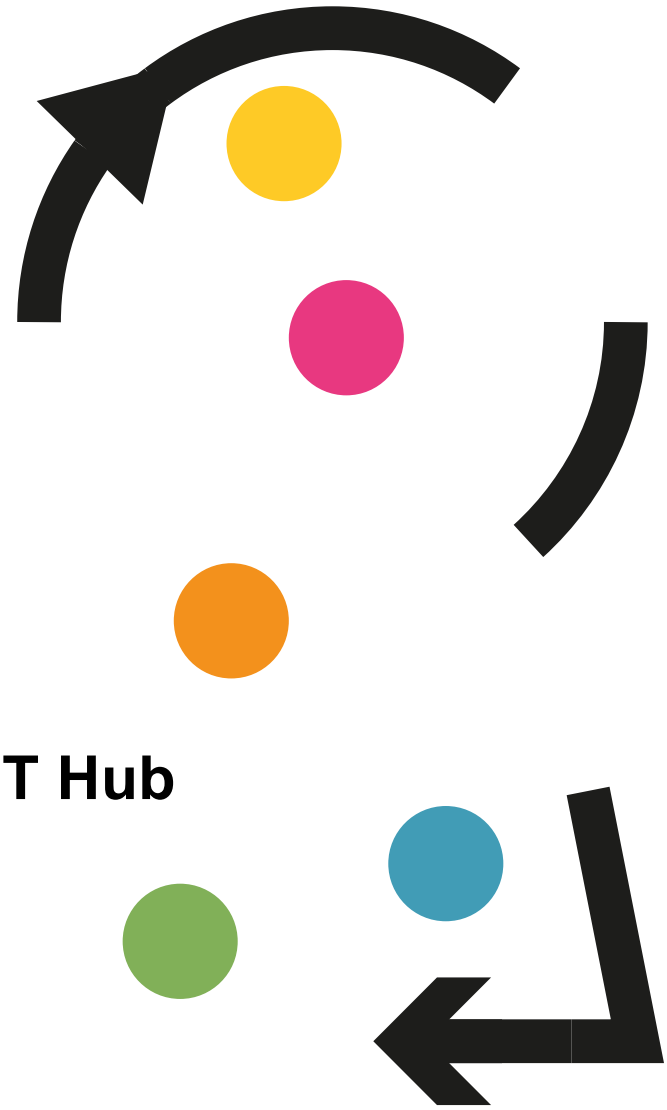
Review of International Developments on the Security of the Internet of Things



PETRAS IoT Hub

Leonie Tanczer
Fareeha Yahya
Miles Elsden
Jason Blackstock
Madeline Carr

UCL WARWICK Imperial College London Lancaster University UNIVERSITY OF SURREY Southampton CARDIFF UNIVERSITY PRIFYSGOL CAERDYDD

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report outlines the current international developments on the Internet of Things (IoT) security and security by default. It examined those international organisations that are shaping the global governance and policy conversations about the security of the IoT and identifies the key issues that the UK should consider in its emerging IoT policy thinking.

While DCMS has a portfolio specifically dealing with consumer products, most discussions on the international landscape do not segment these matters by sector. Most of the literature looks at specific IoT applications such as medical devices, connected autonomous vehicles, and smart cities. This report attempts to draw broad insights into the key factors across the IoT landscape to inform both the work of DCMS on consumer products and the wider UK government work on other IoT applications.

The report identifies ten key themes that cover the main international IoT activities:

1. Security by Default/Design Measures
2. Balance Between Regulation and Self-Regulation
3. Certification and Trust
4. Standardisation
5. Procurement
6. Training and Capacity Building
7. Liability
8. Data Management and Transparency
9. Research and Development
10. International Collaboration, Consensus, and Public-Private Partnerships

'Security by default' and 'security by design' are concepts that are regularly mentioned internationally, but often interchangeably and with no internationally established or agreed definitions. Security by default is frequently used to represent a more holistic security approach that considers the full systems' security and is, therefore, a broader term than 'security by design'. It is commonly recognised that there is a role for government in the coordination and execution of effective measures including support for this from industry.

There is a clear consensus that there is currently no need for new regulation in the IoT space. The international focus is at present on the enforcement of existing legislation, with some actors calling for a mix of soft and hard regulation driven by market needs. This, together with the updating and harmonisation of existing regulations, is considered the best way forward not to stifle innovation in IoT.

IoT certification and a corresponding 'Trusted IoT' label or kite mark has been highlighted by a number of international organisations. This approach is seen to be a useful way to address a variety of issues ranging from user privacy to system security and reliability, as well as enabling informed purchasing decisions and increasing users trust. However, there are a number of outstanding questions as to how such a system would effectively work in the complex IoT ecosystem and how

effective lab-based testing or self-certification could be ensured. The recently proposed EU certification scheme is ground-breaking in this area and will likely provide a basis for more focused international discussion.

There is clearly a need to develop open, internationally recognised, market-driven standards and interoperable solutions as a means to lower barriers to market entry, foster competition while ensuring baseline levels of security and privacy.

There is a consensus that training and capacity building of both developers and users of IoT systems is a core component of delivering a secure IoT ecosystem, as is the need to build more capacity at all levels in the workforce. This clearly aligns with the UK's skill development agenda.

The issue of liability has mostly been discussed at the EU level, though the World Economic Forum and the OECD have also investigated the legal implications of the IoT. The general consensus is that the existing legislative framework is flexible enough to deal with current IoT challenges. Though there will likely be a need to clarify some aspects of the existing product safety and liability regime by means of policy documents and guidance. There may also be demands to review product safety and liability rules as the IoT system develops. This implies the need to monitor developments and intervene when and where necessary. This should include continuing consultation with stakeholders such as consumer representatives, innovators and manufacturers and insurers to gain early sight of potential problems.

Issues around data management and transparency were seen as key areas for action and vital to engender user trust. Transparency of what data is collected, how it is being used (and for what purpose), and how the data is being shared, are all-important to ensure users have confidence in the IoT system. This is clearly a complex area and is not specific to IoT application. However, it is recognised that dealing with these questions will be a key component in ensuring successful development and deployment of future IoT-based devices and services and agreed approaches to general data transparency at an international level are at the moment missing.

Cross-government and cross-industrial collaboration are needed to reach a viable consensus on IoT security and security by default guidelines. There is no obvious international forum that has ownership of creating this consensus. Given the necessity to work globally with governmental and industrial stakeholders the World Economic Forum is the most likely medium for these discussions, with the US, China, Japan, South Korea and India identified as key strategic partners in this space.

It is clear from the findings of this report that debates around security of IoT systems are relatively immature internationally. There are therefore clear opportunities for the UK to take the lead globally in shaping the future governance of the IoT. It is unclear how soon a viable an international mechanism, or consensus, will coalesce around the key themes identified in this report. If the UK wants to influence the formation of IoT working groups, best practices, and guidelines internationally, there is currently a window of opportunity to take the lead. The UK's expertise in ICT procurement

through its Cyber Essential Scheme and its experience with self-regulatory approaches may, therefore, be suitable starting points to foster international discussions.

RECOMMENDATIONS

Balance Between Regulation and Self-Regulation

The international consensus on regulation closely follows the UK approach of exhausting existing laws and regulations to regulate the emerging IoT ecosystem. The UK has considerable expertise in the use of market-driven, self-regulation approaches and would be well placed to take a principal role in developing a global approach to regulation of future IoT systems.

Certification and Trust

International thinking on certification aligns closely with the current UK perspective. The upcoming EU certification scheme is the leading approach internationally currently and will likely form the basis for future global developments in this space. The UK should consider either playing an active role in the development of this EU scheme or maintain a watching brief on how thinking evolves.

Standardisation

There is a general recognition of the need to develop open, internationally recognised, market-driven standards and interoperable solutions to support innovation and growth of the IoT. There is an opportunity here for the UK to actively engage and/or take a leading role in the development of these standards using its strong reputation and links in the international standardisation community.

Training and Capacity Building

The global position on training and capacity building closely aligns with the UK skills agenda. This provides an opportunity for the UK to exploit its world-leading education sector to provide both the UK national need and export to the global market.

International Collaboration, Consensus, and Public-Private Partnerships

There is clearly an opportunity to lead on the development of international cooperation, standards, and regulation and to guide the advancement of the international agreements that will be necessary to ensure a safe and security IoT. There is currently a lack of consensus and leadership in most of the international organisations on these subject matters, with The World Economic Forum seeming to be the most obvious forum where all the key players are engaged. This, together with the OECD and potentially the WTO, would likely be the best route to influence the international agenda. There is an opportunity for the UK to direct and shape this debate.

INTRODUCTION

This report outlines the current international developments on Internet of Things (IoT) security and secure by default1. We reviewed international organisations that are shaping the global governance and policy conversations about the security of the IoT and reflect on the various developments that have taken place. The report therefore offers a preliminary high-level overview summarising core activities, debates and publications in the leading eleven2 international fora. The insights provided here will ensure that the UK government has an appropriate depth of understanding into key initiatives and discussions to best exercise its interests within the emerging and rapidly evolving international IoT landscape.

