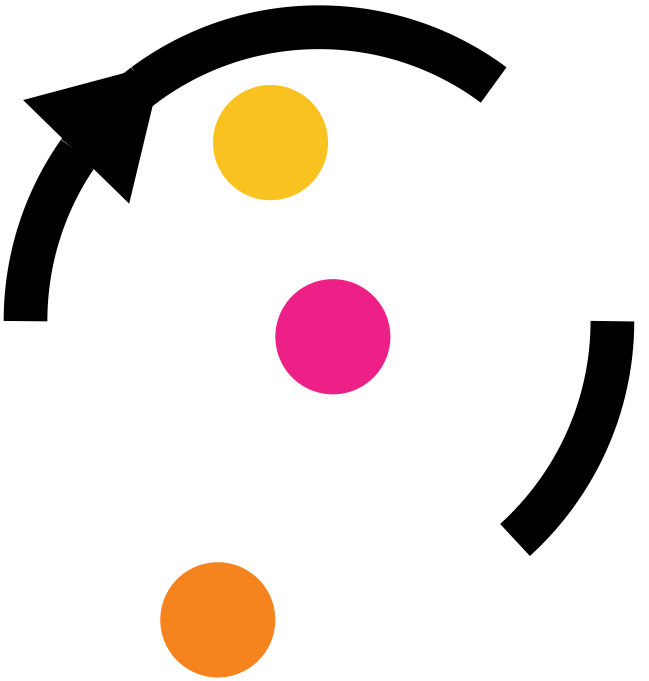
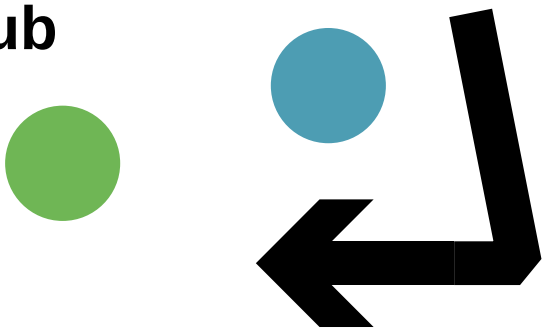
Summary literature review of industry recommendations and international developments on IoT security



PETRAS IoT Hub



Leonie Tanczer
John Blythe
Fareeha Yahya
Irina Brass
Miles Elsden
Jason Blackstock
Madeline Carr

TABLE OF CONTENTS

INTRODUCTION

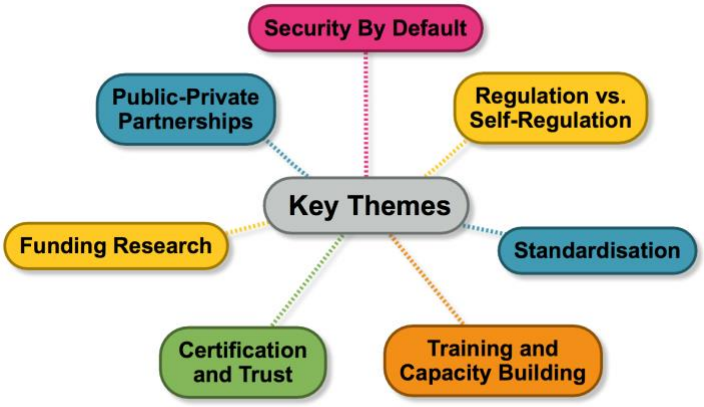
The Department for Digital, Culture, Media and Sport (DCMS) commissioned the PETRAS IoT Research Hub, a consortium of nine leading UK universities that work together to explore critical issues in privacy, ethics, trust, reliability, acceptability, and security of the IoT to conduct two separate literature reviews.[1] The first, on industry recommendations for government to improve IoT security and the second, on the current international developments around IoT security. There were two aims to these reviews: (i) identify the key themes emerging from the literature and (ii) identify international consensus around core Security by Design principles for the IoT.

In this report, we first summarise the emerging themes from the two reviews, then provide recommendations for government and finish with an overview of the consensus around Secure by Design principles.

[1] This literature review represents an analysis of publicly available reports made by industry associations and international organisations. It does not capture the independent position of industry or international experts expressed in other primary research currently conducted.

