Obviously, the success of this model relies on its ability to fundamentality address the underlying externalities, as well as on the universality, integrity, and truthfulness of the certification process. Hence the model needs to be primarily self-regulated by private sectors in order to internalise the social cost of cybersecurity into IoT products, foster a sense of ownership, and be responsive to market conditions. At the same time, there must also be enough public regulation in the background to ensure transparency of policy, fair enforcement, robust governance, sanction for violators, and cross-border cooperation.

The compliance cost that the regulation imposes on the society should not outweigh the social benefit generated by the intervention. Hence, to minimise the social cost of administering the regulation, attempts should be made to exploit existing regulatory

framework and resources that could be naturally utilised or extended to encompass IoT security. A natural and logical candidate would be the regulations for the declaration of consumer product safety, which already exist in many countries for many years and hence these regulations are already highly developed. A prominent example is the mandatory CE marking regulation that applies to many consumer products traded in the European Single Market.

The proposed model should also include a more global, standardised, and integrated eco-system for responsible disclosure and sharing of vulnerability information, and for promptly repairing known IoT defects. Timely availability of accurate, consistent, and relevant information to decision makers in the global market is necessary to fundamentally address the problem regarding inadequate public information about cybersecurity vulnerabilities and incidents. The improved quality and availability of cybersecurity information enables more accurate management and allocation of security risk, as well as better decision-making and policy-making.

With these findings, the project objectives as defined in section 1.2 have been met. Nevertheless, the findings have also accentuated new challenges where further future research and debate are required. The success of the proposed solution hinges on the international adherence to a global framework for attesting the cybersecurity of IoT products based on international standards. Unlike traditional public good (such as pollution or physical security) which can be reasonably regulated nationally or regionally, cybersecurity is entirely virtual and borderless in nature and hence it can only be managed holistically. It is futile to resist this reality and to attempt to regulate cybersecurity nationally or regionally using traditional approaches, which are evident in the proposed regulations examined in section 3.3. Future research and debate could explore new and creative ways: to change the traditional mindset of academics, policymakers, managers, and consumers so that they understand and accept the unique borderless nature of cyberspace; and to educate these decision makers to cooperate internationally in an effective way that is conducive to the new reality of the Internet era.

Bibliography / Reference List

(107 items, all of which are cited in this report.)

[ABB09a] K. W. Abbott and D. Snidal, “Strengthening International Regulation through Transmittal New Governance: Overcoming the Orchestration Deficit,” *Vanderbilt Journal of Transnational Law*, vol. 42, pp. 501–578, 2009.

[ABB09b] K. W. Abbott and D. Snidal, “The Governance Triangle: Regulatory Standards Institutions and the Shadow of the State,” in *The Politics of Global Regulation*, Princeton, New Jersey: Princeton University Press, 2009, pp. 44–88.

[ADA97] J. Adams, “Cars, cholera and cows: virtual risk and the management of uncertainty,” *Science Progress*, vol. 80, no. 3, pp. 253–272, 1997.

[AKA18] Akamai, “State of the Internet / Security Q4 2017 Report,” Akamai Technologies Inc., Cambridge, Massachusetts, Security report Volume 3, Number 4, Feb. 2018.

[AKE70] G. A. Akerlof, “The Market for ‘Lemons’: Quality Uncertainty and the Market Mechanism,” *The Quarterly Journal of Economics*, vol. 84, no. 3, pp. 488–500, Aug. 1970.

[ALB17] R. Albergotti, “Jawbone to Be Liquidated as Rahman Moves to Health Startup,” *The Information*, 06-Jul-2017. [Online]. Available: https://www.theinformation.com/articles/jawbone-to-be-liquidated-as-rahman-moves-to-health-startup. [Accessed: 12-Jun-2018].

[AND01] R. Anderson, “Why information security is hard - an economic perspective,” in *Proceedings of the 17th Annual Computer Security Applications Conference*, New Orleans, LA, USA, 2001, pp. 358–365.

[AND08] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed. Indianapolis, Indiana, USA: Wiley Publishing, 2008.

[AND94] R. J. Anderson, “Why Cryptosystems Fail,” *Communications of the ACM*, vol. 37, no. 11, pp. 32–40, Nov. 1994.