The document draws upon research conducted at the PETRAS IoT Research Hub, a consortium of nine leading UK universities that work together to explore critical issues in privacy, ethics, trust, reliability, acceptability, and security of the IoT. The analysis is based on desk-based research which was conducted by PETRAS' Standards, Governance and Policy (SGP) research team in support of the efforts by the Department for Digital, Culture, Media and Sport (DCMS). It complements a previous SGP report that delivered a standards and guidance landscape mapping [1].

While DCMS has a portfolio specifically dealing with consumer products, most discussions on the international landscape do not segment these matters by sector. Rather, the majority of organisations have engaged with other aspects of IoT, including medical devices, connected autonomous vehicles, and smart cities. Caution should therefore be used to not make assertions in one particular sector, such as consumer products, without acknowledging developments in other realms.

The report discusses some of the most prevalent themes across the analysed organisations and the historical development of these debates. Where evident, we point to consensus and disagreements and highlight key messages. The document starts with secure by default principles identified on the international landscape and moves on to key issues that are of further interest not only to DCMS, but to the wider UK policy community. A comprehensive, tabular summary of these key themes (Table 1) and identified security by default best practices (Table 2) can be found at the end of the document. An extensive addendum (Appendix A) identifies relevant bodies and IoT-specific working groups the UK government may want to further

---

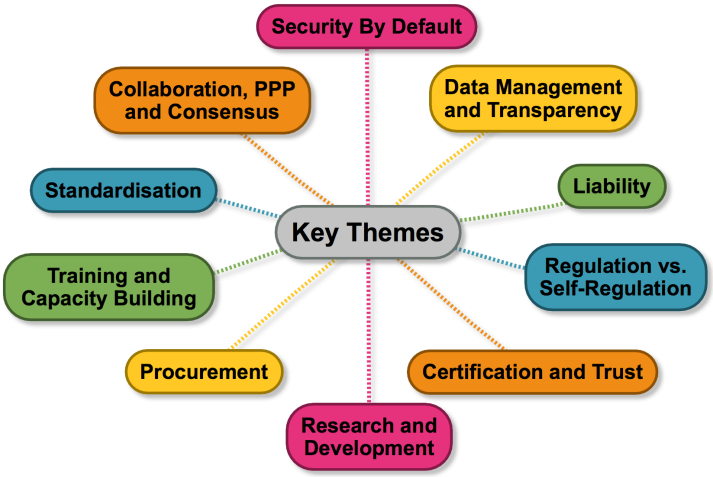
[1] Privacy- and trade-related issues were excluded from this report, although they may require further investigation in the near future.

[2] Four additional organisations have been reviewed, but were excluded from this report, owing to lack of relevant publications on IoT security and secure by default/design. These include the United Nations Educational, Scientific and Cultural Organization (UNESCO) and the Office of the United Nations High Commissioner for Human Rights (OHCHR); both have so far primarily dealt with broader debates on privacy and freedom of expression online. The Organisation for Security and Co-operation in Europe (OSCE) and the North Atlantic Treaty Organisation (NATO); their emphasis was on military IoT applications and the reduction of conflict between states stemming from the use of ICTs.

engage with. These are institutions that will continue to be active in this space and are potential strategic partners for the UK. We also offer hyperlinks to significant documents for further reference.

Key Thematic Issues

Our analysis reveals that there have been several international conversations that have shaped the development of the IoT over the last five years. Debates around issues such as security by default, (self-)regulation, standardisation and security measures have emerged, though they are not necessarily homogenous and not always shared widely across stakeholders. The following pages review ten of the most commonly shared themes. Unsurprisingly, many of the topics overlap with insights gained from an earlier analysis of industry reports by Blythe [2], reinforcing core messages for secure by default principles.



1. Security by Default/Design Measures

Key Findings

- *Security by default and security by design are concepts that are frequently used interchangeably.*
- *Secure by default/design measures are prevalent across various international organisations, although there is a lack of established and internationally agreed global IoT security principles, offering opportunities for future world-wide collaborations.*
- *Coordination and execution of effective measures are likely to require government input and there is support for this from industry.*

The concept of secure/security by default or design is promoted as an organisational measure for both public and private institutions to plan for the development lifecycle of IoT products and services [3]. Although frequently used interchangeably, 'security by design' is generally understood as a *reference architecture model* which is based on agreed security standards, procedures, processes, and risk/impact management [4]. 'Security by default' is defined as proven and securely up-datable system settings which are indispensable throughout a product's design and lifetime [4].

Security by default is part of a holistic security approach. It goes beyond a pure focus of security at the device level and takes into account all components of the IoT architecture, including the application and network layers. Secure communication

links or secure storage infrastructures are also taken into account as are resilience and incident responses [5], [6], [7]. In an expanded view, security by default could even include the promotion of user awareness [3], [8]. This integrated approach means that security by default has to be considered in close relation to certification and standardisation practices as well as the regulation and transparency of IoT, all discussed later in this document.

One of the first references to the necessity for IoT security principles can be found in the EU's Action Plan on the Internet of Things from 2009 in which the European Commission articulated its ambition to finance research projects on privacy and security by design [9]. Several workshops at the EU level have since been held [4], [10], [11], with an upcoming validation workshop on baseline security measures for IoT scheduled for the 20th of October 2017 and ongoing research projects such as SAFURE that studies safety and security by design features in cyber-physical systems [12].

In addition to EU-efforts, our analysis reveals that security by design is also a pressing issue across other international organisations, many of which refer to particular security best practices that fall under the realm of security by default. Table 2 provides a comprehensive summary of these efforts. The table has been amended from Blythe [2] and points to widely shared guidelines that include the use of cryptographic primitives in all design components i.e., universally composable security [13], automated software updates [4], [14] and security best practices based on network restrictions and the disabling by default of non-critical functionalities [15]. Some of the most relevant publications for the security by default work of DCMS are publications by ENISA [3], [11], [16], the European Commission and AIOTI [4] as well as IEEE [17]. They refer to minimum baseline security and privacy requirements and are of particular relevance for IoT services designed for the consumer market.

There is evidence of strong support for the role of the government in providing leadership on these issues [18]. In a survey for the European Commission's efforts on IoT governance more than 70% of respondents agreed that policy makers should offer guidance on security by design measures and should actively support the development of applicable security technologies [19]. However, as past debates have shown, technical security interests can conflict with national security considerations. For instance, while encryption provides secure communication and data storage opportunities essential for many sectors, the use of cryptographic measures is also understood by some to pose a security challenge for governments trying to "balance national security and law enforcement demands" [6, p. 12].

In addition to such divergences, there are currently also no existing, widely agreed security by default guidelines available. Instead, there is a segmentation of principles, with the World Economic Forum [20] arguing that technology providers should begin to inventory and share recommended security practices and potentially work to establish a global security commons. This offers opportunities for the UK government to foster such measures at the international level. If made mandatory, security by default principles could go along with financial penalties for non-compliance [7, p. 26].

2. Balance between Regulation and Self-Regulation

Key Findings

- *International organisations' focus of attention is currently on the enforcement of existing horizontal laws and regulations in opposition to the introduction of new legislation.*
- *Self- and a mix of soft and hard regulation are perceived as the best near-term options to facilitate IoT's growth.*
- *The update, adaption, and harmonisation of existing regulation is considered necessary in areas that stand in the way of IoT innovation (e.g., free flow of data, motor vehicle, aviation, workplace regulations, and insurance).*

Regulations, just as standards and certification, are one of the potential measures policy makers have available to ensure the security of IoT services throughout their lifecycle [21]. However, similar to Blythe's findings (2017), the analysed international organisations were frequently opposed to their usage and primarily in favour of self-regulatory, soft law, and market-driven approaches. Some are considering a mix of soft and hard measures for issues such as privacy, safety, and health [19].This perspective aligns with an international trend, dominated by actors such as the US.

There is an expressed preference for the enforcement of existing horizontal laws, strongly noticeable in AIOTI's WG04 [22]. A core concern for this laissez faire approach is the argument that the adaption of new legislation carries the danger of hindering IoT's growth [21], creating barriers for the IoT's potential benefits [23], and runs the "real risk" of regulatory error resulting in the IoT's development being held back [22, p. 35]. In particular, proposals for the regulation of internet access services / interpersonal communication services would be currently overly restrictive [24] and any sector specific regulation of conveyance of signals services should be limited to requirements relating to security and privacy [24].

Instead of implementing laws and/or regulations that are "not fit for purpose", international actors rally for the evaluation and assessment of the existing legislative framework [22, p. 35]. Any regulatory proposal targeting the IoT should address only well-defined market failures and imbalances that cannot be addressed through existing law and self-regulatory measures [19]. Amendments should also only be implemented in close dialogue and under careful consideration with other stakeholders [6].