INDUSTRY RECOMMENDATIONS

We conducted a scoping literature review between May and July 2017[2] and included[3] industry reports that provided recommendations for government action.[4] Analysis of the industry reports indicated a number of key issues of focus including the role of regulation, trust labels and standards. Below, we present an overview of the key themes that emerged from the review.



Regulation vs. Self-Regulation
There was general consensus that industry was in favour of self-regulation to allow for growth and innovation in IoT. An incremental and flexible approach was preferred to address evolving threats. Conversely, independent security researchers such as Bruce Schneier were often in favour of legally-binding rules and regulations, arguing it is the best option for dealing with the increasing cyber-physical convergence that IoT brings.

Certification and Trust
The role for a trust label to inform consumer decision making was mixed across industry players. Some were in favour, as it provides a visible means for consumers to understand the security of a product. These players were in favour of a label that was: flexible (to allow for online and offline communication), co-designed by government and industry, and aligned with international standards. However, there was recognition amongst industry that cybersecurity is not as easily measurable as

---

[2] Final amendments to this scoping literature review were incorporated in November 2017.
[3] Privacy issues were excluded from the review, although they may require further investigation in the future.
[4] Reports from the following institutions were reviewed: Alliance for Internet of Things Innovation (AIOTI), Cloud Security Alliance, Consumer Technology Association, Ericsson, HP, Infineon, NXP, STMicroeletronics, European Union Agency for Network and Information Security (ENISA), Intel, Internet Society, McKinsey Global Institute, Microsoft, Ofcom, Online Trust Alliance, Software and Information Industry Association, and Telecommunications Industry Association.

other labelling schemes (such as energy) and expressed concerns around what the label would actually represent and who would carry out the certification.

Training and Capacity Building
Industry was in favour of heightening consumer awareness of the risks associated with IoT and emphasised the need for educational investment in school and universities curricula and wider training programs.

Standardisation
Industry want standards that are open, voluntary, collaborative and consensus-based. Most reports were in favour of industry working collaboratively with government to develop standards, but there was concern that too much government intervention is this space may impact on interoperability and routes to market.

Funding Research
A few industry reports discuss the need for government to fund future research on IoT security and to develop industry standards.

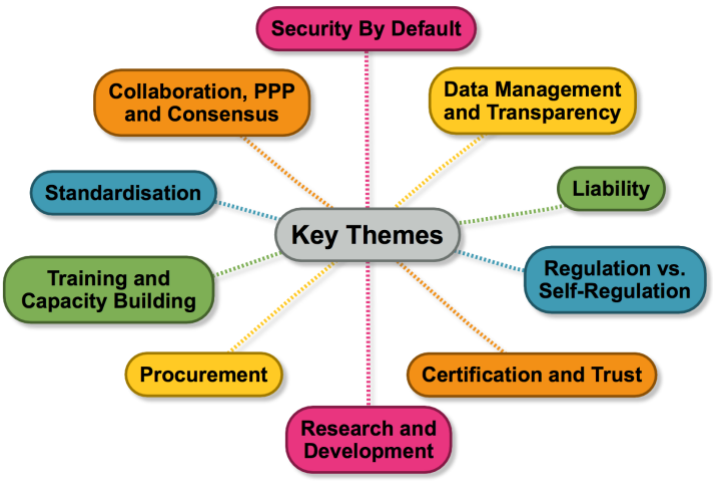
Promote Security by Design Principles and Best Practice
Industry wants government to promote security by design but also to recognise that more sector-specific product development and risk assessment guidelines will be required.

Public-Private Partnerships
To address the issue of IoT security, industry expressed the view that there needs to be ongoing collaboration between the public and private sector in order to drive good practice.

INTERNATIONAL DEVELOPMENT ON IOT SECURITY

We conducted a scoping literature review between September and October 2017[5] and included[6] reports from the leading eleven international fora[7] that are shaping the global governance and policy conversations about the security of the IoT.

Our analysis reveals that there have been some nascent international conversations about the policy implications 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 the content and nature of these debates varies and they are not always inclusive of a wide range of stakeholders. Below, we summarise ten of the most commonly shared themes.