[ANN16] Anna-senpai, “[FREE] World’s Largest Net:Mirai Botnet, Client, Echo Loader, CNC source code release,” *Hack Forums*, 30-Sep-2016. [Online]. Available: https://hackforums.net/showthread.php?tid=5420472. [Accessed: 02-Jun-2018].

[ANT17] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, and Z. Durumeric, “Understanding the Mirai Botnet,” in *Proceedings of the 26th USENIX Security Symposium*, Vancouver, BC, Canada, 2017, pp. 1093–1110.

[AYR95] I. Ayres and J. Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate*. Oxford, New York: Oxford University Press, 1995.

[BAL11] R. Baldwin, M. Cave, and M. Lodge, “Why Regulate?,” in *Understanding Regulation: Theory, Strategy, and Practice*, Oxford: Oxford University Press, 2011, pp. 16–24.

[BAU17] H. Bauer, O. Burkacky, and C. Knochenhauer, “Security in the Internet of Things,” *McKinsey and Company*, May-2017. [Online]. Available: https://www.mckinsey.com/industries/semiconductors/our-insights/security-in-the-internet-of-things. [Accessed: 10-Jun-2018].

[BBC15] BBC, “What did she say?! Talking doll Cayla is hacked,” *BBC News*, 30-Jan-2015. [Online]. Available: https://www.bbc.co.uk/news/av/technology-31059893/what-did-she-say-talking-doll-cayla-is-hacked. [Accessed: 30-May-2018].

[BRA17] T. Bradshaw, “Jawbone reaches end of the road as it goes into liquidation,” *Financial Times*, 07-Jul-2017. [Online]. Available: https://www.ft.com/content/c146f144-62ad-11e7-8814-0ac7eb84e5f1. [Accessed: 12-Jun-2018].

[BRE98] S. Breyer, “Typical Justifications for Regulation,” in *A Reader on Regulation*, R. Baldwin, C. Scott, and C. Hood, Eds. Oxford: Oxford University Press, 1998, pp. 59–92.

[BRI18] British Standards Institution (BSI), “BSI launches Kitemark for Internet of Things devices,” *BSI*, 15-May-2018. [Online]. Available: https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2018/may/bsi-launches-kitemark-for-internet-of-things-devices/. [Accessed: 13-Aug-2018].

[BUS03] M. Bussani, V. V. Palmer, and F. Parisi, “Liability for Pure Financial Loss in Europe: An Economic Restatement,” *American Journal of Comparative Law*, vol. 51, pp. 113–162, 2003.

[BUT13] T. Buthe, *The new global rulers: the privatization of regulation in the world economy*. Princeton: Princeton University Press, 2013.

[CAF12] F. Cafaggi and A. Renda, “Public and Private Regulation: Mapping the Labyrinth,” Centre for European Policy Studies, Brussels, Belgium, CEPS Working Document No. 370, Oct. 2012.

[CAR78] J. S. Carroll, “The effect of imagining an event on expectations for the event: An interpretation in terms of the availability heuristic,” *Journal of Experimental Social Psychology*, vol. 14, no. 1, pp. 88–96, Jan. 1978.

[CBI17] CB Insights, “Why Do So Many Hardware Startups Fail?,” *CB Insights Research*, 27-Sep-2017. [Online]. Available: https://www.cbinsights.com/research/report/hardware-startups-failure-success/. [Accessed: 08-Aug-2018].

[COR96] R. Cornes and T. Sandler, *The Theory of Externalities, Public Goods, and Club Goods*, 2nd ed. Cambridge, UK: Cambridge University Press, 1996.

[DEP18] Department for Digital, Culture, Media and Sport (DCMS), “Secure by Design: Improving the cyber security of consumer Internet of Things Report,” The UK Government, London, UK, Review report, Mar. 2018.

[DIR17] Directorate-General for Communications Networks, Content and Technology, “Proposal for a Regulation of the European Parliament and of the Council on ENISA, the ‘EU Cybersecurity Agency’, and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act''),” European Commission, Brussels, Belgium, Proposal for a regulation COM(2017) 477 final, Sep. 2017.

[DON18] M. De Donno, N. Dragoni, A. Giaretta, and A. Spognardi, “DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation,” *Security and Communication Networks*, vol. 2018 Article 7178164, pp. 1–30, 2018.