This hands-off approach is accompanied by a push for the update, adaption and harmonisation of existing regulations and better defined industry-led standards, best practices, and voluntary schemes [19]. Arguments for the update and adaption of regulation are primarily concerned with adjustments in sectors such as motor vehicle, aviation, workplace regulation, power utility regulation and insurance [20], [25]. There is a collective call to streamline the trans-border data flow and potentially even relax exiting legislation [20], [22], [26]. The latter should remove any barriers to the free geographic movement of data across states. Likewise, harmonisation should only be considered when it helps to remove regulatory barriers [5] and is considered necessary in, for example, the fragmented telecommunications sector [24], [25].

3. Certification and Trust

Key Findings:

- *The certification and labelling of IoT products and services are considered to be advantageous for both users and manufacturers and are a means to enhance users trust.*
- *Certification mechanisms are primarily discussed at the EU level and within technical organisations such as the ITU and IEEE.*
- *The recently proposed EU certification scheme is ground-breaking and will provide a platform for further international debates about its benefits and challenges.*

IoT certification and a corresponding 'Trusted IoT' label or kite mark was highlighted across various publications, including the World Economic Forum, ITU, IEEE and all analysed EU institutions. In doing so, they refer specifically to the certification and accreditation of IoT products with regard to user privacy, user autonomy, systems security and system reliability [19]. IoT certification and labelling is expected to enable informed purchasing decisions [6], enhance users trust [4] and play a critical educational role in a society that is only beginning to understand the effects of these emerging technologies [6].

For manufacturers, such measures would define minimum security requirements which industry actors could rely upon [27], increase business competitiveness [28] and reward and incentivise security best practices [6]. However, these measures also create various challenges for industry actors. Software and network security are extremely complex and context-dependent, and testing in a laboratory may not accurately reflect the realities of a less predictable real-world setting [6].

The majority of international organisations are in favour of IoT certification and labelling schemes. A recent ENISA survey of EU member state agencies, vendors, manufacturers and consumer associations highlighted that 81.8% of respondents agreed that certification and labelling can be effective tools to increase transparency about the level of security assurances of ICT products and services, with 75.7% explicitly identifying a need for ICT security and labelling in the IoT-domain [29].

At a global level, debates continue as to whether:

a) A certification and labelling scheme necessitates an independent security review body that would audit IoT products and services [6], [10], [30];
b) Certification should be voluntary or mandatory, with some actors arguing in favour of an obligatory reference framework that would provide incentives to follow security by default practices [27];
c) A quantifiable certification framework can be generated that allows to assess the security hygiene of IoT products and services [6], [10], [12].
d) A self-certification frameworks could be used which would not require third party testing [31];
e) A case-based assessment measure could be established that accounts for sector-specific needs [10], [31]; and

f) The design features of a kite mark can be made user-friendly and computer-readable e.g., electronically accessible and connected to a digital security certificate [10], [17].

Most recently, an EU-wide cybersecurity certificate scheme is expected to be put in place and implemented by ENISA [32]. The resulting certificate will be recognised in all EU member states, making it easier for businesses to trade across borders and for purchasers to understand the security features of IoT products and services. At this point, the schemes will be voluntary unless future EU legislation prescribes a certificate as mandatory requirement to satisfy a specific cybersecurity need [32]. While the EU initiative is ground-breaking, it remains to be seen how it impacts on international IoT security.

4. STANDARDISATION

Key Findings

- *The development and promotion of open, internationally-recognised, market-driven standards and interoperable solutions is emphasised across all analysed institutions.*
- *Identified standardisation gaps offer an opportunity for the UK government to play a leading role in the international efforts to deliver security and interoperability of IoT devices and services.*

All analysed organisations express a preference for the development of global, market-driven security standards. This is regarded as a means to lower barriers to entry for market newcomers and decrease operational costs for users. Standards are also expected to foster competition at the international level and ensure a baseline level for both security and privacy [9]. Across all stakeholders, particular emphasis is given to standards that are:

a) Open;
b) Global;
c) Industry/market-driven;
d) Collaboratively designed/multi-stakeholder-driven;
e) Voluntary; and
f) Sustainable.

All ten institutions further highlight the importance of standards to guarantee interoperability of components and communication protocols, which is specifically of relevance when it comes to security and privacy by design principles [20], [33], with the European Commission stressing the need to make data protection requirements a mandatory design goal in standardisation processes [19].

Two dedicated working groups are worth mentioning here. AIOTI's WG03 is concerned with the analysis of IoT standards and routes to interoperability. It facilitates discussion on regulatory and legal obstacles to promote IoT take up as well as efforts to develop consensus on standardisation matters through the European Telecommunications Standards Institute (ETSI) and oneM2M [34]. Similarly, ISO's subcommittee ISO/IEC JTC 1/SC 41 maintains an expert role in the

international debates on the standardisation of the IoT and is working on IoT use cases, interoperability systems and consistent definitions and vocabularies [35].

The widely shared perspective on the need for IoT standards goes along with the identification of particular standardisation gaps. Some of these have been comprehensively summarised by AIOIT WG03 [34], including competing communications and networking technologies, the lack of APIs to support application portability among devices/terminals, and fragmentation of standards due to competing platforms. These gaps provide an opportunity for input from stakeholders like the UK. For more details on specific IoT standardisation debates, please consult an earlier report by Brass, Tanczer, Carr, Blackstock [1].

5. Procurement

Key Finding(s)

- *IoT procurement is not a focus point of international organisations, but provides an opportunity for the UK government to foster these debates and best practices globally.*

The procurement of IoT systems as a mechanism for increasing IoT security is discussed predominantly at the EU rather than the international level. European institutions such as the Commission, ENISA and AIOTI promote the uptake of IoT standards in public procurement to avoid lock-in, most notably in the area of smart city services, transport and utilities, including water and energy [11], [16], [33], [36]–[38]. Although procurement is part of an ongoing debate within nation-states (e.g., UK Cyber Essential Scheme, US Internet of Things Cybersecurity Improvement Act) and flags up once in a publication of the World Economic Forum [20], our analysis revealed that the international community is less engaged than it could be with the use of procurement as a tool to drive the security agenda of the IoT. This gap presents an opportunity for further conversation and international linkages. The promotion of this topic within international fora would be an opportunity for the UK government to foster these debates and best practices globally.

6. Training and Capacity Building

Key Findings

- *IoT specific training and capacity building initiatives underpin security by default measures and can help create an overarching culture of security necessary for the emerging IoT ecosystem.*

The analysed international organisations also emphasised training and capacity building measures as relevant activities to ensure the security of the IoT. These stretch from educational initiatives in schools, the higher education sector to professional domains. Such educational means would be of particular relevance for actors involved in the development phase of the IoT [39]. At this stage, fundamental security functions have to be implemented (i.e., security by design/default) and it is point at which programming errors may occur which can consequently create lasting security vulnerabilities. It would therefore be necessary to ensure that:

a) IoT developer teams are skilled enough to follow secure programming [40];
b) Security training is in place for the developers contributing to critical parts; and
c) Security training is in place for all the other developers/testers, as many security flaws can occur in 'non-secure' parts of an IoT product development.

Similar organisational measures are emphasised in a publication on the security of smart airports [41] and may be transferred to development of IoT products in the consumer realm. These recommendations involve:

a) Basic security awareness training for all information system users of an organisation (this training should also include social engineering attacks);
b) Specialist role-based information security training for personnel with security-related responsibilities;
c) Documentation and monitoring of security training activities to ensure individual training records of staff; and
d) Maintenance of ongoing contacts with security groups and association in order to remain up-to-date in a rapidly changing environment.

Further international developments in regards to the expansion of the necessary skill force for the emerging IoT environment include:

a) The quantitative increase of human capital through national education programmes, especially in the higher education sector [18], ICT skills standards [8], and reskilling programmes [20];
b) The adequate training and preparation of the potential workforce e.g., through adaptive learning spaces [42], MOOCs [20], training roadmaps [5], and the education of non-technical professions such as the law enforcement [28];
c) The update of existing training programmes e.g., inclusion of IoT in digital risk management processes [43], e-leadership skills initiatives [20], and responsible engineering practices [17]; and
d) The development and/or adaption of certification schemes e.g., through the inclusion of IoT in these initiatives [5], [14], [18], [20].

