Navigating and Informing the IoT Standards Landscape

A Guide for SMEs and Start-ups

Prepared by BSI and
PETRAS Internet of Things Research Hub

Irina Brass
Kruakae Pothong
Mariyam Hasham

bsi.

PETRAS

Contents

Executive summary

This paper summarizes some of the main opportunities and challenges that IoT SMEs (small and medium size enterprises) and start-ups face when trying to develop connected products and associated IoT services in a responsible and transparent manner. The challenges highlight standardization priorities for these players.

The findings are based on primary research combining inputs from:

- ongoing research conducted by the PETRAS IoT Research Hub;
- discussions that took place during a BSI IoT/1 Committee workshop entitled *SMEs and Start-ups Operating in the IoT Space;* and
- expert guidance from members of the BSI IoT/1 Committee.

The workshop was organized by the BSI IoT/1 Committee in July 2018 and received representation from key stakeholders across the IoT ecosystem, including government and trade and consumer associations.

Key challenges

We identify several challenges for SMEs and start-ups developing IoT products and services. These result from the still fragmented policy and standards landscape for IoT security, safety, privacy, data integrity and data protection:

- Understanding trade-offs between security, operational efficiency and interoperability.
- Managing and implementing security, privacy and data protection in an integrated manner, with associated third-parties across the IoT ecosystems.
- Legal uncertainty over IoT product and service liability, data protection and data integrity, especially due to highly complex data flows.

The consequence of these challenges is that SMEs and start-ups can be disadvantaged in the predominantly price-driven market for consumer IoT products and services. This may hinder brand reputation and business growth.

Priority areas for standardization for IoT SMEs and start-ups

The world of IoT standards and policy making is moving very quickly and in a good direction. However, through the BSI IoT/1 workshop, we identified three priority areas for standardization for IoT SMEs and start-ups:

1. Live repositories of IoT vulnerabilities and best practices: IoT SMEs and start-ups require up-to-date IoT vulnerabilities reports and use case databases to learn from and develop their safety, security and privacy capabilities accordingly. There is scope for standards bodies to lead on the establishment of these repositories as a component of their mission to provide more adaptive IoT standards.

2. Secure client and customer identity management: IoT SMEs and start-ups require integrated standards for conducting safety-security-privacy testing and verification, and for communicating their compliance with best practices in an easy and meaningful manner (e.g. via a label or trust mark). They require supply chain and data management standards to facilitate their data integrity and security assessment across the associated supply chain. These standards can help SMEs and start-ups recover costs of compliance more effectively and provide clarity for negotiating terms with associated third parties and insurance providers.

3. Tiered risk assessment and management standards: IoT SMEs and start-ups need procedures for tiered assessment and management of IoT products and services, based on the combination of their vertical and product/service risk profile, as well as the interaction with the rest of the associated IoT ecosystem. These procedures should help mitigate business risks and uncertainties resulting from price-driven purchasing decisions.

Introduction

The IoT (Internet of Things) has seen exponential growth in recent years [1], from the proliferation of connected consumer devices in the home to the increasing integration of data collection, communication and actuation technologies in transport, manufacturing, industrial systems and the management of critical infrastructures and utilities. While IoT growth and adoption rates are still contested, with estimates that there will be between 20 and 25 billion connected devices worldwide by 2022 [2], one thing is certain: the IoT market is growing.

In this increasingly connected world, consumers and market players alike are asked to put their trust in devices and systems that capture, process and provide services based on the protection, security and integrity of data. However, achieving, ensuring and assuring trust in the IoT is not straightforward. Several consumer organizations have already reported that consumers are increasingly concerned about the security of their products and the protection of their personal data [3]. Similarly, manufacturing associations and industry consortia have identified several challenges when trying to make informed decisions about the security of the IoT solutions they integrate into their product line, their businesses and/or their new services [4][5][6][7][8].

Progress has been made on the policy and standards-development front (Appendix B). In 2018, DCMS (UK Department for Digital, Culture, Media and Sport) published the *Code of Practice for Consumer IoT Security*, aimed to help IoT businesses implement security practices into their own design processes [9]. In February 2019, ETSI published Technical Specification 103 645, *Cyber Security for Consumer Internet of Things*, which builds on the DCMS Code of Practice and brings together essential measures that are widely considered good practice in consumer IoT security [10]. At BSI, privacy by design and interoperability standards for smart consumer products and services are currently under development contributing to several regional and international standards-making initiatives [11] [12]. At ISO, standards are also being developed to set a framework and methodology for IoT trustworthiness [13]. In addition, manufacturers of IoT devices can now test, verify and certify their products across several features – functionality, interoperability and security - through the Open Connectivity Foundation Certification scheme [14] and the IoT BSI Kitemark [15].

However, the IoT standards landscape is still highly complex and fragmented especially across verticals [16] (Appendix B). This is particularly challenging for SMEs and start-ups moving into the IoT space. These important market players have raised several concerns about the IoT, which are shared across consumer associations, industry, governments and international organizations.

- What are the baseline security and privacy requirements for IoT products and services, and how do these fit with existing sector-specific standards and best practices?
- What are the qualities and properties that earn consumer trust in IoT products and services, and how best to communicate good security and privacy practices to consumers?
- What are the best risk management practices to ensure the constant monitoring of connected devices and associated IoT services?
- How will these affect the current lifecycle of products and services, and what opportunities and challenges does the IoT bring for product line continuity, business confidence and brand reputation?

This white paper identifies the main concerns that IoT SMEs and start-ups face when developing new products and services, and summarizes their priority areas for IoT standardization.

1. Critical issues in IoT product and service development: Implications for IoT SMEs and start-ups

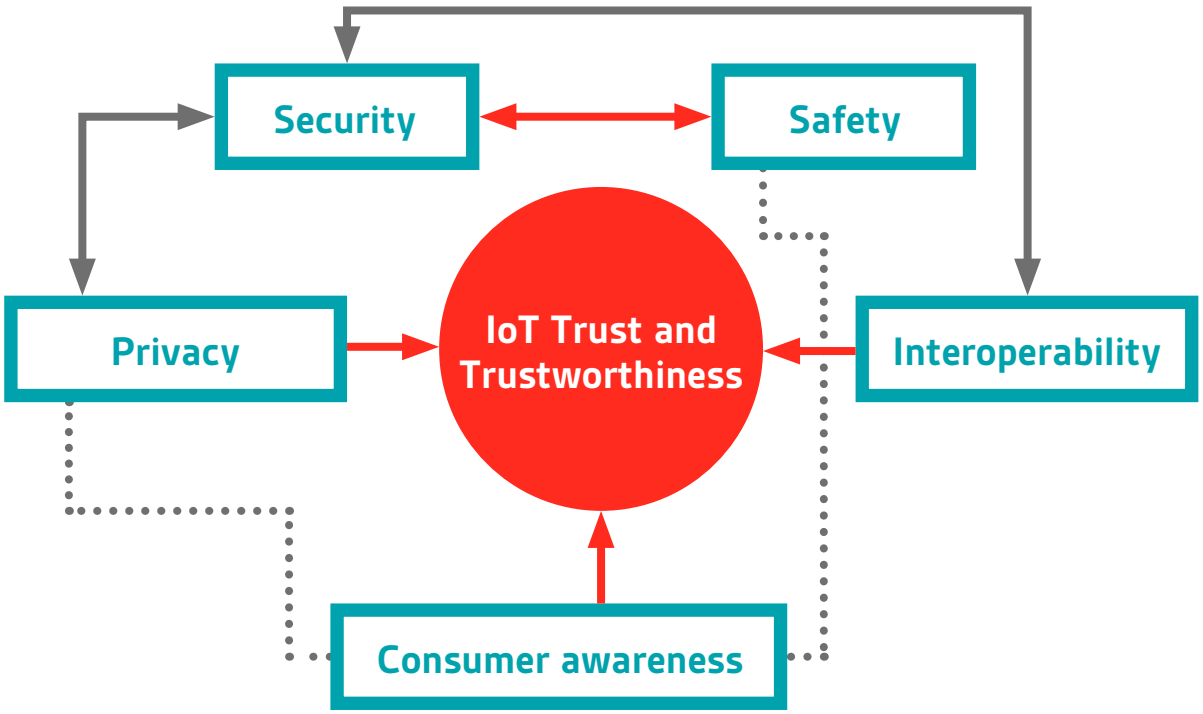
Participants at the BSI IoT/1 workshop, *SMEs and Start-ups Operating in the IoT Space,* focused their attention on six key issues of concern in IoT products and services:

1. security
2. safety
3. privacy and data protection
4. interoperability
5. transparency, and
6. promoting consumer and business awareness.

