
# Rethinking the cybersecurity of consumer Internet of Things (IoT)

**Authors**
Joo-Huat Ng, MSc (Royal Holloway, 2018)
Robert Coles, ISG, Royal Holloway

**Abstract**

The current widespread use of poorly secured consumer IoT products has been causing menace to the overall security of the Internet (or cybersecurity). Ironically, 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. This article explores an alternative and more plausible solution by rethinking the problem from a different and more fundamental perspective. It investigates and analyses how innate psychological factors can influence the thinking process of consumers when they assess the cybersecurity risk of IoT, and how this perception eventually leads consumers and enterprises to make economic decisions that harm the cybersecurity of the Internet. The insights gained are then applied to formulate a plausible framework that would incentivise enterprises to design and make consumer IoT products that are more cyber-secure.[a]

[a]This article is published online by Computer Weekly as part of the 2019 Royal Holloway information security thesis series `https://www.computerweekly.com/ehandbook/Rethinking-the-cyber-security-of-consumer-internet-of-things`. It is based on an MSc dissertation written as part of the MSc in Information Security at the ISG, Royal Holloway, University of London. The full thesis is published on the ISG's website at `https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/research/explore-our-research/isg-technical-reports/`.

## Technology is helpful but insufficient

The exploitation by malicious actors of consumer IoT products connected to the Internet has been increasingly prevalent, intrusive, and damaging. For example, Mirai botnets of commandeered IoT devices were responsible for several high-profile and massive distributed denial of service (DDoS) attacks that disrupted large swathes of the Internet in 2016. Ironically, the underlying knowledge and technology necessary to design and implement secure IoT products was already well-founded and time-honoured in 2016. In fact, many industry groups and government agencies have already incorporated these technological principles into a plethora of at least 30 IoT cybersecurity frameworks and technical guidelines to address the menace. Generally, these guidelines are recommended "best practices" and voluntary.

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

## Psychology of cybersecurity

In his blog, renowned cybersecurity expert Bruce Schneier observed that security risk is both a subjective feeling and an objective reality. One might feel secure when it is insecure 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 the cost of actual harm. Psychologists have long established

that humans display innate cognitive biases that cause them to judge risk based on perceived rather than actual risk. Understanding this innate irrationality could demystify how the divergence between perceived and actual cybersecurity risk of IoT products could (mis)lead consumers to make decisions that collectively cause market failures and undesirable social outcome.

A security risk judgement involves a trade-off between the cost of preventing *perceived harm* and the cost of *actual harm*.

International surveys conducted by various independent organisations, such as the Information Systems Audit and Control Association (ISACA), indicate that average Internet users are generally apathetic about others hacking into their computers and they are unlikely to have personally experienced any hacking incident. Without any personal memory of cyberattack as mental reference, the average IoT consumers are unlikely to be knowledgeable enough to distinguish the cybersecurity quality of IoT products from the relatively superior cybersecurity that they are accustomed to having with their personal computers. Hence, the average IoT consumer expects the price of IoT products to include adequate cybersecurity. Nevertheless, this status quo is unlikely to be acceptable to the numerous enterprises and organisations that bore the brunt of costly DDoS attacks from botnets of commandeered consumer IoT devices.

## A race to the bottom

We can view the current cybersecurity problem involving consumer IoT products as a manifestation of the collective market arrangement which reflects the perception, behaviour, and decisions of consumers. This in turn drives the commercial behaviour of IoT manufacturers. And the eventual market outcome is that many, if not most, IoT products are much less secure than conventional computers. The commercial imperative of minimising cost entails that consumer IoT be equipped with just enough computational capability to perform their advertised functions and not enough to provide adequate cybersecurity.

Consumers expect cybersecurity but are unwilling to pay for it.

Modern globalisation and technological advances, especially in the fields of communication and logistics, have enabled the manufacturing industry to readily operate supply chains at a global scale and with unprecedented degree of efficiency. This in turn enabled the consumer product market to evolve into a global and an intensely competitive one. Hence, more than ever, 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 of pricing and market demand. Such an arrangement is double-edged because it escalates cost competition to a global scale. And this race to the bottom to quote the lowest price inevitably overlook the cybersecurity of IoT products because cybersecurity incurs cost. As we already know, consumers expect cybersecurity but they are unwilling to pay for it. Focusing on the cybersecurity of products is counterproductive for manufacturers as this does not generate profit, increases cost, reduces sales, and increases time-to-market.