7. LIABILITY

Key Finding(s)

- *Liability issues are primarily discussed on the EU level and have been subject to substantial assessments and scrutiny by bodies such as the European Commission and AIOTI.*
- *AIOTI considers the current legislative framework and existing safety and liability regime as flexible enough to sustain the ongoing IoT developments, although clarification on particular principles could be supported through policy documents and guidance.*
- *A review and change of product safety and liability rules should occur as evidence of a need emerges.*

Related to the theme of regulation, and an essential question for the security of the IoT, are discussions on the changing nature of liability. These debates are primarily evident and most strongly developed within the context of the EU, although it is a topic that also flags up in documents of the World Economic Forum [6], [20], the ITU

[30] and the OECD [18]. Liability is of profound importance, considering that the IoT is creating sophisticated interdependencies, characterised by a complex ecosystem [38] and involves a variety of stakeholders, all of which could potentially have a share of IoT's liability [44]. These dependencies are also not static and increase and become more entangled as IoT services evolve [38].

In 2013, the European Commission held an investigation into the liability challenges arising from IoT and robotics [19]. It has since then raised the issues in workshops [45] and European Parliament hearings [46]. Discussions centre on assuring legal certainty and guaranteeing traceability and accountability of potential failures, with the Product Liability Directive (85/374/EE) being one of the corner stones of these debates. While the latter may have potential weaknesses, including the distinction between 'product' and 'service', a recent AIOTI WG04 report [22] rejects the idea that the current legal framework – at least within the EU – is unfit to manage liability concerns emerging from the IoT.

Conversely to the World Economic Forum [20] which proposes a re-examination of liability regulations, AIOTI's [22] assessment emphasises that IoT may be managed within the existing legal framework, which has over the last 30 years proven to be flexible enough to deal with novel technological developments, including the evolution and expansion of the Internet. There would be no evidence of legal uncertainty and consequently no suitable justification to deal with IoT services separately to other products.[3] At the current stage of the IoT development, businesses would be well placed to take appropriate steps such as contractual arrangements or insurance clauses to allocate risk between themselves [47]. Further measures to manage liability and the security of IoT systems could include:

a) The clarification of the existing product safety and liability regimes by means of policy documents and guidance;
b) Market's self-regulation within existing frameworks; and
c) The creation of a dedicated IoT certification scheme [6], [22].

Hence, the UK government may follow AIOTI's WG04 [22] advice and engage in a gradual, reasoned, and cautious approach to the development of a response to address any product safety and liability issues in the IoT space [22]. This includes to:

a) Monitor the development and intervene as soon as evidence of a need emerges;
b) Continue to work with the international community on these issues; and
c) Consult with stakeholders such as consumer representatives, innovators and manufactures and insurers to investigate future areas that may create uncertainties.

[3] While existing legal measures seem efficient, major product liability challenge are expected to emerge with the roll-out of fully autonomous driving [19].

8. Data Management and Transparency

Key Findings

- *There is a collective demand by international organisations to ensure user transparency, access management control, and consent from the time of purchase throughout the lifecycle of the IoT services.*
- *Data security and data management are relevant factors for a potential IoT certification scheme.*

Data management and questions around user transparency are prevalent across many of the analysed international organisations. They closely interlink with security by default principles, some of which have been emphasised in Section 1 and summarised in Table 2. Lawful, responsible, and privacy-/user-friendly data management should be implemented across the lifecycle of the IoT service and be prevalent across all three main layers of the IoT (device, network, cloud) [34]. According to AIOTI WG03 [34] the data lifecycle can be split in seven main phases:

a) Obtain/collect;
b) Create/derive;
c) Use;
d) Store;
e) Share/disclose;
f) Archive; and
g) Destroy/Delete.

Many of the analysed publications touch on best practices across these phases, including measures concerning:

a) Data security (which should involve the application of end-to-end encryption [15]; access control [16]; risk management; and 'smart defaults' e.g., forcing changes to default passwords [21]);
b) Data collection (which should occur fairly, transparently and lawfully [48]; and focus on data minimisation [21]);
c) Data protection (which should be underpinned by privacy impact assessments and be supported by privacy enhancing technologies [22]).

Related to the issue of data management is the question of transparency and accountability in the IoT. IoT's component parts and operations should remain visible and transparent to users [31]. The data subject is expected to give consent to the data collection and processing and to be aware of who is taking what action with its personal information [21]. Transparency is consequently an important means for ensuring user's trust in an organisation [14] and provides awareness of the types of data that are potentially at risk [49]. Collectively emerging transparency principles therefore encompass information about:

a) What data is being collected;
b) How data is being used and processed (i.e., indication of purpose);
c) For what purpose data is being used; and
d) Whether, and if so, what data is distributed to third parties and why.

International organisations further highlight particular needs around data access management, which include:

a) The communication of information – including vulnerabilities impacting on the user's data – in layman terms [39]:
b) Opt-in/opt-out options [42], [50];
c) Data auditability and control i.e., the ability to measuring and monitoring data access [50] and the right to erasure of data [23]; and
d) The decoupling of personal identity from the device identity [4].

At present, no agreed formal modalities for implementing general policy on data transparency are available, although ENISA [39] and AIOTI [21] offer the most comprehensive guidelines. As data management and transparency interconnect with IoT's security, the implementation of above mentioned practices may consequently be one of the principles that could be assessed in the course of proposed ICT certification schemes. Failure to adhere to such recommended measures could make companies be held liable and generate an incentive to further secure and improve IoT products [6]. Conversely to this, the OECD also critically highlights that too much transparency could also undermine security as well as possible oversight mechanisms [18], pointing to potential conflicts that could emerge in this space.

9. Research and Development

Key Findings

- *International organisations are actively involved in IoT R&D initiatives, fund and support cross-country projects and foster a multi-stakeholder engagement in this space.*

Among the analysed international organisations, various research and development (R&D) initiatives were identified that underpin and impact on the development of security by default principles and best practices. Publications highlight the importance of including industry, government and academia in these activities and stress the necessity for strategic engagements with start-ups and in particular SMEs [5], [43].

On the international level, ASEAN's Masterplan 2020 [5] includes the proposal to establish Centres of Excellence (CoE) to promote R&D and create greater collaboration across and recognition of ICT experts in the region. Similarly, the World Economic Forum [20] highlights the demand for long-term R&D collaboration to solve IoT's fundamental technological challenges. Focus should thereby be given to:

a) The management of IoT systemic risks [25], [33], [43];
b) Standardisation and interoperability [30], [32];
c) IoT's impact on legal dimensions [51]; and
d) New mechanisms for anonymous signatures, authentication, and homomorphic encryption [49].

On the EU level, the European Commission proposed the financing of security by design research projects already in 2009 [9], with a European Commission study having comprehensively mapped IoT initiatives in selected EU member states in

2014 [43]. Since the release of this study and with the emerging of the Horizon 2020 programme, relevant EU projects and initiatives have been established that engage with IoT security concerns:

a) The IoT European Research Cluster (IERC) brings together EU-funded project that aim to define a common vision of IoT technologies;
b) The IoT European Platform Initiative (IoT-EPI) develops innovative platform technologies and fosters technology adoption thorough community and business building; and
c) The Connecting Europe Facility (CEF) is a key EU funding instrument to promote growth through targeted infrastructure investment, including the digital realm.

10. International Collaboration, Consensus, and Public-Private Partnerships

Key Findings

- *Cross-government and cross-industry collaboration are perceived to be needed not only to reach consensus on IoT security and security by default guidelines, but also to facilitate information exchange and identify needs and perspectives of other stakeholders.*
- *In particular the World Economic Forum emerges as a suitable platform that possesses a unique ability to focus the attention of decision-makers both in the government as well as in the industry and to provide a forum for IoT security multi-stakeholder cooperation.*
- *The relevance of CSIRTs for the sharing of best practices and information on IoT vulnerabilities was highlighted across various international organisations.*

Along the lines of R&D, training and capacity building, the analysed organisations also emphasise the importance of collaborative approaches and public-private partnerships to reach consensus on IoT security and security by default guidelines. This is primarily evident in regards to standardisation developments, where an multi-stakeholder process would be needed to encourage the use of internationally agreed open standards [6], [18], [26], [52]. Specifically the US, China, Japan, South Korea and India are hereby mentioned as key strategic partners [33], [43]. These cross-collaborative, cross-border engagements are also a means to identify the business communities needs and can foster information exchange [5]. The latter point further refers to the requirement to seek functional information sharing mechanism that allows to respond to IoT security vulnerabilities [5], [14], [19].

Cross-sectoral industry collaboration were also highlighted. The ITU [30] proposes that businesses themselves should work on developing appropriate partnerships to fill capacity gaps and address IoT's security challenges. Although competitive and institutional reasons prevent such open communications channels, informal and formal alliances, such as the Industrial Internet Consortium, can smooth security operations within the IoT market and can be a peer mechanism to share concerns and best practices in order to build a common knowledgebase for risks and remediation strategies [6], [18], [43], [53].

There would also be a need to overcome the suspicion that is prevalent within industry towards the government and hindering the building and maintenance of partnerships due to the fundamental lack of trust [6]. Governments embody a multitude of roles in respect to Internet and IoT security, ranging from being a facilitator, regulator and collaborator, but has sometimes opposing interests to commercial businesses (e.g., the use of vulnerabilities) which may create conflict, obstacles and tensions for effective collaboration.