The discussions showed the interconnected nature of these facets of IoT trust and the trade-offs businesses are faced with when trying to implement all of them in a coherent, consistent and cost-effective manner (Figure 1).

Despite full agreement among experts concerning the relationship between security, safety and privacy, workshop participants indicated strong connections between the features of IoT products, the type of data generated through the use of these products, and their overall security, safety and privacy. During the workshop, a consensus was reached that, in the context of consumer IoT, cybersecurity is seen as an enabler of data protection, data integrity and privacy, and is a feature just as important as safety.

Figure 1: Critical issues in IoT product and service development



Participants in the workshop identified several commercial and consumer behaviours that are a challenge to the development of IoT products and services and have an impact on the complex task of IoT business innovation, as well as on the development of comprehensive and effective IoT standards.

1.1 Security

There are four areas of concern regarding security.

Security in the connected ecosystem: The scale of connectivity among objects and devices communicating with one another, as well as with other systems, heightens the importance of security across the IoT ecosystem. One compromised device can serve as a foothold, providing a gateway to compromising other devices and systems connected to it, as observed in the case of the home environment or industrial IoT [17][18]. While we tend to look at IoT product security in isolation, most IoT products are integrated with other smart devices in highly connected environments. In this case, IoT manufacturers can be faced with a business trade-off between product security and interoperability.

Smart security cameras are a good example. Consumers want these cameras to be easily integrated with existing smart home platforms, but product manufacturers have no guarantee that the platforms themselves are secure. It is not viable for IoT SMEs and start-ups to build their own home management ecosystem in order to ensure its security, as it is not feasible to compete with existing big players. And, if consumers ask for product interoperability with several home platforms, then designing secure IoT products will not be sufficient to guarantee the security of the entire home ecosystem. In addition, as the IoT environment is shifting from *IoT as product* to *IoT as service*, the importance of secure cloud services becomes a paramount aspect of IoT ecosystem security.

A business case for providing security updates: Even when looking at consumer IoT products, there are known discrepancies between their physical lifecycle and the time span for supplying support/patches/updates for the smart function of physical products. IoT manufacturers are expected to update software, but the point at which it becomes commercially unviable differs from business projections modelled on the lifespan of physical products. Most physical products outlive security updates at the intelligence layer (i.e. the smart aspect of connected devices). However, consumers are likely to continue using the physical products as long as the hardware still functions as expected.

Domestic appliances are a good example. Their lifespan can vary between five and ten years. What should customers do if software is no longer supported? Ideally, they should be able to switch off the smart functionality of the device once the software is no longer supported. Transparency at the point of purchase about these issues is needed. But this transparency could encourage purchasing decisions against products that display information about their software support timeframe, if not all manufacturers adhere to the same principle. IoT manufacturers need to consider the software update policy they offer in relation to the lifespan of their product line.

Building security expertise in enterprises: Cybersecurity is an increasingly important add-on to IoT products and services, but it is not a familiar component of business know-how for a lot of enterprises. Companies operating in the IoT space are increasingly concerned about their limited expertise in providing robust cybersecurity for their devices and services. They recognize that there is a problem with easily identifying what 'good' data protection and security means, and how to best convey it to their customers.

For IoT manufacturers with limited resources, being able to target both interoperability and cybersecurity could be achieved by working together with established smart ecosystem providers to integrate responsible security in the entire ecosystem. While limited security expertise can be inhibiting for IoT manufacturers, it presents opportunities for established players to act as partners or third parties, and to promote a distributed approach to software maintenance.

Costs: It remains unclear how and to what extent IoT businesses can recover the cost of complying with the latest best practices for IoT security, data protection and integrity, as well as commercial transparency. IoT manufacturers and service providers stressed that compliance with these guidelines doesn't determine consumer purchasing decisions. While complying with best practices can improve brand reputation, it is less clear how the costs of compliance bring positive financial gains to small IoT businesses, especially if consumers are not willing to pay more for secure IoT products and services.

Implications for IoT SMEs – Security

SMEs whose business relies on adding connectivity to their existing product line have reported limited expertise in designing and implementing security in their connected devices and adjacent services. While this gap presents opportunities for partnerships with established players and third-party security support services, these cannot address all the challenges IoT SMEs face. These challenges include:

- Assessing trade-offs between:
  - security and operational effectiveness (e.g. between providing software maintenance and investing in new product development);
  - investing in the development of interoperable products, the development of entire ecosystems (which might have a higher level of security) and providing IoT security as a service.
- Negotiating device security through third-party contracts with established players.

1.2 Safety

In the context of IoT devices, safety is heavily discussed in connection with security. Concerns over safety manifest in two ways: known risks or harm, and uncertainty about future risks.

The known risks and harms in IoT revolve around the misuse and abuse of their remote-control functions. The remote-control function poses risks to safety when decisions to switch devices or systems on and off are made without clear and accurate information about the locations to which the remote-control is applied. For example, remotely controlling temperatures in the home or particular rooms in the homes of elderly people, without clear information regarding occupancy or the needs of residents, could result in ill health.

In addition, manufacturers remarked that they should be able to lock down devices remotely when they become unsafe to use. Risk assessment frameworks and standards should capture both known risks and uncertainty over future IoT risks. Discussions in the BSI IoT/1 workshop, *SMEs and Start-ups Operating in the IoT Space,* highlighted the need for a risk assessment framework for the remote-control functionality. Workshop participants deemed that remote-control functions must pass risk assessment for safety, not just security. This position is aligned to that of several consumer associations, which propose that assessing the security of a device should become a component of product safety regulation (i.e. security for safety [3]).

Implications for IoT SMEs – Safety

Several IoT SMEs are concerned about the risk assessment and governance frameworks they are currently using to map out the integrated security and safety risks associated with their connected products. Some of the reported challenges include:

- Assessing the interaction between security and safety features once connected products are deployed in different consumer contexts and on several platforms (e.g. smart homes).
- Limited availability of risk assessment guidelines for IoT SMEs interested in developing security and safety maintenance services for connected products via a subscription model.
- Developing contingency plans for compromised devices and providing incentives for customers to share their data with manufacturers for safety reasons.

1.3 Privacy and data protection

A key concern in this area stems from the function of smart devices to collect, communicate and store data about their customers in the cloud. IoT firms are increasingly concerned about the best way in which to integrate product and service security assessment into their Data Protection Impact Assessment, which is fundamental to making business risk assessment frameworks compliant with the GDPR (General Data Protection Regulation) [19].

Participants at the BSI IoT/1 workshop agreed that without security, it is not possible to ensure data protection and privacy. However, in the absence of standards on the security of IoT products and services that go beyond the baseline set by the DCMS *Code of Practice*, how can businesses assess the risks of their new ventures? And how do they estimate the cost of compliance with responsible product/service security practices on top of their data protection compliance costs? For example, IoT businesses looking to provide remote smart appliance maintenance services need to fully understand, assess and govern this risk in terms of data protection, security of service and product safety.