## Economics of cybersecurity

Economists regard a public good as a commodity or service that is “non-rivalrous” and “non-excludable”. Non-rivalry means that consuming the good normally does not reduce its supply available to others. Non-exclusion means that, while providing the good, it is impractical to exclude certain people from consuming the same good. In contrast, a private good is rivalrous and excludable because it is sold to those who can afford its market price, and hence exclude those who cannot afford the price. Clean air is an example of public good. A person enjoying clean air typically does not reduce its availability to others. Also, providers of the good (namely, the clean air) typically cannot restrict its supply only to selected people. In contrast, restaurant food is a private good as the restaurant has full control over its food supply and which customers to sell the food to.

These inherent properties of the public good enables somebody to free-ride and freely enjoy the benefit

of public goods provided by others, hence there is no natural incentive in the free market for someone to pay for the supply of these goods. Consequently, the problem of free riding causes market failure in the form of public goods shortage in the free market. These rational but selfish decisions of individuals collectively result in the over-consumption and under-supply of public goods, and hence to the detriment of overall social well-being.

Cybersecurity resembles public good because it is non-rivalrous and non-excludable. An enterprise which builds IoT products that resist exploitation by botnets will intrinsically contribute to the overall cybersecurity of the Internet by raising the cost of attack. This positive outcome will be enjoyed by all Internet users as it is impractical to restrict this enjoyment only to those who have paid for these devices. Unfortunately, such desirable outcome is unsustainable in practice because competitors and other Internet users will free-ride on the benefit. This prevents manufacturers of secure IoT products from getting adequately rewarded for their extra cost of providing the cybersecurity service. Unless cybersecurity features are mandated by the law or strong social norm, there is no incentive for manufacturers to voluntarily build robust cybersecurity into their IoT products.

Cybersecurity resembles non-rivalrous and non-excludable public goods which allow free-riding without paying for the benefits.

## Misaligned incentives - nobody is accountable

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.

*Misaligned incentive*: Those who neglected security are not the same as those who suffered economic loss.

This notion of misaligned incentive is apparent in the context leading to the recent DDoS attacks involving botnets. Both the manufacturers and consumers of those IoT devices that were commandeered to launch the attacks were not legally liable to the actual victims who suffered substantial disruptions and economic loss wreaked by the attacks. In fact, economic loss is generally not claimable in the courts of the UK, USA, and many European countries. Hence there is largely no legal duty to exercise reasonable care and no incentive for both manufacturers and consumers to care about the cybersecurity of their IoT products.

## Rationale for regulation

The problems of free-riding and the observed market failures indicate that the private sector alone is incapable of providing cybersecurity in the free market. Moreover, an insecure cyberspace also jeopardises the economy's critical information infrastructure, which depends largely on the private sector to ensure connectivity. These are compelling reasons for governments to intervene. Any governmental intervention would have to address the underlying causes of market failure in order to fundamentally overcome the problem. To successfully counteract the underlying causes, 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 provision and enforcement of well-founded baseline cybersecurity specifications that must be met by all consumers IoT products in the market.

- The verifiable disclosure of information about the cybersecurity features of all consumer IoT products in the market.
- A global scheme for the disclosure of information about new vulnerabilities and cyberattacks pertaining to consumer IoT products.

## Public regulation

Theoretically, governments may remedy market failures with public regulation by mandating producers to meet minimum quality standards on goods and services. 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 must be disclosed alongside the products and services. Nevertheless, such schemes must also include safeguards against unintentional and counter-productive social outcomes. These 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.

*Public regulation*: Governments mandate producers to meet minimum quality standards on goods and services.

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. This is particularly relevant in the case of regulating IoT products, because 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 the specific needs of consumers. Hence policymakers are compelled to rely on private parties, at least for defining implementation measures and technical specifications. 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.

## 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, 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. Most of these arrangements are governed by a combination of companies and industry groups whose practices are targets of regulation, non-governmental organisations (NGOs), and other civil society groups, including labour unions and socially responsible investors.

*Self-regulation*: Private organisations undertake governance responsibilities which include setting standard, monitoring, and enforcing compliance.

Numerous research studies, such as those by Professor Jorge Rivera of George Washington University, have found no conclusive evidence that participants of voluntary quality management schemes perform better than non-participants. This finding suggests that effective industry self-regulation entails explicit governance oversight and sanctions for violators. This requisite for effective governance is substantiated by the findings of a study by Harvard Business School's Professor Michael Toffel. His research revealed convincingly that the ISO 14001 standard (Environmental Management System), which include a robust compliance verification process by independent and certified auditors, not only attracts adopters with superior environmental performance but also leads to further performance improvement. This strongly implies that the effective self-regulation of quality management schemes must include robust independent verification mechanisms.