The World Economic Forum [6] therefore proposes to make use of *blended governance approaches* that would leverage the perspectives of governments, companies, civil society, and academia. The Forum itself is also - due to its unique international multi-stakeholder composition - a suitable platform where the UK could actively seek engagement with other international actors. The World Economic Forum could consequently help to facilitate internationally agreed security by default principles and be a setting were key actors collectively create incentives to ensure built-in security and privacy mechanisms.

Another way to potentially deal with the challenges of industry and governmental collaboration is the effective use of Computer Security Incident Response Teams (CSIRTs). CSIRTs relevance was a topic that was prevalent in many of the analysed international organisations, with various forums emphasising the need to strengthen CSIRT collaboration [5], [18], [19], [38], [54]. From our ongoing research within the PETRAS IoT Hub we expect that CSIRTs and especially Product Security Incident Response Teams (PSIRTs) are going to increase in importance as the IoT ecosystem expands. The international CSIRT network is also an established and accepted structure through which security best practices and information about vulnerabilities can be shared.

Concluding Remarks

It is clear from the findings of this report that discussions around security of IoT systems are relatively immature internationally. There are therefore substantial opportunities for the UK to take the lead internationally in shaping the future governance of the Internet of Things. It is unclear how soon a viable an international mechanism, or consensus, will coalesce around the key themes identified in this report. If the UK wants to influence the formation of IoT working groups, best practices and guidelines internationally, there is currently a window of opportunity to take the lead. The UK's expertise in ICT procurement through its Cyber Essential Scheme and its experience with self-regulatory approaches may therefore be suitable starting points to foster international discussions.

Recommendations

Balance Between Regulation and Self-Regulation

The international consensus on regulation closely follows the UK approach of exhausting existing laws and regulations to regulate the emerging IoT ecosystem. The UK has considerable expertise in the use of market-driven, self-regulation approaches and would be well placed to take a principal role in developing a global approach to regulation of future IoT systems.

Certification and Trust

International thinking on certification aligns closely with the current UK perspective. The upcoming EU certification scheme is the leading approach internationally currently and will likely form the basis for future global developments in this space. The UK should consider either playing an active role in the development of this EU scheme or maintain a watching brief on how thinking evolves.

Standardisation

There is a general recognition of the need to develop open, internationally recognised, market-driven standards and interoperable solutions to support innovation and growth of the IoT. There is an opportunity here for the UK to actively engage and/or take a leading role in the development of these standards using its strong reputation and links in the international standardisation community.

Training and Capacity Building

The global position on training and capacity building closely aligns with the UK skills agenda. This provides an opportunity for the UK to exploit its world-leading education sector to provide both the UK national need and export to the global market.

International Collaboration, Consensus, and Public-Private Partnerships

There is clearly an opportunity to lead on the development of international cooperation, standards, and regulation and to guide the advancement of the international agreements that will be necessary to ensure a safe and security IoT. There is currently a lack of consensus and leadership in most of the international organisations on these subject matters, with The World Economic Forum seeming to be the most obvious forum where all the key players are engaged. This, together with the OECD and potentially the WTO, would likely be the best route to influence the international agenda. There is an opportunity for the UK to direct and shape this debate.

REFERENCES

[1] I. Brass, L. Tanczer, M. Carr, and J. Blackstock, “Secure by Default IoT: Standards and Guidance Landscape Mapping,” PETRAS IoT Hub; Department for Digital, Culture, Media & Sport, London, 2017.

[2] J. Blythe, “Literature Review of Industry Recommendations for Government Levers for Securing the Internet of Things,” Secure by Default, Department for Digital, Culture, Media & Sport, London, 2017.

[3] ENISA, “Cyber Security and Resilience of smart cars: Good practices and recommendations,” European Union Agency for Network and Information Security, Heraklion, Greece, Dec. 2016.

[4] European Commission and AIOTI, “Report on Workshop on Security & Privacy in IoT,” European Commission; AIOTI, Brussels, Jan. 2017.

[5] ASEAN, “ASEAN ICT Masterplan 2020,” The Association of Southeast Asian Nations, Jakarta, 2015.

[6] World Economic Forum, “Global Agenda Council on Cybersecurity,” World Economic Forum, Cologny/Geneva, Apr. 2016.

[7] Dutch Cyber Security Council, “European Foresight Cybersecurity Meeting: Public Private Academic Recommendations to the European Commission About Internet of Things And Harmonization of Duties of Care,” Dutch Cyber Security Council, Cologny/Geneva, 2016.

[8] ENISA, “IoT Security: User awareness,” European Union Agency For Network And Information Security, Heraklion, Greece, Nov. 2016.

[9] European Commission, “COM(2009) 278 final: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Internet of Things: An Action Plan for Europe,” European Commission, Brussels, Jun. 2009.

[10] AIOTI, “Report on Workshop on Security and Privacy in the Hyper-Connected World,” The Alliance for the Internet of Things Innovation, Brussels, 2016.

[11] ENISA, “ENISA Workshop on Cyber security for IoT in Smart Home Environments,” *ENISA*, Oct-2015. [Online]. Available: https://www.enisa.europa.eu/events/copy_of_enisa-workshop-on-cyber-security-for-iot-in-smart-home-environments. [Accessed: 26-Sep-2017].

[12] AIOTI WG11, “Smart Manufacturing,” Alliance for Internet of Things Innovation, Brussels, 2015.

[13] R. Canetti, “Universally composable security: a new paradigm for cryptographic protocols,” in *Proceedings 2001 IEEE International Conference on Cluster Computing*, Las Vegas, Nevada, USA, 2001, pp. 136–145.

[14] OECD, “OECD Digital Economy Outlook 2015,” Organisation for Economic Co-operation and Development, Paris, 2015.

[15] Article 29 Data Protection Working Party, “Opinion 8/2014 on the on Recent Developments on the Internet of Things,” Article 29 Data Protection Working Party, Brussels, 2014.

[16] ENISA, “Smart Hospitals: Security and Resilience for Smart Health Service and Infrastructures,” European Union Agency For Network And Information Security, Heraklion, Greece, Nov. 2016.

[17] IEEE, “Internet of Things (IoT) Security Best Practices,” Institute of Electrical and Electronics Engineers, New York, Feb. 2017.

[18] OECD, “Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document,” OECD Publishing, Paris, 2015.
[19] European Commission, “Conclusions of the Internet of Things public consultation,” European Commission, Brussels, Feb. 2013.
[20] World Economic Forum and Accenture, “Industrial Internet of Things: Unleashing the Potential of Connected Products and Services,” World Economic Forum, Cologny/Geneva, 2015.
[21] AIOTI WG01, “Internet of Things Applications,” Alliance for Internet of Things Innovation, Brussels, 2015.
[22] AIOTI WG04, “AIOTI Digitisation of Industry Policy Recommendations,” The Alliance for the Internet of Things Innovation, Brussels, 2016.
[23] OECD, “The Internet of Things: Seizing the Benefits and Addressing the Challenges,” OECD Publishing, Paris, May 2016.
[24] AIOTI, Cable Europe, and GSMA, “Joint Industry Statement: Enabling Europe to be the Future Leader in IoT and Innovation,” The Alliance for the Internet of Things Innovation, Brussels, 2017.
[25] ITU and CISCO, “Harnessing the Internet of Things for Global Development,” International Telecommuniation Union, Geneva, Switzerland, 2016.
[26] OECD, “OECD Council Recommendation on Principles for Internet Policy Making,” Organisation for Economic Co-operation and Development, Paris, Dec. 2011.
[27] Infineon, NXP, STMicroelectronics, and ENISA, “Common Position on Cybersecurity,” European Union Agency for Network and Information Security, Heraklion, Greece, Dec. 2016.
[28] European Parliament, Council of the European Union, European Economic, Social Committee, and Committee of the Regions, “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,” European Commission;, 2013.
[29] ENISA, “Considerations on ICT security certification in EU: Survey Report,” European Union Agency For Network And Information Security, Heraklion, Greece, Aug. 2017.
[30] ITU, “ITU Internet Report: The Internet of Things,” International Telecommuniation Union, Geneva, 2005.
[31] AIOTI WG04, “AIOTI Working Group 4 – Policy,” Alliance for Internet of Things Innovation, Brussels, Oct. 2015.
[32] European Commission, “SWD(2017) Commission Staff Working Document: Communication on the Mid-Term Review on the Implementation of the Digital Single Market Strategy. A Connected Digital Market for All,” European Commission, Brussels, Oct. 2017.
[33] European Commission, “COM(2016) 176 final: ICT Standardisation Priorities for the Digital Single Market,” European Commission, Brussels, Apr. 2016.
[34] AIOTI WG03, “High Level Architecture (HLA; Release 3.0),” Alliance for Internet of Things Innovation, Brussels, 2017.
[35] ISO/IEC JTC 1/SC 41, “Standard and/or project under the direct responsibility of ISO/IEC JTC 1/SC 41 Secretariat,” *International Organization for Standardization*, 29-Sep-2017. [Online]. Available: https://www.iso.org/committee/6483279/x/catalogue/p/0/u/1/w/0/d/0. [Accessed: 29-Sep-2017].