Implications for IoT SMEs – Privacy

Several IoT SMEs and start-ups have found there is no clear guidance on how to implement and integrate data protection, security, and safety impact assessments into their business models. Some of the reported challenges include:

- Estimating the costs of implementing, monitoring and communicating compliance with best practices for data protection, security and safety.
- Uncertainty about how risk management standards and guidelines are helping IoT SMEs and start-ups assess their data protection and security risks. An accurate assessment is needed so that they can get the right insurance policy in place.
- Uncertainty about their legal liability as IoT product and service providers, especially in an increasingly complex data flow and processing ecosystem.

1.4 Interoperability

Connectivity — the fundamental aspect of IoT devices such as locks, bikes or domestic appliances — requires a common language to ensure interoperability among devices, systems and platforms. IoT businesses see the current lack of standardized ontologies and data communication protocols as a barrier. IoT businesses are aware that consumers do not want to be locked into single supplier ecosystems; they want interoperable products and services that speak and understand each other in a seamless manner.

1.5 Transparency

For responsible IoT businesses, the protection of their customers' data and privacy is underpinned by transparency and apparency. Apparency refers to the communication model between the IoT product or service provider and their customers. The model centres on communicating data flows and transfers, the associated risks of using a particular technology, and the options available in B-2-C interactions [20]. At the moment, responsible IoT businesses think there is a lack of labels or trust marks that they can use to convey meaningful information about their security and data processing practices, and this is affecting their openness to innovate at the IoT product and service level.

1.6 Raising consumer and business awareness

All the participants at the BSI IoT/1 workshop stressed the importance of raising awareness about known vulnerabilities of IoT devices, as well as how to communicate compliance with best practices in privacy and security in B-2-B and B-2-C interactions. Having formal testing and certification frameworks, as well as clear communication policies, were seen as paramount [21].

Consumers lack awareness of the privacy, security and safety risks associated with a large number of IoT devices that are on the market. The consequences of the rapid uptake of IoT devices in everyday life are not fully understood by consumers [22]. Neither are consumers aware of the added costs that IoT businesses have to internalize in order to comply with best practice for transparency, privacy and security. This lack of awareness is reflected in consumers' purchasing decisions, which are mostly driven by price only and this doesn't give IoT businesses a commercial incentive to invest in providing transparency, device and service security, and privacy.

Educating businesses is needed because of the varying degrees of IoT maturity across different sectors. Sharing and understanding the specific B-2-B and B-2-C dynamics that occur in different verticals and sub-markets is very important. Learning from more mature IoT sectors, such as Building Information Modelling or Industrial IoT, is fundamental to the responsible development of IoT consumer products.
All the participants at the workshop stressed the importance of raising awareness about known vulnerabilities of IoT devices, as well as how to communicate best practice for privacy and security in B-2-B and B-2-C interactions.

Implications for IoT SMEs – Awareness

Consumer awareness is highly important for IoT SMEs because the predominantly price-driven consumer purchasing decisions have direct implications on SMEs' competitiveness and business continuity. Poor consumer awareness about what a secure connected device looks like and how to identify manufacturers that are acting responsibly means that it is a challenge for SMEs to make a business case for:

- The implementation of best practices for privacy and security in IoT products and services.
- Testing and certifying new IoT products.
- Investing in new personnel and building brand reputation based on responsible security, privacy and data protection in product design.

1.7 Accessing knowledge

All participants of the BSI IoT/1 workshop agreed that there is a need for a comprehensive knowledgebase on IoT vulnerabilities and best practices for business use and development. It should include information about discrete and sector-specific vulnerabilities, emerging risks, and relevant use cases [23]. The information repositories that do exist have not been mapped in a systematic manner and require an advanced level of technical expertise. At the moment, there is not much live data on current IoT vulnerabilities that can be accessed by IoT SMEs and start-ups.

This leads to a demand for risk assessment frameworks, both horizontal and domain specific (e.g. a framework for a secure home), to help IoT businesses assess risks associated with connected products and services. IoT SMEs are also interested in assessing the consumer risk appetite, i.e. trying to understand whether the residual risk is within an acceptable tolerance for the consumer.

Implications for IoT SMEs – Knowledge

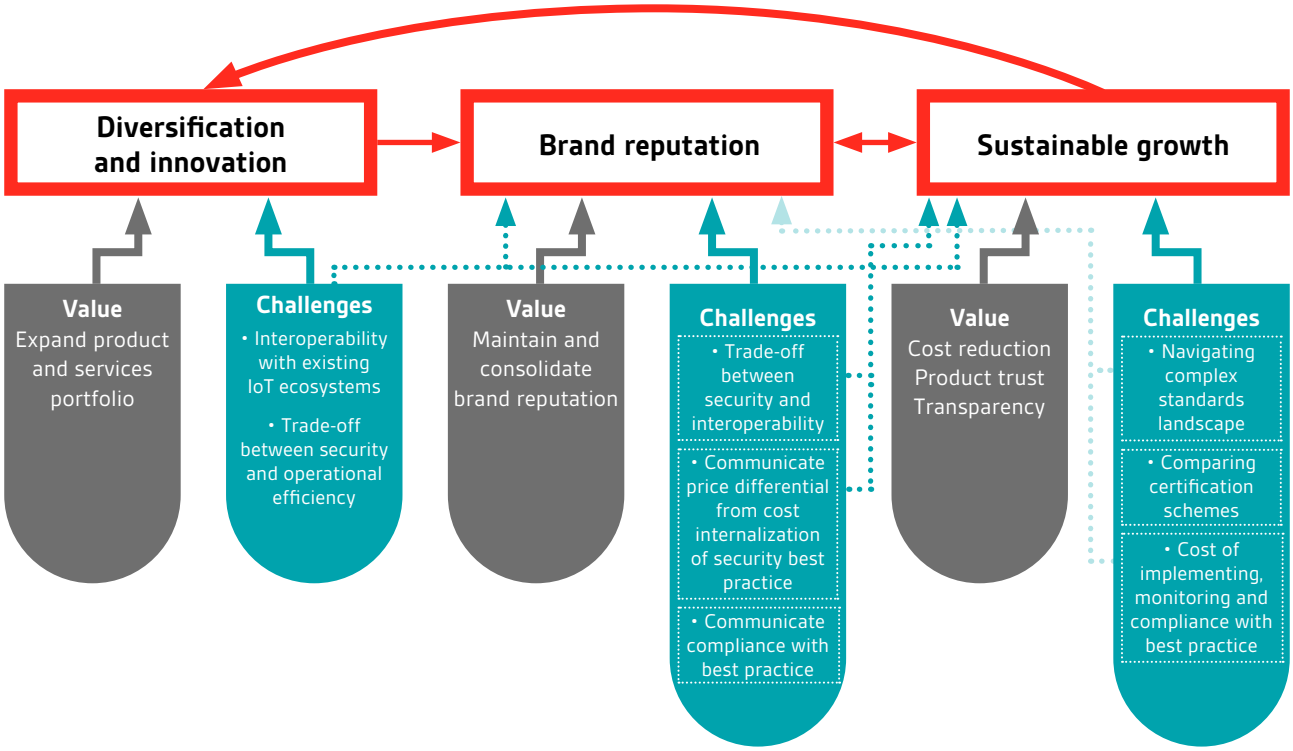
SMEs need access to the knowledge base and learnings from various sectors in order to tailor a risk assessment framework to their IoT products and services, while taking into consideration the broader ecosystem of associated products, systems and platforms. The absence of easily accessible repositories on IoT and sector-specific vulnerabilities, emerging risks, and risk management best practices means that IoT SMEs and start-ups:

- lack awareness of the latest best practices on security and privacy by design, informed by ongoing and new vulnerabilities; and
- are uncertain about the benefits and costs of investing in new IoT products and services.