## Independent regulations will be futile

There are signs that governments have begun to take regulatory actions to address the failures in the consumer IoT market by enforcing minimum cybersecurity requirements on IoT products. In 2017, the US Senate proposed the Internet of Things Cybersecurity Improvement Act, which seeks to impose minimum cybersecurity requirements on federal government procurements of IoT products. In 2018, the European Council formally proposed the Cybersecurity Act, which includes establishing a European cybersecurity certification scheme that attest the compliance of eligible IoT products and services to pre-defined cybersecurity standards. In March 2018, the UK government published the "Secure by Design: Improving the cyber security of consumer Internet of Things Report", which revealed the government's intent for a voluntary labelling scheme for consumer IoT products to aid consumer purchasing decisions and to facilitate consumer trust in companies. The UK's independent national standards body, British Standards Institution (BSI), subsequently launched a pilot BSI Kitemark Certification scheme for IoT cybersecurity in May 2018.

Independent regulatory actions at a national or regional level would be futile. The success of any solution relies on its universal enforcement.

Although these regulatory actions will contribute toward resolving the IoT cybersecurity problem, they are insufficient because the fundamental socio-economic rationale that underlies the problem remains largely unaddressed. Cybersecurity is a non-excludable good. Consequently, the menace of insecure IoT is omnipresent in the cyberspace due to 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 cybersecurity 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 its universal enforcement.

## A global problem needs a global solution

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 inter-governmental organisations (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.

We propose a more robust and improved regulatory framework that should (ideally) be universally mandatory and be based on independent international standards or its equivalence within the rules of the WTO Agreement on Technical Barriers to Trade. The more universally the framework can be enforced, the more successful its outcome will be. Because this framework is mandatory, it is critical 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.

## Don't reinvent the wheel

Instead of creating from scratch, attempts should be made to use existing regulatory framework and resources that could be naturally exploited or extended to encompass IoT cybersecurity. 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 prod-

ucts to indicate certification. IoT cybersecurity could be added to such regulations as a new category of product safety. This is consistent with how the other product categories (such as telecommunication equipment) had been added to these regulations as new consumer products emerged alongside technological progress.

In the short run, the UK's BSI Kitemark for IoT scheme, as well as other similar schemes in the Single Market, 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.

Use existing regulatory framework and resources that could be naturally extended to encompass IoT cybersecurity.

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 extend consumer product safety regulations in as many countries as possible to include the cybersecurity of IoT. Governments could use these existing networks and partnerships 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 Agreements could be used to enable different jurisdictions to recognise each other's product certification.

Policymakers should provide a fair competitive environment, as well as fundamentally eliminate the economic reasons for free-riding. They should collaborate globally with an objective of enforcing mandatory cybersecurity certification on all consumer IoT in the entire global market. This goal could be facilitated by an internationally recognised certification and cybersecurity marking scheme that is based on international standards. This would foster product information transparency and enhance consumer trust. Obviously, the success of this improved framework depends on the adherence, universality, and integrity of the certification process. Hence the framework needs to be primarily self-regulated by the private sector 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, fair enforcement, good governance, sanction for violators, and cross-border cooperation.

## Embrace, not resist, reality

Unlike traditional public goods, such as environmentally pollutive activities or physical security, which can be reasonably regulated nationally or regionally, cybersecurity is inherently virtual and borderless. Hence it should be managed holistically. It is futile to resist this reality and to attempt to regulate cybersecurity nationally or regionally using traditional approaches. Instead, academics, policymakers, managers, and consumers should accept and embrace the unique borderless nature of cyberspace, and cooperate internationally in an effective way that is conducive to the new reality of the Internet era.

**Biographies**

*Joo-Huat Ng* received his MSc (Distinction) in Information Security from Royal Holloway, University of London in 2018. Joo has been working as an SAP consultant for more than 20 years. His work involves helping large enterprises to engineer and enable their complex business processes using SAP technology. He is particularly interested in the growing importance of information security and its

governance in our modern digital age. Joo can be contacted at joohng@ymail.com.

*Robert Coles* is currently the CISO for the NHS and health and care system. He also has his own consulting business, and was a Visiting Professor at Royal Holloway, University of London and an Honorary Professor at UCL. Prior to this, Robert was the first Chief Information Security Officer at GSK from 2013 to 2018.

Robert held several CISO roles prior to joining GSK. He was the first CISO at National Grid and Merrill Lynch before that. In all these roles, he owned the information security risk and was responsible for providing global leadership. He was accountable to the Executive and PLC Boards for establishing information security strategy and direction. Building global information security capabilities and overseeing all of the information security initiatives across the organisations has been his primary career focus.

Robert has been working in the field of Information Security for over 30 years, including "head of" roles at Royal Bank of Scotland, and the lead partner in KPMG's Information Security Services for EMEA.

*Series editor: S.- L. Ng*