[ELK18] M. Elkin, “Crime in England and Wales: year ending March 2018,” *Office for National Statistics*, 19-Jul-2018. [Online]. Available: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2018. [Accessed: 09-Aug-2018].

[ETH16] D. Etherington, “Large DDoS attacks cause outages at Twitter, Spotify, and other sites,” *TechCrunch*, 21-Oct-2016. [Online]. Available: http://social.techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/. [Accessed: 10-Jul-2018].

[EUR18] European Commission, “International aspects of the Single Market,” *European Commission*, 17-Aug-2018. [Online]. Available:

https://ec.europa.eu/growth/single-market/goods/international-aspects_en. [Accessed: 18-Aug-2018].

[FIN00] M. L. Finucane, A. Alhakami, P. Slovic, and S. M. Johnson, “The Affect Heuristic in Judgments of Risks and Benefits,” *Journal of Behavioral Decision Making*, vol. 13, no. 1, pp. 1–17, Jan. 2000.

[FOR16] Forbrukerrådet, “#Toyfail An analysis of Consumer and Privacy Issues in Three Internet-Connected Toys,” Norwegian Consumer Council, Oslo, Consumer report, Dec. 2016.

[FOW15] G. A. Fowler, “Talking Toys Are Getting Smarter: Should We Be Worried?,” *Wall Street Journal Online*, 17-Dec-2015. [Online]. Available: https://www.wsj.com/articles/talking-toys-are-getting-smarter-should-we-be-worried-1450378215. [Accessed: 15-Aug-2018].

[GAR17] Gartner, “Internet of Things endpoint spending worldwide by category from 2014 to 2020 (in billion U.S. dollars),” *Statista*, Feb-2017. [Online]. Available: https://www-statista-com.ezproxy01.rhul.ac.uk/statistics/485252/iot-endpoint-spending-by-category-worldwide/. [Accessed: 10-Jun-2018].

[GOO16] D. Goodin, “Record-breaking DDoS reportedly delivered by >145k hacked cameras,” *Ars Technica*, 29-Sep-2016. [Online]. Available: https://arstechnica.com/information-technology/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/. [Accessed: 10-Jul-2018].

[GRE15] A. Greenberg, “Hackers Remotely Kill a Jeep on the Highway - With Me in It,” *WIRED*, 21-Jul-2015. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. [Accessed: 31-May-2018].

[GRI14] J. Griffin, “Pure Economic Loss: Out of Negligence and into the Unknown,” *Oxford University Undergraduate Law Journal*, vol. 2014, pp. 44–54, 2014.

[GUN95] N. Gunningham, “Environment, Self-Regulation, and the Chemical Industry: Assessing Responsible Care,” *Law & Policy*, vol. 17, no. 1, pp. 57–109, Jan. 1995.

[HAR68] G. Hardin, “The Tragedy of the Commons,” *Science*, vol. 162, no. 3859, pp. 1243–1248, Dec. 1968.

[HMG16] HM Government, “National Cyber Security Strategy 2016 to 2021,” Her Majesty’s Government, London, UK, Policy paper, Nov. 2016.

[IOT18] IoT Security Foundation (IoTSF), “Best Practice User Mark FAQ and Terms of Use,” *IoT Security Foundation*. [Online]. Available: https://www.iotsecurityfoundation.org/. [Accessed: 10-Aug-2018].

[ISA15a] ISACA, “2015 ISACA IT Risk/Reward Barometer - US Consumer Results,” Information Systems Audit and Control Association, Schaumburg, Illinois, Survey results, Oct. 2015.

[ISA15b] ISACA, “2015 ISACA IT Risk/Reward Barometer - UK Consumer Results,” Information Systems Audit and Control Association, Schaumburg, Illinois, Survey results, Oct. 2015.

[ISA15c] ISACA, “2015 ISACA IT Risk/Reward Barometer - Australia Consumer Results,” Information Systems Audit and Control Association, Schaumburg, Illinois, Survey results, Oct. 2015.