1.8 Summary of critical issues for IoT SMEs and start-ups

Overall, IoT SMEs and start-ups face several challenges when trying to develop new connected products and digital services while following responsible business innovation practices. Figure 2 summarizes these challenges.

Figure 2: Key issues for SMEs operating in the IoT Space



The IoT SMEs and start-ups present at the BSI IoT/1 workshop, *SMEs and start-ups operating in the IoT space,* agreed that there are benefits to be gained from innovating in a responsible manner. Diversifying their product and service line contributes to brand reputation and sustainable business growth. Building and maintaining brand reputation by adding data capture, analytics, automation and communication capabilities to existing products promotes sustainable business growth. In return, sustainable business growth enhances brand reputation and contributes to business maturity by further diversifying product and service lines and taking on new ventures and opportunities.

While SMEs are keen to extend their portfolios to offer IoT products and services, the absence of horizontal standards makes it difficult for SMEs to effectively and efficiently integrate their products and services with third-party providers or platforms. An example is the absence of standardized ontologies for communication across devices, systems and platforms. The absence of this standard to facilitate interoperability risks consumer lock-in and limits SMEs' competitiveness, particularly against more established brands with broader products and service portfolios. Poor interoperability also limits the prospects of SMEs being able to work towards providing comprehensive IoT services. Calculating trade-offs between security and operational efficiency (e.g. choosing between continuing security patches and rolling out new products) is yet another challenge faced by IoT SMEs. Miscalculation of these trade-offs, combined with poor interoperability across devices, systems and platforms can damage brand reputation and inhibit business growth.

Many SMEs venturing into the IoT market have the reputation of their established products and services to protect. Before adding connectivity to their existing products and services they need to consider the trade-off between security and interoperability. Unlike established companies, with horizontally and vertically integrated products and services, most SMEs rely on interoperability with third-party products, services, systems, and platforms. However, SMEs have little control over third-party security, privacy and data protection practices, which can create or break trust in their products and services.

SMEs also face challenges justifying price differentials resulting from responsible manufacturing and service development practices, because consumers' purchasing decisions are driven predominantly by price. The ability to communicate the benefits of compliance with best practice to the consumer is vital for SMEs' competitiveness, brand reputation and sustainable business growth; if the consumer understands the price differential and is willing to pay it, this justifies the cost.

Having limited resources, SMEs are keen to be cost efficient in implementing the core principles that contribute to trust in their products and services. While standards can serve as operational tools for implementing these core principles, and certification schemes can serve as compliance signifiers, the IoT standards landscape is still complex. As a consequence, SMEs are not always clear about which testing, verification and certification scheme to use. Another challenge SMEs and established IoT businesses face is that comprehensive standards and certification for dynamic digital features – such as security and data integrity – are more difficult to achieve than, for instance, assessing and certifying the safety of a product or system. Collectively, the costs of compliance, of monitoring and of communicating it in a meaningful and effective manner are likely to disadvantage SMEs more than they do established businesses.

2. SMEs' priority areas for IoT standards development

Research conducted across academia, industry, trade and consumer associations has already highlighted several priority areas for IoT standardization, ranging from the development of ontologies to ensure interoperability of IoT devices and systems, to establishing principles and methodologies for assessing the trustworthiness of IoT systems and services [24][25].

While some of these issues are already addressed by national and international standards, participants at the BSI IoT/1 workshop, *SMEs and start-ups operating in the IoT space*, highlighted three standardization priority areas for IoT SMEs. We present these below and provide examples of three IoT SMEs present at the workshop:

1. **Live repositories of IoT vulnerabilities and best practices**
2. **Secure customer and client identity management, respectful of individual privacy and adhering to data protection requirements**
3. **Tiered risk assessment and management standards**

2.1 Live repositories of IoT vulnerabilities and best practices

Formal national and international standards bodies have a unique position in setting standards that represent consensus knowledge about what 'best practice' looks like, based on expert input from a broad range of stakeholders, from individual firms to trade and consumer associations, to government and academia. The fact that membership of national standards development committees is free and open to all in the UK is also crucial in the IoT context. However, developing formal standards can take a long time, especially as the consultation and review process is public.

In the interim, standards bodies can be proactive and establish repositories of IoT vulnerabilities and live use case databases. This will help IoT SMEs and start-ups share and access information, contribute to and learn from each others' product and service development, business challenges and best practices (see section 1.7). This falls in line with the need to produce more adaptive standards and to establish a community of IoT businesses, trade and consumer associations, which BSI has championed [26][27].

Case Study: ERA Home Security

ERA has a long standing reputation for home security products (e.g. locks, doors, windows). In rolling out smart versions of existing home security products, the company positions itself at the intersection of edge products and the communications layer of the IoT ecosystem. The vision is to provide consumers with a sense of security, convenience and flexibility through security solutions ranging from smartware, cloud-based alarm systems and community security applications.

The common smart functionalities added to ERA's existing products include remote-control configuration and access to its home security products and systems. Connectivity is central to these functionalities. Security of the devices as well as the supporting communication infrastructure, is of paramount importance to maintaining ERA's reputation. Interoperability is also significant for building customer confidence, trust, return on investment, consumer choice and promoting greater adoption.

Since connectivity is integral to the functionalities of ERA's smart security solutions, the company is concerned with:

- security of the supporting communications networks, systems and components;
- protocols on communication networks and their interoperability; and
- data protection.

ERA is most concerned not only with the security built into its own products, but also third-party platforms (e.g. home management systems) on which ERA places its products and services and also the supporting communications networks, components and storage systems. This has implications for customer trust and confidence in the ERA brand. Yet, ERA struggles to navigate the varying levels of security offered by these third parties.

The heterogeneity of the protocols for communications networks and systems complicates product development. This is due to heavy reliance on connectivity and interoperability with third-party devices, platforms and services. Hinderance to connectivity and interoperability could impinge on product uptake as well as the SME's return on investment.

The information generated by the smart security solutions is valuable and can have implications for customers' safety and security. Safety and security are the foundations of ERA's reputation and customer trust in the products. Hence, ERA is concerned with the location and security of the storage space for the data that is generated by the usage of its smart security solutions.

To efficiently navigate the heterogeneity of the IoT ecosystem, ERA expects standards to:

- set minimum requirements for security of IoT devices, platforms and communication systems;
- give guidelines for auto-generated password or access codes; and
- unify communication protocols for interoperability.

Accessing and sharing information about IoT security vulnerabilities and the development of secure devices, platforms and communication systems is important for ERA. In addition, ERA believes that the establishment of testing and verification schemes, such as Open Connectivity Foundation Certification Scheme [14] or the BSI IoT Assurance Services and Kitemark [15], are paramount for validating and communicating the high security and reliability of their product and services range.

2.2 Secure client and customer identity management

Several IoT SMEs need to know the most appropriate way to provide real-time IoT services that ensure the management of client and customer identities in a safe and secure manner. For SMEs providing IoT services, it is paramount to take a continuous and integrated approach to developing security-safety-privacy impact assessment.

But understanding the best way to integrate security, safety and data protection impact assessment into a business model is not straightforward (see section 1.3). Integrated standards for conducting and showing compliance with security and data protection requirements are crucial for IoT SMEs. These can allow SMEs to reduce costs and showcase adherence to best practice to their partners and customers.

IoT SMEs and start-ups would also like to see new supply chain and data management standards that allow them to assess data integrity and security in the entire data supply chain. These standards can provide clarity when negotiating with third parties and insurance providers.

Case Study: GeoEnable

GeoEnable is best known for Asset Information Management (e.g. utilities and rail) and geospatial and geomatics solutions (e.g. land/location survey, GIS, CAD, remote sensing). Positioning itself in the IoT ecosystem as an information management consultancy, GeoEnable targets large organizations, such as airports, rail and highway authorities, hospitals and convention centres. Through advanced web-mapping, remote sensor and location-based analytics, the company enables clients to provide precise location intelligence, data workflow mapping and geospatial solutions for all aspects of mapping.