Security by Default/Design Measures
Security by default and security by design are concepts that are frequently used interchangeably. Measures for secure by default/design 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. A recent development in this space is the publication of ENISA's

[5] Final amendments to this scoping literature review were incorporated in December 2017.
[6] Privacy and trade-related issues were excluded from the reviews, although they may require further investigation in the near future.
[7] Reports from the following institutions were reviewed: European Commission, EU Article 29 Working Party, European Union Agency for Network and Information Security (ENISA), Alliance for the Internet of Things Innovation (AIOTI), Organisation for Economic Co-Operation and Development (OECD), World Economic Forum (WEF), Association of Southeast Asian Nations (ASEAN), International Organization for Standardization (ISO), International Telecommunication Union (ITU), GSM Association (GSMA), and Institute of Electrical and Electronics Engineers (IEEE).

Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures in which detailed security measures and good practices are outlined.

Balance between Regulation and Self-Regulation
International organisations' focus of attention is currently on the enforcement of existing laws and regulations in opposition to the introduction of new legislation**.** Self- and a mix of voluntary and legally-binding regulations are perceived as the best near-term options to facilitate the growth of the IoT. The update, adaption, and harmonisation of existing regulations 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).

Certification and Trust
Contrary to the mixed review by UK industry (above) the certification and labelling of IoT products and services was generally referred to in the international literature as potentially advantageous for both users and manufacturers and as 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 framework is a first attempt to explore compliance of specified requirements. It is recommended on a voluntary basis, and may provide a worked example of debates surrounding potential benefits and challenges.

Standardisation
The development and promotion of open, internationally-recognised, market-driven standards and interoperable solutions is emphasised across all analysed institutions. The IoT security standards landscape is currently highly fragmented, with several international industry alliances proposing de facto standards and (self-)certification schemes. Although there are signs of convergence towards a set of core technical and organisational requirements for IoT security among these organisations (see Table below), gaps still persist. The need for standards alignment offers an opportunity for the UK government to play a leading role in international efforts to deliver security and interoperability of IoT devices and services.

Procurement
IoT procurement is not a focus point of the analysed international organisations. However, there are some national developments such as the US proposed *Internet of Things (IoT) Cybersecurity Improvement Act of 2017*. The nature of the global supply chain and the imperative of coordinating international procurement poses an opportunity for the UK government to foster these debates and best practices globally.

Training and Capacity Building
The analysed international organisations highlight that 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.

Liability
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 ongoing IoT developments, although clarification on particular principles could be supported through policy documents and guidance. Several organisations highlight that a review and potential change to product safety and liability rules should occur as the IoT develops.

Data Management and Transparency
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 IoT services. Data security and data management are relevant factors for a potential IoT certification scheme.

Research and Development
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.

International Collaboration, Consensus, and Public-Private Partnerships
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 government as well as across 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.

Concluding Remarks

It is clear that industry recognise the importance of securing the Internet of Things (IoT) and are keen to work alongside the government in their efforts. Industry are concerned that too much intervention may impact on innovation and government should allow industry the opportunity to self-regulate. Industry are keen to see developments in standards, the promotion of security by design, capacity building and exploring the role of trust marks.

Discussions in international organisations around IoT security are relatively immature. There are therefore substantial opportunities for the UK to take the lead in shaping the future governance of the IoT. It is unclear how soon a viable international mechanism, or consensus, will coalesce around the key themes identified in this report. If the UK wishes to influence the formation of IoT working groups, best practices and guidelines, 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 of promoting an environment for self-regulation may therefore be suitable starting points to foster international discussions.

Recommendations

Balance Between Regulation and Self-Regulation

There is an international consensus on promoting self-regulation, although there is increasingly a mix of positions, some quite in favour of regulation. The UK would be well placed to take a principal role in developing a global approach to regulation of future IoT systems, given its expertise in the use of market-driven, self-regulatory approaches.

Standardisation

Internationally and within industry, there is a general recognition of the need to promote 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 mobilise its world-leading education sector to provide both the 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 international agreements that will be necessary to ensure a safe and secure 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 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.

Certification and Trust

The proposed EU cybersecurity certification scheme may form the basis for future international discussions in this space. While the certification process is meant to be of voluntary nature, the EU proposal includes an obligation for member states to implement the institutional requirements to support the scheme at the national level. This expectation – and concerns such as the measurability of cybersecurity, the consistency and equivalence of evaluation methods as well as the enforceability of certificates across the entire lifecycle of IoT products and services – continue to be the subject of debate.