[36] AIOTI WG05, “Smart Living Environment for Ageing Well,” Alliance for Internet of Things Innovation, Brussels, 2015.
[37] AIOTI WG08, “Smart City LSP: Recommendations Report,” Alliance for Internet of Things Innovation, Brussels, 2015.
[38] European Commission, “SWD(2016) 110 Final: Advancing the Internet of Things in Europe. Digitising European Industry Reaping the full benefits of a Digital Single Market,” European Commission, Brussels, 2016.
[39] European Union Agency For Network And Information Security, *Security and resilience of smart home environments: good practices and recommendations.* Heraklion: ENISA, 2015.
[40] OWASP, “OWASP Secure Coding Practices Quick Reference Guide,” The Open Web Application Security Project, 2010.
[41] ENISA, “Securing Smart Airports,” European Union Agency for Network and Information Security, Heraklion, Greece, Dec. 2016.
[42] ISO/IEC JTC 1, “Smart Cities. Preliminary Report 2014,” International Organization for Standardization, Geneva, Switzerland, 2015.
[43] International Data Corporation and TXT e-solutions, “Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination,” European Commission, Brussels, 2014.
[44] I. Brass, M. Carr, L. Tanczer, C. Maple, and J. Blackstock, “Unbundling the Emerging Cyber-Physical Risks in Connected and Autonomous Vehicles,” Pinsent Masons, London, May 2017.
[45] European Commission, “Workshop Report - Building A European Data Economy,” *European Commission*, 2016. [Online]. Available: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=34617. [Accessed: 26-Sep-2017].
[46] The Greens / European Free Alliance, “#WannaCry: Lessons learned for Security and Liability in the Internet of Things,” *Greens/EFA*, 06-Jul-2017. [Online]. Available: https://www.greens-efa.eu/en/article/event/wannacry/. [Accessed: 23-Jun-2017].
[47] GSMA, “IoT Security Guidelines for IoT Service Ecosystem. Version 1.1,” GSM Association, unknown, 2016.
[48] J. Kohnstamm and D. Madhub, “Mauritius Declaration on the Internet of Things,” presented at the 36th International Conference of Data Protection and Privacy Commissioners, Balaclava, Mauritius, 2014.
[49] ENISA, “Security and Resilience of Smart Home Environments. Good Practices and Recommendations,” European Union Agency for Network and Information Security, Heraklion, Greece, 2015.
[50] AIOTI, “Report on Workshop on Security and Privacy in the Hyper-Connected World,” The Alliance for the Internet of Things Innovation, Brussels, 2016.
[51] AIOTI WG09, “Smart Mobility,” Alliance for Internet of Things Innovation, Brussels, 2015.
[52] AIOTI WG02, “Innovation Ecosystems,” Alliance for Internet of Things Innovation, Brussels, 2015.
[53] GSMA, “IoT Security Guidelines Endpoint Ecosystem. Version 1.1,” GSM Association, unknown, 2016.
[54] GSMA, “IoT Security Guidelines for Network Operators. Version 1.1,” GSM Association, unknown, 2016.

[55] ASEAN, “ASEAN ICT Masterplan 2015,” The Association of Southeast Asian Nations, Jakarta, 2011.
[56] M. Schallbruch, “The European Network and Information Security Directive – a Cornerstone of the Digital Single Market,” in *Digital Marketplaces Unleashed*, Berlin, Heidelberg: Springer, 2018, pp. 287–295.
[57] DSIT, “Discover the OECD Directorate for Science, Technology and Innovation,” Organisation for Economic Co-operation and Development, Paris, 2017.
[58] A. L. Tao, “IoT security not a priority for Asean organisations,” *ComputerWeekly.com*, 29-Mar-2016.
[59] ASEAN, “ASEAN ICT Masterplan 2015: Completion Report,” The Association of Southeast Asian Nations, Jakarta, 2015.
[60] GSMA, “IoT Security Guidelines Overview Document. Version 1.1,” GSM Association, unknown, 2016.

TABLE 1: SUMMARY TABLE OF KEY ISSUES

Issues	Organisations									
	SbD	(Self-) Regulation	Certification & Trust	Standardisation	Procurement	Training & Capacity	Liability	Data	R&D	Collab. & PPP
EC	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
29WP	✓	-	✓	✓	-	-	-	✓	-	-
ENISA	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
AIOTI	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
OECD	✓	✓	-	✓	-	✓	✓	✓	✓	✓
WEF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ASEAN	✓	✓	-	✓	-	✓	-	✓	✓	✓
ISO	✓	✓	-	✓	-	✓	-	✓	✓	✓
ITU	-	✓	✓	✓	-	✓	✓	✓	✓	✓
GSMA	✓	-	-	✓	-	-	✓	✓	-	-
IEEE	✓	-	✓	✓	-	-	-	✓	✓	-

TABLE 2: OVERVIEW OF PRINCIPLES AND BEST PRACTICE FOR IOT SECURITY

Overarching principle	Specific recommendations	References
Strong authentication	Strong authentication by default (ship with password protection)	IEEE, GSMA, OECD, EC, ENISA, AIOTI
	No default passwords	IEEE, GSMA, OECD, ENISA
	Use certificates securely	IEEE, GSMA, ASEAN**, EC, ENISA, AIOTI
	Consider biometrics for authentication	GSMA, WEF, EC, ENISA
	Followed accepted and secure password reset processes	IEEE, GSMA, EC, AIOTI
	Use two-/ multi-factor authentication	IEEE, GSMA, ASEAN, WEF, EC
	Salt, hash and/or encrypt credentials	IEEE, GSMA, OECD, EC, ENISA, AIOTI
	Require “strong” passwords	IEEE, GSMA, WEF, OECD, ENISA, AIOTI
	Reaffirm authentication throughout time of access	WEF, EC, ENISA
Software updates	Routine, reliable secure updates from vendors providing firmware and software patches	IEEE, GSMA, WEF, OECD, 29WP, EC
	Cryptographic checks to allow updates from an authorized source – signed/ verified from trusted source	IEEE, GSMA, WEF, EC, ENISA
	Mechanism for automatic secure software updates	GSMA, OECD, 29WP, ENISA, AIOTI
	Provide users the ability to approve, authorize or reject updates	
	Fall back/rollback option	GSMA, ENISA
	Thoroughly tested updates	GSMA, EC, ENISA
	Ship with most up-to-date stable version	WEF
Device functionality	Offer some functionality or alarm user if internet connectivity/cloud back end fails	EC, ENISA
	Build in controls to disable connectivity or disable ports to mitigate potential threats, while maintaining core product functionality	IEEE, GSMA, EC
Policies	Easy to find and understandable policies covering privacy and security, support policies, data retention	IEEE, GSMA, EC, ENISA
Disclosures and transparency	Empower user to understand what is going on with the device and the data it is sharing	IEEE, GSMA, ISO, ASEAN, OECD, 29WP, EC, AIOTI
	Disclose what will happen to device functionality when services fail	IEEE, 29WP
	Disclose what happens to data when ownership is transferred	IEEE, GSMA, AIOTI
	Disclose what happens when user declines/opts out of policy and the consequences of this to product functionality	EC, AIOTI
	Disclose what rights to remotely decrease IoT device functionality	
	Disclose what sensitive data is collected and how it is used	IEEE, OECD, 29WP, EC, ENISA, AIOTI
	Disclose product capabilities and limitations (e.g. encryption, data communication)	29WP, AIOTI