The core functionality of GeoEnable's service is to help clients achieve resource optimization, which can be facilitated, for example, by physical asset management and resource optimization. To do this, geospatial and location data collection and analytics are key. These processes require GeoEnable to advise their clients on how to deliver transparency (of data collection, processing, use and reuse) in compliance with data security standards, data quality standards and privacy regulations. The clients also need to assess the possibility for individuals to be tracked or identified, in line with GDRP requirements. In addition, secure communication and storage of data is fundamental to ensure the integrity of the data that is used to provide real-time services.

Again, the complexity of the data supply chain could make it more challenging for GeoEnable to advise their clients. One of the concerns raised is the lack of understanding of the use of data-as-a-service in real time by a wider community. This is especially the case in situations when real-time dashboards and KPIs for asset and facility performance monitoring would bring great benefits, but at the moment the current processes and workflows involved for data integration and the underlying technologies can be too complex for non-technical professionals to understand.

Given GeoEnable's interest in geospatial and location data, the company would like to see interoperability standards that align geospatial, survey and location data with that of the IoT in a secure and accurate manner.

2.3 Tiered risk assessment and management standards

IoT SMEs are using several formal risk assessment and management standards at the moment. These span across normative risk management guidance such as BS ISO 37000, *Risk management* [29], the ISO 9000 family of *Quality management* standards [30] (including *Supply chain quality management*) or the ISO 27000 family of *Information security management system* standards [31].

However, IoT SMEs find that these standards allow them to only partly understand, map, prepare and mitigate the risks associated with their IoT products and services. This is in part due to the complex interactions between connected devices, complex data flows and new digital service models.

The IoT SMEs that took part in the BSI IoT/1 workshop stressed that they would like the introduction of a regulatory framework for connected products and digital services, possibly updating the current product safety and product liability regulatory frameworks, which would allow the development of standards that take into account different risk classifications for connected products and services. This could be similar to the REACH EU regulation for chemicals [32], which establishes procedures for how firms should collect and assess information on the properties and hazards of certain substances.

IoT SMEs would like standards that provide basic priority provisions for devices that have certain general features, and a tiered approach for different product and service categories based on verticals, use case-generated risk profiles, or a combination of both. Such standards would also help to avoid the development of separate device and software policies or warranties, which most IoT SMEs find risky for their business models, especially if customers do not understand the difference.

Case Study: GTech

GTech is a well-known brand for floor care products. Positioning itself as an edge provider, GTech is expanding into the consumer IoT market with an aim to make existing products smart, offering added value for consumers. These smart products range from consumer electronics to home appliances (e.g. e-bikes, vacuum cleaners, floor care or garden appliances).

The common added IoT features among these products are primarily connectivity with other devices, systems and services. In terms of added functionality, the smart vacuum cleaner is designed to assist with maintenance, health status monitoring, updates and usage reports. The added functionality of e-bikes includes: motor assisted peddling; increased speed and climbing ability, adaptability to different terrains, tracking of the bikes for security as well as journey profiling, energy data consumption collection, and smart lock and storage.

Given the added IoT features and the smart functionalities of the featured products, GTech is primarily concerned with the security of the device, communication and data. This security concern has three dimensions: technical, relationships with third parties in the IoT ecosystem, and relationships with customers.

The technical dimension refers to the security built into the devices (e.g. smart vacuum cleaners and e-bikes) and the security of the connections between the devices and third-party platforms, networks, and the smart grid for tariff information.

The security of the connectivity — particularly with third-party platforms, networks and systems — implies a relationship with a wide range of third parties where there is a lot of uncertainty in terms of expectations and scope of liability on both GTech, as an edge provider, and the third parties concerned. The security of the intelligence added to devices and the resulting data from customers' usage of the product implies a more dynamic relationship with and more responsibilities towards customers. This new type of customer relationship raises concerns for GTech about the expectations of consumers regarding the length of software maintenance and updates. GTech is mindful to balance these expectations with financial viability. In addition to security, GTech has concerns about compliance with GDPR and the implications of the varying degrees of sensitivity of data collected for safety (e.g. health stats, location data, energy consumption). Thus, different IoT products and services could have higher associated risks than others.

Given the aforementioned complexity and uncertainties that the added IoT functionality and features present, GTech acknowledges that the smart functionalities added to simple products could appear overcomplicated and thus off-putting for consumers and would therefore require careful thinking, planning and management. To navigate these complexities and uncertainties, consumer IoT standards are expected to address security, privacy and safety issues in an integrated manner. Having standards to address these issues would make product development quicker and the resulting products better aligned with customers' expectations. Having a set of suitable standards and certification schemes would make their operations more efficient and also bring down the costs of compliance.

3. Next steps

So, what can the BSI IoT/1 Committee do now to address the priority areas for IoT standards development?

3.1 Create live repositories of IoT vulnerabilities, and best practices

The BSI IoT Community [33] was developed by BSI to help build communities for organizations that are being affected by the ever-growing presence of the IoT. The community holds regular events, meetings and workshops to share best opportunities and challenges in business development and implementation of IoT solutions.

We will propose the creation of a new group in the BSI IoT Community where IoT vulnerabilities, use cases and best practices can be shared in a safe, transparent and accessible manner.

3.2 Developing guidelines that allow IoT product and service innovators to manage and control client and customer identities in a secure and safe manner

The BSI IoT/1 Committee will continue to work closely with experts across industry, trade and consumer associations and government to ensure that standards for connected products and digital services are being developed taking an integrated approach to security, privacy and safety. The DCMS *Code of Practice* [9], the ETSI TS 103 645 *Cyber Security for Consumer Internet of Things* standard [10], and the testing and certification services offered by established organizations such as the BSI and the OCF, have paved the foundations for responsible innovation in IoT products and services.

In the BSI IoT/1 Committee, the IoT/1/-/5 panel is currently contributing to the development of the ISO/PC 317 standard on *Consumer Protection: Privacy by design for consumer goods and services*, which provides guidance on how to take a privacy-minded approach through the entire lifecycle and operations of businesses developing connected products and digital services.

3.3 Tiered risk assessment and management standards

The BSI IoT/1 Committee will explore the possibility of developing risk assessment and management standards based on regulations and guidelines that set out clear procedures for how organizations should collect and assess information on the properties and hazards of their products and services. IoT/1 will reach out to established risk standards committees in the process.

3.4 Get involved in our active engagement with IoT SMEs

This white paper sets the scene for a long-term ambition of the BSI IoT/1 Committee and the Standards, Governance and Policy team of the PETRAS IoT Research Hub to engage with IoT SMEs in an active and informed manner.
We welcome your comments, feedback and participation. Please contact:

Dr Irina Brass, Lecturer in Regulation, Innovation and Public Policy at UCL STEaPP, i.brass@ucl.ac.uk; or
Sophie Erskine, Programme Manager for the BSI IoT/1 Committee, at BSI, sophie.erskine@bsigroup.com

Over the next months, we will continue our active engagement and research to understand and capture the needs of IoT SMEs and how standards can support their innovative product and service development. This work will be carried out as part of a student-led project between BSI and UCL Department of Science, Technology, Engineering and Public Policy (STEaPP), supervised by Dr Irina Brass, Lecturer in Regulation, Innovation and Public Policy at UCL STEaPP. Please get in touch with Irina Brass if you would like to hear more about the project and to get involved in this research.