Over the next year, the UK's ongoing involvement in the negotiations on the certification scheme provides a potential forum for advancing the UK's leadership in this space. The UK has an opportunity to drive the development of specified certification criteria and may, in the course of these negotiations, explore alignment with self-governance and standardisation agendas pursued elsewhere.

OVERVIEW OF PRINCIPLES AND BEST PRACTICE FOR IOT SECURITY

Presented below is a tabular summary of the key overarching principles around best practice for IoT security. We have included recommendations that have been referenced at least twice in reports and use the following colours to indicate frequency:

- Green – Referenced in 10 or more reports
- Orange – Referenced in 5-10 reports
- Yellow – Referenced in less than 5 reports

Overarching principle	Specific recommendations	
Strong authentication	Strong authentication by default (ship with password protection)	
	No default passwords	
	Follow accepted and secure password reset processes	
	Use two-/multi-factor authentication	
	Use certificates securely	
	Consider biometrics for authentication	
	Salt, hash and/or encrypt credentials	
	Require “strong” passwords	
	Reaffirm authentication throughout time of access	
Software updates	Routine, reliable secure updates from vendors providing firmware and software patches	
	Cryptographic checks to allow updates from an authorized source – signed/verified from trusted source	
	Mechanism for automatic secure software updates	
	Fall back/rollback option	
	Thoroughly tested updates	
	Ship with most up-to-date stable version	
Device functionality	Build in controls to disable connectivity or disable ports to mitigate potential threats, while maintaining core product functionality	
	Offer some functionality or notify user if internet connectivity/cloud back end fails	
Policies	Easy to find and understand policies covering privacy and security, support policies, data retention	

Disclosures and transparency	Empower user to understand what is going on with the device and the data it is sharing	
	Disclose duration of product support including what to expect at end of lifespan	
	Disclose what sensitive data is collected and how it is used	
	Disclose what happens to data when ownership is transferred	
	Disclose what will happen to device functionality when services fail	
	Disclose what happens when user declines/opts out of policy and the consequences of this to product functionality	
	Disclose product capabilities and limitations (e.g. encryption, data communication)	
Reset mechanism	Provide a mechanism to reset to manufacturer state	
	Support label – to help authorized operator identify device and find support information	
	Manufacturers should provide clear options on contacts for support	
	Mechanism for dissemination of information about software vulnerabilities or other issues to consumer	
Vulnerability reporting and disclosures	Report discovery and remediation of vulnerabilities that pose threats to consumers	
	Provide a vulnerability report process	
Cryptography protocols and best practices	Encryption by default, especially in instances where sensitivity of data is being collected	
	Use best practice cryptography protocols	
Secure the supply chain and associated services	Secure the supply chain, including raw circuit board components e.g., cryptographic tokens, read only memory (ROM), firmware, and other core attributes of an embedded system	
Minimum requirements necessary	Design devices to minimum requirements necessary required for operation	

	Design to collect only the minimum amount of data necessary	
Compliance and risk assessment	Conduct security and data compliance risk assessments including data classification and security across the data lifecycle	
Secure development	Undergo a secure development process (such as threat modelling, inventory of codes)	
Test and harden devices	Test and harden devices	
No backdoors or known vulnerabilities	Do not ship with backdoors or known vulnerabilities	
User choice	Provide opt-in/opt-out requirements for IoT devices	
	Provide user or proxy option to delete personal data on company services upon end of service with company	
	Request users consent to share personal data with third parties	
	Allow for data control by the user at any point of the lifecycle	
	Provide privacy-friendly default settings	
	Provide controls to edit privacy settings	
	Provide choice for data collected beyond what is needed for device operation	
Physical security	Implement measures to help prevent physical tampering of devices and physical access to devices	
Logging	Secure event logging for aiding fault and security management	
Secure device boot	Trusted/secure boot sequence minimises the risk of rogue code being run at boot time	
Network segmentation	Establish smaller local networks using VLANs, IP address ranges to create security zones controlled and connected by a firewall	

REFERENCES

A. L. Tao, “IoT security not a priority for Asean organisations,” ComputerWeekly.com, 29-Mar-2016.

AIOTI WG01, “Internet of Things Applications,” Alliance for Internet of Things Innovation, Brussels, 2015.