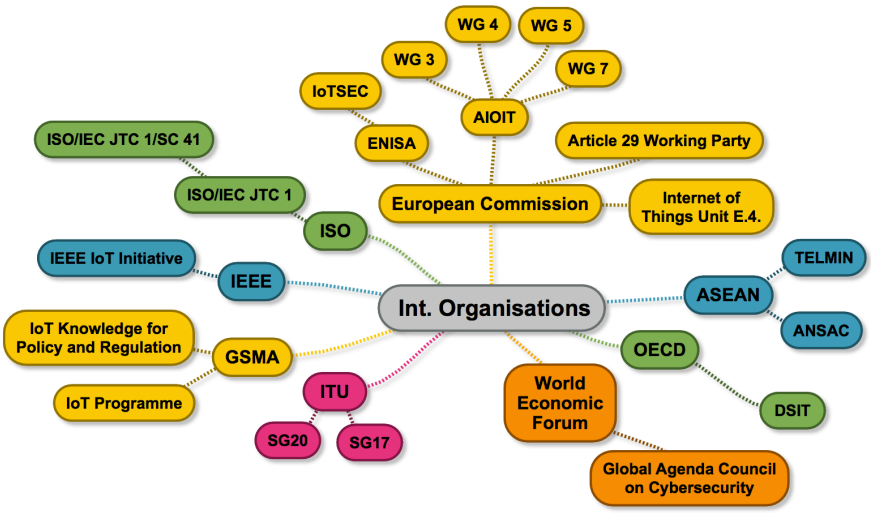
	Disclose duration of support of product including what they should expect at end of lifespan	IEEE, OECD, 29WP, EC, ENISA, AIOTI
	Use QR codes, short URLS and other methods to maximise disclosure at point of sale	GSMA
Reset mechanism	Provide a mechanism to reset to manufacturer state	ENISA
Manufacturer support	Manufacturers should provide clear options on contacts for support	EC
	Methods to contact consumers to disseminate information about software vulnerabilities or other issues	
	Contact information and support forum	
	Online access to manuals and instructions	
	Online and over-the-phone support including a security hotline	
	Support label – to help authorized operator identify it and find support information	IEEE, OECD
Vulnerability reporting and disclosures	Report discovery and remediation of vulnerabilities that pose threats to consumers	WEF, ENISA
	Provide a vulnerability report process	ENISA
Cryptography protocols and best practices	Encryption by default needed, especially appropriate to sensitivity of data	*, EC, ENISA
	Use best practice cryptography protocols	IEEE, WEF, ENISA
Secure the supply chain and associated services	Secure the supply chain, including raw components that the circuit board are composed e.g., the silicon, cryptographic tokens, read-only-memory (ROM), firmware, and other core attributes of an embedded system	GSMA, EC, ENISA, AIOTI
Minimum requirements necessary	Design devices to minimum requirements necessary required for operation	IEEE, GSMA
	Design to collect only the minimum amount of data necessary	29WP, EC, AIOTI
Compliance and risk assessment	Conduct security and data compliance risk assessments including data classification and security across data lifecycle	GSMA, OECD, EC, ENISA, AIOTI
Secure development	Undergo a secure development process (such as threat modelling, inventory of codes)	IEEE, GSMA
Test and harden devices	Test and harden devices	IEEE, GSMA, EC, ENISA, AIOTI
No backdoors or known vulnerabilities	Do not ship with backdoors or known vulnerabilities	GSMA, ENISA
User choice	Allow for data control by the user at any point of the lifecycle	GSMA, 29WP, EC, AIOTI
	Request user confirmation when paring, connecting with devices, services etc.	
	Request users consent to share personal data with third parties	OECD, 29WP, EC, ENISA, AIOTI
	Provide controls to edit privacy settings	GSMA
	Provide privacy-friendly default settings	EC, ENISA, AIOTI
	Provide choice for data collected beyond what is needed for device operation	AIOTI
	Provide opt-in/opt-out requirements for IoT devices	ISO, 29WP, ENISA, AIOTI

	Provide user or proxy option to delete personal data on company services upon end of service with company	IEEE, 29WP, EC, AIOTI
Physical security	Implement measures to help prevent physical tampering of devices and physical access to devices	IEEE, GSMA, EC
Logging	Secure event logging for aiding fault and security management	GSMA, EC, ENISA, AIOTI
Secure device boot	Trusted/secure boot sequence minimises the risk of rogue code being run at boot time	IEEE, GSMA, EC, ENISA, AIOTI
Network segmentation	Establish smaller local networks using VLANs, IP address ranges to create security zones controlled and connected by a firewall	IEEE, ENISA, AIOTI

Note. Adapted from Blythe [2].
*The World Economic Forum [6, p. 12] argues that end-to-end encryption also poses a security challenge for governments trying to "balance national security and law enforcement demands for additional information and the need for security in devices to prevent crime and fraud".
**ASEAN's [55] references on strong authenticity and data disclosure are part of its 2015 ICT Masterplan in relation to ICT. The security guidelines are equally applicable to IoT devices.

APPENDIX A: KEY ORGANISATIONS

Following the extraction of key themes across the analysed international organisations, Appendix A briefly discusses some of these bodies and their respective IoT working groups. These fora are part of a broader landscape of stakeholders that drive the secure by default IoT discussions and are consequently realms the UK government may consider to engage with more closely, actively monitor the activities, and try to use their expertise and publications to deliver evidence-based policy.



1. EUROPEAN COMMISSION

As seen from the above analysis, the European Commission has produced a range of legislative and policy measures that are relevant from an IoT security perspective. These activities are frequently driven by the European Commission's Internet of Things Unit E.4, which is responsible for the policy, research, standardisation, adoption and take up of the IoT. The Unit advances strategic and policy issues and promotes and implements soft law and/or legislative initiatives. Its emphasis on examining a mix of regulatory responses ranging from rule setting, elements of self-regulation and stimulating market mechanisms [56], characterise the Commission's current approach to IoT.

Relevant Publications

Year	Title
2009	COM(2009) 278 Final: Internet of Things — An action plan for Europe
2013	Conclusions of the Internet of Things Public Consultation
	JOIN(2013) 1 Final: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace
2014	Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination
2015	COM(2015) 192 Final: A Digital Single Market Strategy for Europe
2016	Directive (2016/1148): Concerning the Measures for A High Common Level of Security of Network and Information Systems Across the Union
	SWD(2016) 110 Final: Advancing the Internet of Things in Europe

	COM(2016) 176 Final: ICT Standardisation Priorities for the Digital Single Market
	Workshop Report: Building A European Data Economy
	Best Available Techniques Reference Document for the Cyber-Security and Privacy of the 10 Minimum Functional Requirements of the Smart Metering Systems
2017	Report on Workshop on Security & Privacy in IoT
	COM(2017) 228 Final: Communication on the Mid-Term Review on the implementation of the Digital Single Market Strategy. A Connected Digital Single Market for All
	COM(2017) 10 Final: Proposal for a Regulation on Privacy and Electronic Communications

Further Details

Contact Point(s) Internet of Things (Unit E.4)
Events https://ec.europa.eu/digital-single-market/en/content/internet-things-unit-e4

1.1. EU Article 29 Working Party

The Working Party is set up by a representative from the data protection authority of each EU member state, the European Data Protection Supervisor and the European Commission and has so far produced an Opinion 8/2014 on the developments of IoT addressing concerns of its privacy and security [15]. The European Data Protection Board (EDPB) will replace the Article 29 Working Party under the EU General Data Protection Regulation (GDPR 2016/679), with the Working Party being incorporated in EDPB's activities. The newly established EDPB will function as the EU's independent data protection authority. This does not make the Working Parties activities obsolete, but rather requires the UK to monitor the activities of this institutions in the next year more closely.

Relevant Publications

Year	Title
2014	Opinion 8/2014 on the on Recent Developments on the Internet of Things

Further Details

Contact Point(s) Article 29 Working Party

1.2. European Union Agency for Network and Information Security

ENISA is currently actively involved in the IoT space and is to be transformed into the EU Cybersecurity Agency to assist member states in dealing with cyber- and IoT-related attacks. ENISA's efforts on IoT security are manifold and range from the evaluating of threats, the promotion of security good practices e.g., cybersecurity of smart homes [39] to the liaison with policy makers. ENISA is frequently coordinating IoT-specific events, including its workshop on cybersecurity for IoT in smart home environments in October 2015, its IoT security and privacy workshop in January

2017, and its upcoming Europol-ENISA IoT security conference from the 18-19 October 2017 in The Hague. ENISA is consequently one of the most active bodies involved in the development of recommended IoT security practices and recently set up an IoT Security Expert Group (IoTSEC) which aims at gathering experts in the domains of the entire IoT spectrum.

Relevant Publications

Year	Title
2015	Security and Resilience of Smart Home Environments: Good Practices and Recommendations
2016	Smart Hospitals: Security and Resilience for Smart Health Service and Infrastructures
	Cyber Security and Resilience of Smart Cars: Good Practices and Recommendations
	Securing Smart Airports
	IoT Security: User Awareness
	Common Position On Cybersecurity
2017	Considerations on ICT Security Certification in EU: Survey Report

Further Details

Contact Point(s) ENISA's IoT Security (IOTSEC) Experts Group
Events https://www.enisa.europa.eu/events/listing#b_start=0

1.3. The Alliance for the Internet of Things Innovation

Part of the European Commission's IoT activities was the launch of the Alliance for Internet of Things Innovation (AIOTI) in March 2015. AIOTI should support the creation of an innovative and industry driven European IoT ecosystem and flags the intention of the European Commission to work closely with various stakeholders. This member-driven alliance is active in building consensus on IoT reference architectures and supports standardisation to fill any identified gaps. AIOTI has 13 working groups, with AIOTI's Working Group 3 (Standardisation), Working Group 4 (IoT Policy), Working Group 5 (Smart Living Environment for Aging Well) and Working Group 7 (Wearables) being probably of most relevance to DCMS. AIOTI agrees on its organisational strategy on its annual General Assembly, in which members consisting of corporates, SMEs, governmental organisations, research institutes and end-users come together.