Appendix A: Background to the white paper

Overview

IoT/1 (the BSI IoT Committee) has worked closely with the UK Government, leading industry players, manufacturing and consumer organizations to set IoT security, privacy, interoperability, trust and trustworthiness at the top of its standards development priorities. Over the past two years, the Committee has actively engaged in reviewing and understanding the complex IoT standards landscape. This has facilitated informed debate about the main gaps and challenges in IoT standardization as well as the best routes to design clear, accessible, inclusive and comprehensive IoT standards that achieve the appropriate balance between minimum horizontal requirements and industry specifications across a wide range of verticals and sectors. Throughout this process, IoT/1 has reached consensus that the voice of SMEs and start-ups operating in the IoT field is not sufficiently heard and understood in formal standards making processes.

Rationale and scope

This white paper is part of an on-going effort to understand, include and capture the voice and role of IoT SMEs in the process of standards development. It is one of the first documents that directly addresses how national standards can respond in a proactive and non-intrusive manner to support their business development and ambitions. The paper is only the first step of a longer dialogue about the opportunities and challenges SMEs face when developing IoT products and services, and about how standards development communities can support and engage with them.

The regulatory and standardization landscape is becoming increasingly complex and difficult to navigate for both established and new market entrants in the IoT space. While governments around the world are considering the most appropriate balance between nudging the market via best practice guides, mandatory regulations and procurement processes to ensure that IoT products and services are secure and safe [9][28][34], the standardization community is also challenged by the best manner in which to approach the development of IoT standards to holistically address security, privacy and safety risks and to integrate these with existing horizontal and vertical standards. Equally, the standards community is increasingly concerned with the most appropriate risk assessment and management practices for IoT businesses and the best ways to test and show compliance with best practices[15][35].

While this period of regulatory and standardization transition is not unique in the history of managing risks emerging from disruptive digital technologies, it does lead to considerable uncertainties especially for SMEs (small and medium sized enterprises) that are interested in innovating and promoting new IoT products and services.

SMEs currently operating in the IoT market can be classified into three groups (Figure 3).

Businesses that:

1. add connectivity to their existing product line (e.g. home appliances);
2. integrate IoT solutions to diversify their business models (e.g. healthcare or agriculture); and
3. are IoT solutions innovators (e.g. software, hardware, cloud services).

SMEs in these categories have different demands, objectives and priorities. To enhance their competitiveness and support innovation across all types of market entities, this white paper examines how standards can cater to SMEs' specific business requirements, supporting their objectives and priorities.

Figure 3: Types of SMEs operating in the IoT space

Objectives

This white paper follows from direct engagement with SMEs operating in the IoT space, as well as other key stakeholders that represent and can support their voices, such as trade associations for manufacturers, testing and assurance services, experts in domestic and international standards organizations as well as UK Government representatives.

The main objectives of the paper are to:

- Identify the main opportunities and challenges that SMEs and start-ups are facing with regard to the IoT standards landscape;
- Develop use cases, validated or co-developed with SMEs and other key stakeholders to understand what these challenges are. Examples of these challenges include: sustainable product line diversification and up-scaling, ensuring interoperability with existing smart ecosystems, navigating the fragmented standards landscape, adopting and implementing existing and new IoT standards and best practices.
- Help SMEs and start-ups understand the latest developments in the standardization of IoT security, privacy, trust, interoperability.
- Identify priority areas for standardization and ways of ensuring that SMEs are taking an active role in IoT standardization.

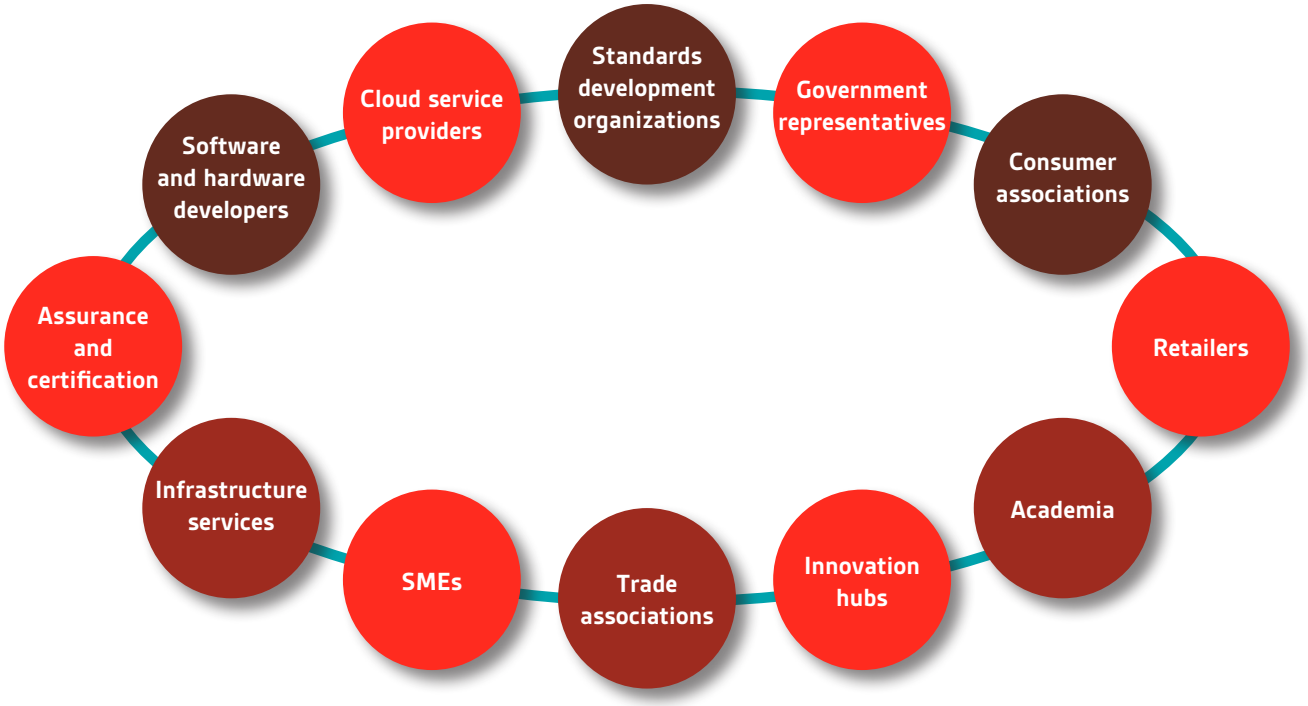
Methodology

The white paper summarizes research findings that were carried out via:

- Expert commentary from members of the BSI IoT/1 Committee.
- A workshop entitled *SMEs and Start-ups Operating in the IoT Space,* organized by the BSI IoT/1 Committee, with participation from key stakeholders across the IoT ecosystem (Figure 4).
- Several IoT use cases developed by workshop participants.

The workshop served as a platform for open discussion among SMEs, standards development organizations, government representatives, consumer associations, and representatives of various industries involved and interested in IoT. The objectives of the workshop were to identify the latest IoT policy initiatives, standards, assurance and certification processes, and to identify SMEs' priority areas and respective gaps in IoT standardization.

Figure 4: Representation of workshop participants



The BSI IoT/1 workshop, *SMEs and Start-ups Operating in the IoT Space,* opened with a plenary session featuring expert input from representatives from the DCMS (UK Department for Digital, Culture, Media and Sport) and the BSI IoT/1 Committee, covering the latest developments in IoT policy-making, domestic and international standardization. It was followed by a roundtable discussion on the main IoT opportunities and challenges for SMEs. Participants were then invited to co-develop use cases following a methodology that allowed them to map the range of IoT products and/or services they are developing to key business challenges and standardization priorities.

Appendix B: The IoT policy and standards landscape

IoT businesses are under growing pressure to demonstrate the trustworthiness of their products, services and organizational practices in order to mitigate the privacy, security and safety risks associated with connected products. IoT standards have been identified, both in research conducted by the PETRAS IoT Hub and during the BSI IoT/1 workshop, *SMEs and Start-ups Operating in the IoT Space,* as fundamental means to ensure a way to build consumer trust in IoT products and services [36][37].