AIOTI WG02, “Innovation Ecosystems,” Alliance for Internet of Things Innovation, Brussels, 2015.

AIOTI WG03, “High Level Architecture (HLA; Release 3.0),” Alliance for Internet of Things Innovation, Brussels, 2017.

AIOTI WG04, “AIOTI Digitisation of Industry Policy Recommendations,” The Alliance for the Internet of Things Innovation, Brussels, 2016.

AIOTI WG04, “AIOTI Working Group 4 – Policy,” Alliance for Internet of Things Innovation, Brussels, Oct. 2015.

AIOTI WG05, “Smart Living Environment for Ageing Well,” Alliance for Internet of Things Innovation, Brussels, 2015.

AIOTI WG08, “Smart City LSP: Recommendations Report,” Alliance for Internet of Things Innovation, Brussels, 2015.

AIOTI WG09, “Smart Mobility,” Alliance for Internet of Things Innovation, Brussels, 2015.

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

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

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.

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.

ASEAN, “ASEAN ICT Masterplan 2015,” The Association of Southeast Asian Nations, Jakarta, 2011.

ASEAN, “ASEAN ICT Masterplan 2015: Completion Report,” The Association of Southeast Asian Nations, Jakarta, 2015.

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

AT&T, “The CEO’s Guide to Securing the Internet of Things. AT&T Cybersecurity Insights Volume 2”, 2016. Available from https://www.business.att.com/cybersecurity/docs/exploringiotsecurity.pdf.

B. Schneier, “Click Here to Kill Everyone”, 2017. Retrieved from http://nymag.com/selectall/2017/01/the-internet-of-things-dangerous-future-bruce-schneier.html

BITAG, “Internet of Things (IoT) Security and Privacy Recommendations: A Uniform Agreement Report”. A Broadband Internet Technical Advisory Group Technical Working Group Report, 2016. Available from https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

Consumer Technology Association, “Internet of Things : A framework for the next administration”, 2016. Retrieved from https://www.cta.tech/cta/media/policyImages/policyPDFs/CTA-Internet-of-Things-A-Framework-for-the-Next-Administration.pdf

CSA, “Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products”. Presented by the IoT working Group, Cloud Security Alliance, 2016. Available from https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf.

CSA, “Security Guidance for Early Adopters of the Internet of Things (IoT)”, Cloud Security Alliance, 2015. Retrieved from https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

DSIT, “Discover the OECD Directorate for Science, Technology and Innovation,” Organisation for Economic Co-operation and Development, Paris, 2017.

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.

ENISA, “Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures,” European Union Agency For Network And Information Security, Heraklion, Greece, Nov. 2017.

ENISA, “Considerations on ICT security certification in EU: Survey Report,” European Union Agency For Network And Information Security, Heraklion, Greece, Aug. 2017.

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

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].

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

ENISA, “Securing Smart Airports,” European Union Agency for Network and Information Security, Heraklion, Greece, Dec. 2016.

ENISA, “Security and Resilience of Smart Home Environments. Good Practices and Recommendations,” European Union Agency for Network and Information Security, Heraklion, Greece, 2015.

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

Ericsson, “IoT Security: Ericsson White Paper”, February 2017. Retrieved from https://www.ericsson.com/assets/local/publications/white-papers/wp-iot-security-february-2017.pdf

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

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.
European Commission, "COM(2016) 176 final: ICT Standardisation Priorities for the Digital Single Market," European Commission, Brussels, Apr. 2016.
European Commission, "Conclusions of the Internet of Things public consultation," European Commission, Brussels, Feb. 2013.
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.
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.
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].
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.
European Union Agency For Network And Information Security, Security and resilience of smart home environments: good practices and recommendations. Heraklion: ENISA, 2015.
GSMA, "IoT Security Guidelines Endpoint Ecosystem. Version 1.1," GSM Association, unknown, 2016.
GSMA, "IoT Security Guidelines for IoT Service Ecosystem. Version 1.1," GSM Association, unknown, 2016.
GSMA, "IoT Security Guidelines for Network Operators. Version 1.1," GSM Association, unknown, 2016.
GSMA, "IoT Security Guidelines Overview Document. Version 1.1," GSM Association, unknown, 2016.
HP, "Securing the Internet of Things: Explore security and privacy in an interconnected world", Hewlett-Packard, 2015. Retrieved from http://h20195.www2.hpe.com/V3/getpdf.aspx/4aa6-3369enw
I. Brass, L. Tanczer, M. Carr, and J. Blackstock, "Secure by Default IoT: Standards and Guidance Landscape Mapping," PETRAS IoT Hub; (Working Paper, available upon request), London, 2017.
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.
IEEE, "Internet of Things (IoT) Security Best Practices," Institute of Electrical and Electronics Engineers, New York, Feb. 2017.
Infineon, NXP, STMicroelectronics, and ENISA, "Common Position on Cybersecurity," European Union Agency for Network and Information Security, Heraklion, Greece, Dec. 2016.
Intel, "Policy Framework for the Internet of Things (IoT)", 2014. Retrieved from https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/policy-iot-framework.pdf