[KAH02] D. Kahneman and S. Frederick, “Representativeness Revisited: Attribute Substitution in Intuitive Judgment,” in *Heuristics and Biases: The Psychology of Intuitive Judgment*, D. Griffin, D. Kahneman, and T. Gilovich, Eds. Cambridge: Cambridge University Press, 2002, pp. 49–81.

[KAH03] D. Kahneman, “Maps of Bounded Rationality: Psychology for Behavioral Economics,” *American Economic Review*, vol. 93, no. 5, pp. 1449–1475, Dec. 2003.

[KAH11] D. Kahneman, *Thinking, fast and slow*. London: Allen Lane, 2011.

[KAH79] D. Kahneman and A. Tversky, “Prospect Theory: An Analysis of Decision under Risk,” *Econometrica*, vol. 47, no. 2, pp. 263–291, 1979.

[KAS18] Kaspersky Lab, “Most Commonly Encountered Cyber Threats According to Global Internet Users as of 2nd Half 2017,” *Statista*, Apr-2018. [Online]. Available: https://www.statista.com/statistics/767612/most-common-cyber-threats-worldwide/. [Accessed: 18-Jun-2018].

[KIM84] O. Kim and M. Walker, “The free rider problem: Experimental evidence,” *Public Choice*, vol. 43, no. 1, pp. 3–24, Jan. 1984.

[KIN00] A. A. King and M. J. Lenox, “Industry Self-Regulation Without Sanctions: The Chemical Industry’s Responsible Care Program,” *Academy of Management Journal*, vol. 43, no. 4, pp. 698–716, Aug. 2000.

[KOL17] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, “DDoS in the IoT: Mirai and Other Botnets,” *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[LEN03] M. J. Lenox and J. Nash, “Industry self-regulation and adverse selection: a comparison across four trade association programs,” *Business Strategy and the Environment*, vol. 12, no. 6, pp. 343–356, Nov. 2003.

[LIN12] M. A. Lindsay, “Safeguarding the Standard: Standards Organizations, Patent Hold-up, and other Forms of Capture,” *The Antitrust Bulletin*, vol. 57, no. 1, pp. 17–57, Mar. 2012.

[LLO80] W. F. Lloyd, “W. F. Lloyd on the Checks to Population,” *Population and Development Review*, vol. 6, no. 3, pp. 473–496, 1980.

[LOD15] D. Lodge, “My Friend Cayla. Updated app; Updated security fails. How to make her swear (again!),” *Pen Test Partners*, 22-Jun-2015. [Online]. Available: https://www.pentestpartners.com/security-blog/my-friend-cayla-updated-app-updated-security-fails-how-to-make-her-swear-again/. [Accessed: 30-May-2018].

[LUI12] E. Luiijf, “Understanding Cyber Threats and Vulnerabilities,” in *Critical Infrastructure Protection*, Springer, Berlin, Heidelberg, 2012, pp. 52–67.

[MAN16] S. Mansfield-Devine, “DDoS goes mainstream: how headline-grabbing attacks could make this threat an organisation’s biggest nightmare,” *Network Security*, vol. 2016, no. 11, pp. 7–13, Nov. 2016.

[MIL15] C. Miller and C. Valasek, “Remote Exploitation of an Unaltered Passenger Vehicle,” presented at the Black Hat USA 2015, Las Vegas, Nevada, 2015.

[MIN18] Mind Commerce, “Smart Pill Delivery, Monitoring, and Diagnostics: IoT enabled Medicine and 3D Printing enabled Drug Delivery 2018 – 2023,” Mind Commerce, Seattle, Washington, Market report, Apr. 2018.

[MOO11] T. Moore and R. Anderson, “Economics and Internet Security: a Survey of Recent Analytical, Empirical and Behavioral Research,” Harvard Computer Science Group, Harvard University, Cambridge, Massachusetts, Technical report TR-03-11, 2011.

[MOR05] C. K. Morewedge, D. T. Gilbert, and T. D. Wilson, “The Least Likely of Times: How Remembering the Past Biases Forecasts of the Future,” *Psychological Science*, vol. 16, no. 8, pp. 626–630, Aug. 2005.

[MUN15] K. Munro, “Making children’s toys swear,” *Pen Test Partners*, 23-Jan-2015. [Online]. Available: https://www.pentestpartners.com/security-blog/making-childrens-toys-swear/. [Accessed: 30-May-2018].