Relevant Publications

Year	Title
2015	WG01 Internet of Things Applications
	WG02 Report on Innovation Ecosystems
	WG04 Report on Policy Issues
	WG05 Smart Living Environment for Ageing Well
	WG06 Smart Farming and Food Safety Internet of Things Applications – Challenges for Large Scale Implementations
	WG07 Wearables Report
	WG08 Smart City LSP: Recommendations Report

	WG09 Smart Mobility Report
	WG11 Smart Manufacturing Report
2016	WG03 IoT LSP Standard Framework Concepts
	Report on Workshop on Security and Privacy in the Hyper- Connected World
	AIOTI Digitisation of Industry Policy Recommendations
2017	Joint Industry Statement: Enabling Europe to Be the Future Leader in IoT and Innovation
	WG03 High Level Architecture (HLA)

Further Details

Contact Point(s)	AOITI Working Group 3 (Standardisation) AOITI Working Group 4 (IoT Policy) AOITI Working Group 5 (Smart Living Environment for Aging Well) AOITI Working Group 7 (Wearables)
Events	https://aioti.eu/events/

2. Organisation for Economic Co-operation and Development

The OECD is still primarily concerned with 'traditional' cybersecurity questions, but has in December 2014 organised its first and so far, only IoT-related event at the OECD Technology Foresight Forum 2014 in Paris. Nonetheless, one relevant OECD body to engage with is the Directorate for Science, Technology and Innovation [57]. DSIT is involved in declarations on the authentication for e-commerce, the protection of privacy on global networks, and laid the ground work for the OECD Council Recommendation on Principles for Internet Policy Making that urges policy makers to protect the openness of the Internet to unleash innovation, creativity and economic growth [26].

Relevant Publications

Year	Title
2011	OECD Council Recommendation on Principles for Internet Policy Making
2015	Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document
	OECD Digital Economy Outlook 2015
2016	The Internet of Things: Seizing the Benefits and Addressing the Challenges
	Ministerial Declaration on the Digital Economy ('Cancún Declaration')

Further Details

Contact Point(s)	OECD Directorate for Science, Technology and Innovation (DSTI)
Events	https://www.oecd.org/newsroom/upcomingevents/

3. World Economic Forum

In 2012, the World Economic Forum set up a Global Agenda Council on Cybersecurity, which is one of its 80 Global Agenda Councils and explores and develops practical solutions to the challenging questions on changing cybersecurity trends, including IoT. The council's members include cybersecurity experts, policy-makers, business executives, civil society representatives and academics and possesses a unique ability to focus the attention of decision-makers at the highest levels of both the public and private sectors. Two ongoing initiatives are worth exploring, including the 'Digital Protocol Network on AI, IoT and the Future of Trust' as well as the 'Digital Protocol Network on Industrial IoT Safety'. Most recently, the World Economic Forum participated together with more than twenty other relevant stakeholders in the first European Foresight Cybersecurity meeting, organised by the Dutch Cyber Security Council [7]. The report that derived from this meeting proposes recommendations to the European Commission and focused in parts at security by default principles. It is expected that the World Economic Forum and its Council on Cybersecurity will increase in relevance as security of IoT concerns expand. It might be a suitable forum for the UK government to seek cooperative partners in its efforts on security by default.

Relevant Publications

Year	Title
2015	Industrial Internet of Things: Unleashing the Potential of Connected Products and Services
2016	Global Agenda Council on Cybersecurity

Further Details

Contact Point(s)	World Economic Forum's Global Agenda Council on Cybersecurity
Events	https://www.weforum.org/events/

4. Association of Southeast Asian Nations

ASEAN's member countries represent a fast-growing economic region that are anticipated to be an important market for the IoT. Nonetheless, according to Intel Security, ASEAN is not highlighting the importance of security in their IoT developments enough [58]. This is reflected in their publications such as their ICT Masterplans in 2015 [55] and 2020 [5]; both barely touch on security and issues related to the emerging IoT ecosystem. Instead, ASEAN seems to be primarily focused on the development and economic growth of ICT in the region. The ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN) plays an important role in this regard and hold regular summits where digital aspects are being discussed. A further development has contributed significantly to the enhancement of security in the region involves the establishment of the ASEAN Network Security Action Council (ANSAC). Outcomes arising from ANSAC meetings include greater cybersecurity awareness, the establishment of a common framework for network security, and the development of an ASEAN cybersecurity incident handling and escalation procedure [59].

Relevant Publications

Year	Title
2011	ASEAN ICT Masterplan 2015
2015	ASEAN ICT Masterplan 2020

Further Details

Contact Point(s) ASEAN Telecommunications and IT Ministers Meeting (TELMIN)

5. International Organization for Standardization

ISO's ISO/IEC JTC 1 Information Technology technical committee subsumes the ISO/IEC JTC 1/SC 41 Internet of Things and Related Technologies subcommittee. Created in 2017, the subcommittee is responsible for the standardisation developments in the IoT realm, including sensor networks and wearables technologies and provides guidance to other entities such as the International Electrotechnical Commission. As of September 2017, there are currently eleven IoT-specific standards published, with 9 more under development. We strongly expect that ISO/IEC JTC 1/SC 41 is a central body that will drive the international discussions on the interoperability and security of the IoT [35].

Relevant Publications

Year	Title
2014	ISO/IEC JTC 1: Internet of Things (IoT) Preliminary Report 2014
	Smart Cities: Preliminary Report

Further Details

Contact Point(s) Technical Committee ISO/IEC JTC 1/SC 41 Internet of Things and Related Technologies

6. International Telecommunication Union

ITU has two study groups that are worth highlighting. Firstly, ITU-T Study Group 17 (SG17 - Security) coordinates all security-related work across the agency and is often working in cooperation with other standards development organisations and various ICT industry consortia. SG17 deals with a broad range of standardisation issues, including cybersecurity and the security of applications and services for the IoT. ITU-T Study Group 20 (SG20 - IoT, Smart Cities & Communities) is working to address the standardisation requirements of IoT technologies, with an initial focus on IoT applications in smart cities and communities. While the focus is not necessarily on consumer products, some of their publications may be transferable to other contexts.

Relevant Publications

Year	Title
2005	ITU Internet Report: The Internet of Things
2012	Overview of the Internet of Things
2016	Harnessing the Internet of Things for Global Development

Further Details

Contact Point(s)	ITU's ITU-T Study Group 17 (SG17; Security) ITU-T Study Group 20 (SG20; Internet of Things, Smart Cities and Communities)
Events	http://www.itu.int/en/events/Pages/Calendar-Events.aspx?sector=ITU-T

7. GSM Association

GSMA as an international trade body representing the interest of mobile operators worldwide has produced dedicated IoT Security Guidelines [60]. These guidelines are a set of GSMA security recommendations that are intended to help the nascent IoT industry establish a common understanding of IoT security issues. The Overview Document (CLP.11) complements the IoT Security Guidelines for IoT Service Ecosystems (CLP.12), Endpoint Ecosystems (CLP.13) and Network Operators (CLP.14). These guidelines are backed by an IoT Security Assessment scheme to provide a proven and robust approach to end-to-end security and part of GSMA's Internet of Things Programme which is an industry initiative designed to mobile operators accelerate the delivery of compelling and secure IoT solutions. GSMA also offers a IoT Knowledgebase for Policy and Regulation which contains a variety of resources including case studies, consultations, market statistics and forecasts. The online tool is designed to help policymakers and regulators to learn more about international emerging policy and regulatory best practices.

Relevant Publications

Year	Title
2016	IoT Security Guidelines: An Overview Document
	IoT Security Guidelines for Service Ecosystems
	IoT Security Guidelines for Endpoint Ecosystems
	IoT Security Guidelines for Network Operators
	Automotive IoT Security: Countering the Most Common Forms of Attack

Further Details

Contact Point(s)	GSMA's GSMA Internet of Things Programme GSMA's IoT Knowledgebase for Policy and Regulation
Events	https://www.gsma.com/iot/events/

8. Institute of Electrical and Electronics Engineers

IEEE as a professional association is active in the IoT space not only through its academic engagements but also through the IEEE Internet of Things (IoT) Initiative which was launched in 2014. The latter serves as the gathering place for the global technical community working on the IoT and provides a platform where professionals can learn, share knowledge, and collaborate. The IEEE IoT Technical Community is engaged in developing a widely-accepted definition of the IoT and offers an IoT Scenario programme to highlight use cases and potential privacy and security concerns. The latter can be a suitable platform for policy makers to fully understand the application, implementation, and execution of IoT in the real world.

Relevant Publications

Year	Title
2017	Internet of Things (IoT) Security Best Practices

Further Details

Contact Point(s)	IEEE Internet of Things (IoT) Initiative
Events	https://iot.ieee.org/conferences-events.html