International Data Corporation and TXT e-solutions, “Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination,” European Commission, Brussels, 2014.

Internet Society. “The Internet of Things: An Internet Society Public Policy Briefing”, 2015. Retrieved from https://www.internetsociety.org/wp-content/uploads/2015/10/ISOC-PolicyBrief-Privacy-20151030-nb-1.pdf

IoT SF. “Connected Consumer Products: Best Practice Guidelines”, IoT Security Foundation, 2016. Available from https://iotsecurityfoundation.org/wp-content/uploads/2016/12/Connected-Consumer-Products.pdf

IOTiap, “Principles, Practices and a Prescription for Responsible IoT and Embedded Systems Development”, 2017. Available from https://www.iotiap.com/principles.pdf.

ISO/IEC JTC 1, “Smart Cities. Preliminary Report 2014,” International Organization for Standardization, Geneva, Switzerland, 2015.

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].

ITU and CISCO, “Harnessing the Internet of Things for Global Development,” International Telecommuniation Union, Geneva, Switzerland, 2016.

ITU, “ITU Internet Report: The Internet of Things,” International Telecommuniation Union, Geneva, 2005.

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.

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.

McKinsey Global Institute, “The Internet of Things: Mapping the value beyond the hype”, 2015.

Microsoft, “Cybersecurity policy for the Internet of Things”, 2017. Retrieved from https://mscorpmedia.azureedge.net/mscorpmedia/2017/05/IoT_WhitePaper_5_15_17.pdf

OECD, “Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document,” OECD Publishing, Paris, 2015.

OECD, “OECD Council Recommendation on Principles for Internet Policy Making,” Organisation for Economic Co-operation and Development, Paris, Dec. 2011.

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

OECD, “The Internet of Things: Seizing the Benefits and Addressing the Challenges,” OECD Publishing, Paris, May 2016.

Ofcom, “Review of latest developments in the Internet of Things”, March 2017. Retrieved from https://www.ofcom.org.uk/__data/assets/pdf_file/0007/102004/Review-of-latest-developments-in-the-Internet-of-Things.pdf

Online Trust Alliance, ‘IoT Security & Privacy Trust Framework v2.0”, 2017. Available from

https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework2.1.pdf.

Online Trust Alliance, “Challenges of the connected auto, gym, home & office”, 2017. Retrieved from https://otalliance.org/system/files/files/resource/documents/iot_sharedroles.pdf

OWASP, “IoT Security Guidance”. The Open Web Application Security Project, 2016. Available from https://www.owasp.org/index.php/IoT_Security_Guidance

OWASP, “OWASP Secure Coding Practices Quick Reference Guide,” The Open Web Application Security Project, 2010.

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.

Software and Information Industry Association, “Empowering the Internet of Things: Benefits, Solutions, and Recommendations for Policymakers”, 2016. Retrieved from http://www.siia.net/Portals/0/pdf/Policy/Reports/Empowering the Internet of Things.pdf

Telecommunications Industry Association, “Realizing the Potential of the Internet of Things: Recommendations to Policy Makers”, 2015. Retrieved from https://www.tiaonline.org/sites/default/files/pages/TIA-White-Paper-Realizing_the_Potential_of_the_Internet_of_Things.pdf

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].

World Economic Forum and Accenture, “Industrial Internet of Things: Unleashing the Potential of Connected Products and Services,” World Economic Forum, Cologny/Geneva, 2015.

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