[NAI97] J. Naimon and K. Shastri, “Do Environmental Management Programs Improve Environmental Performance Trends? A study of Standard & Poors 500 Companies,” *Environmental Quality Management*, vol. 7, no. 1, pp. 81–90, Sep. 1997.

[OGU94] A. I. Ogus, “Public Interest Grounds for Regulation,” in *Regulation : Legal Form and Economic Theory*, 1st ed., London: Hart Publishing, 1994, pp. 29–54.

[OGU95] A. I. Ogus, “Rethinking Self-Regulation,” *Oxford Journal of Legal Studies*, vol. 15, no. 1, pp. 97–108, Mar. 1995.

[ORG09] Organisation for Economic Co-operation and Development, *OECD Guidelines for Multinational Enterprises*. Paris: OECD Publishing, 2009.

[ORG92] Organisation for Economic Co-operation and Development, “OECD Guidelines for the Security of Information Systems, 1992 - OECD,” *OECD.org*, Nov-1992. [Online]. Available: http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm. [Accessed: 27-Jun-2018].

[OXF18] Oxford University Press, “Internet, n.,” *OED Online*, Jun-2018. [Online]. Available: http://www.oed.com/view/Entry/248411. [Accessed: 15-Aug-2018].

[PAG86] A. C. Page, “Self-Regulation: The Constitutional Dimension,” *Modern Law Review*, vol. 49, no. 2, pp. 141–167, 1986.

[PAR02] C. Parker, *The Open Corporation: Effective Self-regulation and Democracy*. Cambridge: Cambridge University Press, 2002.

[PIG32] A. C. Pigou, *The Economics of Welfare*, 4th ed. London: Macmillan and Co., 1932.

[PON15] Ponemon Institute, “2015 Cost of Cyber Crime Study: United Kingdom,” Ponemon Institute LLC, Traverse City, Michigan, Research report, Oct. 2015.

[PON16] Ponemon Institute, “Cost of Denial of Services Attacks,” Ponemon Institute LLC, Traverse City, Michigan, Research report, May 2016.

[RIV04] J. Rivera and P. D. Leon, “Is Greener Whiter? Voluntary Environmental Performance of Western Ski Areas,” *Policy Studies Journal*, vol. 32, no. 3, pp. 417–437, Aug. 2004.

[RIV06] J. Rivera, P. D. Leon, and C. Koerber, “Is Greener Whiter Yet? The Sustainable Slopes Program after Five Years,” *Policy Studies Journal*, vol. 34, no. 2, pp. 195–221, May 2006.

[ROS66] D. Rosenhan and S. Messick, “Affect and expectation,” *Journal of Personality and Social Psychology*, vol. 3, no. 1, pp. 38–44, Jan. 1966.

[SAL75] J. H. Saltzer and M. D. Schroeder, “The protection of information in computer systems,” *Proceedings of the IEEE*, vol. 63, no. 9, pp. 1278–1308, Sep. 1975.

[SAM54] P. A. Samuelson, “The Pure Theory of Public Expenditure,” *The Review of Economics and Statistics*, vol. 36, no. 4, pp. 387–389, 1954.

[SCH08] B. Schneier, “Essays: The Psychology of Security (Part 1),” *Schneier on Security*, 18-Jan-2008. [Online]. Available: https://www.schneier.com/essays/archives/2008/01/the_psychology_of_se.html. [Accessed: 12-Jun-2018].

[SCO08] M. D. Scott, “Tort Liability for Vendors of Insecure Software: Has the Time Finally Come,” *Maryland Law Review*, vol. 67, no. 2, pp. 425–484, 2008.

[SHA98] C. Shapiro and H. R. Varian, *Information rules : a strategic guide to the network economy*. Boston, Mass.: Harvard Business School Press, 1998.

[SHE85] S. J. Sherman, R. B. Cialdini, D. F. Schwartzman, and K. D. Reynolds, “Imagining Can Heighten or Lower the Perceived Likelihood of Contracting a Disease: The Mediating Effect of Ease of Imagery,” *Personality and Social Psychology Bulletin*, vol. 11, no. 1, pp. 118–127, Mar. 1985.