The IoT standards landscape is complex and fragmented. This fragmentation results from the heterogeneity of the processes and technologies associated with the IoT:

- data collection/sensing,
- communication technologies,
- cloud services,
- automation,
- actuation, and
- the different application domains and verticals in which the IoT is deployed.

In response to this diversity, several industry alliances and consortia have been developing baseline practices and de facto, high-level standards for IoT security, data protection and risk assessment processes [16].

In addition, several national and international organizations, such as ENISA (the European Union Agency for Network and Information Security), NIST (the US National Institute of Standards and Technology) and BSI (the British Standards Institution) have conducted comprehensive reviews of IoT security standards, privacy by design, asset management and risk assessment best practices [38][39][40][41].

The UK Government has also been at the forefront of promoting a baseline for responsible IoT security for smart consumer goods. In 2018, the DCMS published the *Code of Practice for Consumer IoT Security*, together with a comprehensive *Mapping of IoT Security Recommendations, Guidance and Standards* to support the implementation of the *Code of Practice* by organizations (also available in JSON file, to make it easier for businesses to adopt it into their own design mechanisms) [9]. The Code brings together, in thirteen high-level and outcome-focused Guidelines, what is widely considered good practice in this area and applies to all consumer IoT products. The mapping allows businesses to find existing recommendations and standards that are appropriate to the context of their product and thus to implement the high-level *Code of Practice*. In February 2019, the key principles of the *Code of Practice* were transposed into the ETSI TS 103 645 standard, *Cyber Security for Consumer Internet of Things* [10].

While the ETSI standard and the DCMS *Code of Practice* address major security failings in IoT devices and propose design principles that are deeply pragmatic, they are high-level provisions that still require the development and alignment of several technical specifications, product, process and system standards to ensure the adequate implementation of IoT standards into business practices. Participants in the BSI IoT/1 workshop acknowledged the ongoing challenge of implementing sectoral and horizontal standards that equally and efficiently address all dimensions of consumer trust in an IoT product and service, without excessively burdening manufacturers and developers (especially SMEs) or relying too heavily on consumer awareness.

The BSI IoT/1/-/5 panel, *Privacy by Design*, is currently providing UK input into the development of an international standard on Privacy by Design, ISO 31700. It aims to provide a comprehensive privacy-driven governance framework for organizations that develop connected products and digital services. The standard factors in consumer behaviour and their needs for privacy and security to be included in the design of the product or service. Privacy by design is seen as security plus real-time privacy control over data processing and management, taking into consideration practical challenges associated with IoT user behaviour and consumer practices [19]. This definition of privacy by design highlights the interdependence between privacy, data protection, data integrity and cyber security.

This approach aligns with the position of several consumer associations involved in standards-making and legislative processes. For instance, ANEC (the European Association for the Coordination of Consumer Representation in Standardization) is advocating amendments to existing EU general and sector-specific product safety regulations to include baseline security assessments for connected consumer products [3]. ANEC pushes for security requirements to be complemented with mandatory cyber security certification in high-risk connected products, such as self-driving cars, toys/children's products, home appliances and smart home-security products.

In addition, BEIS (the UK Government's Department for Business, Energy and Industrial Strategy) has recently launched a consultation to set regulatory requirements for smart appliances through primary and secondary legislation, based on principles of interoperability, data protection, grid and cyber security [20]. BEIS has worked closely with BSI to produce a standards landscape report on the *Secure and interoperable use of smart appliances and electric vehicle smart charge points through standards* [42], which will inform the future development of standards and legislation for smart appliances, based on dynamic consumption patterns and resource availability in the electricity grid. This standards development work is continuing in the BSI IST/6/-/12 panel, *Home Electronics* and in the BSI IoT/1 Committee, *Internet of Things*.

However, the current IoT standards landscape remains highly fragmented. Research conducted by BSI showed that even with a sectoral approach to IoT standards along verticals, the volume of existing standards in place is highly daunting for businesses to navigate. Via comprehensive market research, BSI profiled the formal standards landscape for IoT relevant standards. When preliminary keyword searches produced in excess of 400,000 standards, a more focused, sectoral approach was taken. Despite this, initial searches generated in excess of 50,000 standards for one sector based on keyword searches in a technical regulations reference database. The database contains entries from over 200 standards organizations in 23 countries. There are inconsistencies in how standards are indexed for inclusion in the database, thus resulting in duplications or exclusions of standards depending on how they are indexed. Some European and international organizations use unique numbering systems, version identifiers or other tagging criteria that are not replicated in ISO or EN standards. Standards may also appear under multiple search terms, and therefore be duplicated in search results.

The complexity of results produced was an indication of how difficult the standards landscape is to define and navigate even for standards experts. To refine the segmentation of IoT technology layers and assist in producing meaningful results, a matrix was created that identified technology layers related to IoT and vertical industry segments where IoT plays an important part. The resulting matrix was used to generate keywords which were verified by sector experts before another series of searches was conducted. The final searches produced approximately 400 standards for one industry vertical.

In addition, the structured approach to searching for formal standards does not map easily to market-driven or de facto standards produced by industry alliances and consortia. Concept mapping assisted with generating thematic keywords to be used for open source searches. Dedicated searches drilling into the open standards ecosystem uncovered thematic clusters of standards making by inter-related groups or consortia that formed solely for the purpose of rapidly creating and disseminating standards.

The results of the searches were more limited in number than the formal standards but more difficult to classify. Key findings from this phase of the research underscored the difficulty of navigating and aligning the formal and informal standards landscape. It was difficult to discover sites where informal standards making was occurring in a consistent and recognizable manner, with definable outputs. The communities that make up de facto standards making entities can be fluid and dynamic, and there is very limited knowledge about the uptake and ease of implementation of informal standards.

Overall, the research conducted at BSI into both formal and informal standards making reiterated the difficulties companies, whether large or small, face in finding and implementing IoT-related standards. Further complexities arise with regards to interoperability, data sharing, and shared working within the SME sectors where standards would facilitate market entry, partnerships, and consortia type projects.

References

[1] T. Winchcomb, "Review of latest developments in the Internet of Things," p. 143, 2017.

[2] Ericsson, "Internet of Things forecast – Ericsson Mobility Report," *Ericsson.com*, 09-Nov-2016. [Online]. Available: https://www.ericsson.com/en/mobility-report/internet-of-things-forecast. [Accessed: 20-Nov-2018].

[3] C. Giovanni and F. Silva, "Cybersecurity for Connected Products: A Position Paper." ANEC, 03-Jun-2018.

[4] GSMA, "IoT Security Assessment," *Internet of Things*, 2018.

[5] IoT Security Foundation, "IoT Security Compliance Framework." IoT Security Foundation, 2017.

[6] IoT Security Foundation, "Connected Consumer Best Practice Guidelines," IoT Security Foundation, 2017.

[7] IoT Security Foundation, "Vulnerability Disclosure." IoT Security Foundation, Dec-2017.

[8] OWASP, "Principles of IoT Security - OWASP," 2016. [Online]. Available: https://www.owasp.org/index.php/Principles_of_IoT_Security. [Accessed: 20-Nov-2018].

[9] DCMS, "Code of Practice for consumer IoT security," *GOV.UK*, 2018. [Online]. Available: https://www.gov.uk/government/publications/secure-by-design. [Accessed: 18-Oct-2018].

[10] ETSI, *ETSI TS 103 645 v1.1.1 Cyber Security for Consumer Internet of Things*. 2019. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf [Accessed 17-Apr-2019]

[11] CENELEC, "Standards Development - List of Technical Bodies -." [Online]. Available: https://www.cenelec.eu/dyn/www/f?p=104:110:863958080833601::::FSP_ORG_ID,FSP_PROJECT,FSP_LANG_ID:1258281,66523,25. [Accessed: 29-Mar-2019].