[SHO08] J. L. Short and M. W. Toffel, “Coerced Confessions: Self-Policing in the Shadow of the Regulator,” *The Journal of Law, Economics, and Organization*, vol. 24, no. 1, pp. 45–71, May 2008.

[SHO13] J. L. Short, “Self-Regulation in the Regulatory Void: ‘Blue Moon’ or ‘Bad Moon’?,” *The ANNALS of the American Academy of Political and Social Science*, vol. 649, no. 1, pp. 22–34, Sep. 2013.

[SHW17] O. Shwartz, Y. Mathov, M. Bohadana, Y. Elovici, and Y. Oren, “Opening Pandora’s Box: Effective Techniques for Reverse Engineering IoT Devices,” in *Smart Card Research and Advanced Applications*, Lugano, Switzerland, 2017, pp. 1–21.

[SIM55] H. A. Simon, “A Behavioral Model of Rational Choice,” *The Quarterly Journal of Economics*, vol. 69, no. 1, pp. 99–118, Feb. 1955.

[SIM90] H. A. Simon, “Invariants of Human Behavior,” *Annual Review of Psychology*, vol. 41, no. 1, pp. 1–20, Jan. 1990.

[SLO04] P. Slovic, M. L. Finucane, E. Peters, and D. G. MacGregor, “Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk, and Rationality,” *Risk Analysis*, vol. 24, no. 2, pp. 311–322, Apr. 2004.

[SLO96] S. A. Sloman, “The empirical case for two systems of reasoning,” *Psychological Bulletin*, vol. 119, no. 1, pp. 3–22, Jan. 1996.

[SMI15] G. S. Smith, “Management models for international cybercrime,” *Journal of Financial Crime*, vol. 22, no. 1, pp. 104–125, Jan. 2015.

[SPE15] M. Spector and D. Yadron, “Regulators Investigating Fiat Chrysler Cybersecurity Recall,” *Wall Street Journal Online*, 25-Jul-2015. [Online]. Available: https://www.wsj.com/articles/fiat-chrysler-recalls-1-4-million-vehicles-amid-hacking-concerns-1437751526. [Accessed: 15-Aug-2018].

[SUN03] C. R. Sunstein, “Terrorism and Probability Neglect,” *Journal of Risk and Uncertainty*, vol. 26, no. 2–3, pp. 121–136, Mar. 2003.

[SWA96] M. Swanson and B. Guttman, “SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems,” *NIST Computer Security Resource Center*, Sep-1996. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-14/archive/1996-09-03. [Accessed: 27-Jun-2018].

[THO16] R. Thomson and B. Perkins, “Switch on to the connected home,” Deloitte LLP, London, UK, Consumer review report, Jul. 2016.

[TOF05] M. W. Toffel, “Resolving Information Asymmetries in Markets: The Role of Certified Management Programs,” University of California at Berkeley, Berkeley, California, Working paper, Sep. 2005.

[TOF11] M. W. Toffel and J. L. Short, “Coming Clean and Cleaning Up: Does Voluntary Self-Reporting Indicate Effective Self-Policing?,” *The Journal of Law and Economics*, vol. 54, no. 3, pp. 609–649, Aug. 2011.

[TVE74] A. Tversky and D. Kahneman, “Judgment under Uncertainty: Heuristics and Biases,” *Science*, vol. 185, no. 4157, p. 1124, Sep. 1974.

[TVE81] A. Tversky and D. Kahneman, “The framing of decisions and the psychology of choice,” *Science*, vol. 211, no. 4481, pp. 453–458, Jan. 1981.

[TVE83] A. Tversky and D. Kahneman, “Extensional versus intuitive reasoning: The conjunction fallacy in probability judgment,” *Psychological Review*, vol. 90, no. 4, pp. 293–315, Oct. 1983.

[UNI17] United States Computer Emergency Readiness Team, “Alert (TA16-288A) Heightened DDoS Threat Posed by Mirai and Other Botnets,” *US-CERT*, 17-Oct-2017. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA16-288A. [Accessed: 10-Jul-2018].

[VAR00] H. R. Varian, “Economic Scene: Managing Online Security Risks,” *The New York Times*, New York, p. C2, 01-Jun-2000.

[VOA16] J. Voas, “Networks of ‘Things,’” National Institute of Standards and Technology, Gaithersburg, Maryland, USA, Special Publication SP 800-183, Jul. 2016.

[WAR17] M. Warner, “Text - S.1691 - 115th Congress (2017-2018): Internet of Things (IoT) Cybersecurity Improvement Act of 2017,” *CONGRESS.GOV*, 01-Aug-2017. [Online]. Available: https://www.congress.gov/bill/115th-congress/senate-bill/1691/text. [Accessed: 17-Aug-2018].

[WEI80] N. D. Weinstein, “Unrealistic optimism about future life events,” *Journal of Personality and Social Psychology*, vol. 39, no. 5, pp. 806–820, Nov. 1980.

[WOR18] World Trade Organization (WTO), “Agreement on Technical Barriers to Trade,” *World Trade Organization*. [Online]. Available: https://www.wto.org/english/docs_e/legal_e/17-tbt_e.htm. [Accessed: 16-Aug-2018].

[YIN14] R. K. Yin, *Case study research: design and methods*, 5th ed. Los Angeles, California: SAGE, 2014.

APPENDIX: LIST OF IOT GUIDELINES

Guidelines Title	Organisation
Automotive Cybersecurity Best Practices, July 2016	Auto-ISAC
Baseline Security Recommendations for IoT, Nov 2017	ENISA
Best Current Practices for Securing Internet of Things (IoT) Devices, Jul 2017	IETF
Careful Connections: Building Security in the Internet of Things	FTC
Connected Consumer Products, Dec 2017	IoTSF
Embedded Hardware Security for IoT Applications, Dec 2016	SCA
Five Star Automotive Cyber Safety Framework, Feb 2015	I Am The Cavalry
Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products, 2016	CSA
Identity and Access Management for the Internet of Things, 2016	CSA
Industrial Internet of Things Volume G4: Security Framework, Sep 2016	IIC
Internet of Things (IoT) Security and Privacy Recommendations, Nov 2016	BITAG
Internet of Things security best practices, Jan 2018	Microsoft
Internet of Things Security Guideline, Nov 2017	IoTAA
IoT Security & Privacy Trust Framework v2.5, 2017	OTA
IoT Security Compliance Framework, Dec 2017	IoTSF
IoT Security Guidance, Feb 2017	OWASP
IoT Security Guidelines for Endpoint Ecosystems, Oct 2017	GSMA
IoT Security Guidelines For Service Ecosystems, Oct 2017	GSMA

ITU-T Y.4806 Security capabilities supporting safety of the Internet of things	ITU
NYC Guidelines for the Internet of Things, City of New York, Jul 2017	NYC
Postmarket Management of Cybersecurity in Medical Devices, Dec 2016	FDA
Principles of cyber security for connected and automated vehicles, Aug 2017	CPNI
Principles of IoT Security, May 2016	OWASP
Secure by Design: Improving the cyber security of consumer Internet of Things Report	DDCMS
Security and Resilience of Smart Home Environments	ENISA
Security Guidance for Early Adopters of the Internet of Things (IoT), April 2015	CSA
Security Reference Architecture for the Internet of Things (IoT)	Symantec
Strategic Principles for Securing the Internet of Things (IoT), Nov 2016	DHS
Technical Report. Security, Aug 2016	OneM2M
Vulnerability Disclosure Best Practice Guidelines, Dec 2017	IoTSF

Abbreviations:

Auto-ISAC Automotive Information Sharing and Analysis Center.

BITAG Broadband Internet Technical Advisory Group

CPNI Centre for the Protection of National Infrastructure

CSA Cloud Security Alliance

DDCMS Department for Digital, Culture, Media and Sport

DHS	Department of Homeland Security
ENISA	European Union Agency for Network and Information Security
FDA	Food and Drug Administration
FTC	Federal Trade Commission
GSMA	Global System for Mobile communications Association
IETF	Internet Engineering Task Force
IIC	Industrial Internet Consortium
IoTAA	IoT Alliance Australia’
IoTSF	Internet of Things Security Foundation
ITU	International Telecommunication Union
NYC	New York City
OneM2M	One Machine to Machine
OTA	Online Trust Alliance
OWASP	Open Web Application Security Project
SCA	Smart Card Alliance