[12] ISO, "ISO/PC 317 - Consumer protection: privacy by design for consumer goods and services." [Online]. Available: https://www.iso.org/committee/6935430/x/catalogue/p/0/u/1/w/0/d/0. [Accessed: 29-Mar-2019].

[13] ISO/IEC, "ISO/IEC JTC 1/SC 41 - Internet of Things and related technologies," ISO. [Online]. Available: http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/committee/64/83/6483279.html. [Accessed: 03-Apr-2019]

[14] OCF, "OCF Certification: Getting connected to the Internet of Things," *Open Connectivity Foundation (OCF)*. [Online]. Available: https://openconnectivity.org/certification. [Accessed: 01-Apr-2019].

[15] BSI, "IoT Assurance Services," 2018. [Online]. Available: https://www.bsigroup.com/en-GB/industries-and-sectors/Internet-of-Things/IoT-Assurance-Services/. [Accessed: 20-Nov-2018].

[16] I. Brass, L. Tanczer, M. Carr, and J. Blackstock, "Standardising a Moving Target: The Development and Evolution of IoT Security Stanadards," in *Living in the Internet of Things: Cybersecurity of IoT 2018*, London, 2018.

[17] K. Pothong, "IoT in the Home Demonstrator," 2019. [Online]. Available: https://www.petrashub.org/iot-in-the-home-demonstrator/. [Accessed: 04-Mar-2019].

[18] K. Pothong, L. Pschetz, J. Watson, J. Gbadamosi, and A. Asaturyan, "Making IoT Security Policies Relevant, Inclusive and Practical for People: A Multi-Dimensional Method," in *Living in the Internet of Things: Realising the Socioeconomic Benefits of an Interconected World*, London, 2019.

[19] ICO, "Data protection impact assessments," 2019. [Online]. Available: https://icoumbraco.azurewebsites.net/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/. [Accessed: 04-Mar-2019].

[20] S. Y. L. Wakenshaw, C. Maple, M. Schraefel, R. Gomer, and K. Ghirardello, "Mechanisms for Meaningful Consent in Internet of Things," Jan. 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8379701 [Accessed 17-Apr-2019

[21] J. Blythe and M. Johnson, "Rapid Evidence Assessment on Labelling Schemes and Implications for Consumer IoT Security," Dawes Centre for Future Crime, PETRAS IoT Hub, Department for Digital, Culture, Media and Sport (DCMS), London, 2018.

[22] L. Tanczer, T. Patel, and S. Parkin, "Gender and IoT: Techn Abuse Guide," STEaPP, PETRAS IoT Hub, London, 2018.

[23] OWASP, "OWASP Internet of Things Project," 2018. [Online]. Available: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project. [Accessed: 04-Mar-2019].

[24] Consumers International, "Consumer IoT Trust by Design 2019: Guidelines and Chicklistt," Consumers International, 2019.

[25] ISO, "ISO/IEC NP 30147 Information technology-- Internet of Things -- Methodology for Trustworthiness of IoT System/service," *ISO*, 2019. [Online]. Available: http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/32/53267.html. [Accessed: 04-Mar-2019].

[26] J. Tait and G. Banda, "Proportionate and adaptive governance of innovative technologies," BSI, London, 2018.

[27] BSI, "Internet of Things - Creating best practice, sharing new opportunities and tackling global IoT challenges | BSI Group," 2019. [Online]. Available: https://www.bsigroup.com/en-GB/industries-and-sectors/Internet-of-Things/. [Accessed: 04-Mar-2019].

[28] HM Government, "The key principles of vehicle cyber security for connected and automated vehicles," *GOV.UK*, 2017. [Online]. Available: https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles. [Accessed: 20-Nov-2018].

[29] ISO, "ISO 31000 Risk management," *ISO*, 2018. [Online]. Available: http://www.iso.org/cms/render/live/en/sites/isoorg/home/standards/popular-standards/iso-31000-risk-management.html. [Accessed: 04-Mar-2019].

[30] ISO, "ISO 9001 Quality management," *ISO*, 2015. [Online]. Available: http://www.iso.org/cms/render/live/en/sites/isoorg/home/standards/popular-standards/iso-9001.html. [Accessed: 04-Mar-2019].

[31] ISO, "ISO/IEC 27001 Information security management," *ISO*, 2018. [Online]. Available: http://www.iso.org/cms/render/live/en/sites/isoorg/home/standards/popular-standards/isoiec-27001-information-securit.html. [Accessed: 04-Mar-2019].

[32] ECHA, "Understanding REACH," 2007. [Online]. Available: https://echa.europa.eu/regulations/reach/understanding-reach. [Accessed: 04-Mar-2019].

[33] BSI, "The BSI IoT Community," *BSI IoT Community*. [Online]. Available: https://iot.bsigroup.com/. [Accessed: 01-Apr-2019].

[34] M. Segura, M. C. Woo, C. M. Butler, and B. P. Cadigan, "Sticker shock? The Cyber Shield Act of 2017 attempts to make IoT manufacturers prioritize IoT security | Perspectives | Reed Smith LLP," 2018. [Online]. Available: https://www.reedsmith.com/en/perspectives/2018/03/sticker-shock-the-cyber-shield-act-of-2017. [Accessed: 20-Nov-2018].

[35] IoT Security Foundation, "Best Practice Guidelines," 2018.

[36] L. Harriss and C. West, "Cyber Security of Consumer Devices," Feb. 2019.

[37] K. Pothong, I. Brass, and M. Carr, "Cybersecurity of the Internet of Things: PETRAS Stream Report," PETRAS IoT Research Hub, London, 2019.

[38] ENISA, "Baseline Security Recommendations for IoT — ENISA," 2017. [Online]. Available: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot. [Accessed: 17-Oct-2018].

[39] ENISA, "Security Challenges and best practices in the IoT Environment — ENISA," 2017. [Online]. Available: https://www.enisa.europa.eu/publications/ed-speeches/security-challenges-and-best-practices-in-the-iot-environment/view. [Accessed: 17-Oct-2018].

[40] NCSC, "Secure by Default Principles," May-2017. [Online]. Available: https://www.ncsc.gov.uk/articles/secure-default. [Accessed: 17-Oct-2018].

[41] R. Ross, M. McEvilley, and J. Carrier Oren, "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," National Institute of Standards and Technology, NIST SP 800-160, Nov. 2016.

[42] BSI, "Secure and interoperable use of smart appliances and electric vehicle smart charge points through standards: Standards landscape research." 2018.

BSI (British Standards Institution) is the UK's National Standards Body. BSI represents UK economic and social interests across all European and international standards organizations and in the development of business information solutions for British organizations of all sizes and sectors.

Standards provide the knowledge that organizations need to implement best practice and succeed. They can offer a set of powerful tools to make your organization more innovative and productive.

BSI is keen to hear your views on this paper, or for further information please contact us here: sophie.erskine@bsigroup.com

The BSI IoT/1 Committee is the central BSI committee addressing horizontal standardization issues pertaining to the privacy, security, safety and interoperability of the Internet of Things. The Committee is actively working to align IoT standardization efforts at national and international level. The BSI IoT/1 Committee mirrors ISO/IEC JTC 1/ SC41 – Internet of Things and Related Technologies.

The Committee has a wide expert representation across several industry verticals, consumer associations and academia. Over the past years, it has focused on the security of connected devices and industrial systems. The Committee is responsible for the IoT/1/-/5 panel, which is currently working on developing a Privacy by Design standard in the context of connected devices.

IoT/1 is dedicated to developing standards that respond to the needs of SMEs operating in the IoT context. In July 2018 we held a workshop designed to understand the main opportunities and challenges that SMEs operating in the IoT context are facing and how standards can support to meet some of these challenges.

The PETRAS Internet of Things Research Hub is a consortium of leading UK universities that have been working together over the past three years to explore critical issues in the privacy, ethics, trust, reliability, acceptability, and security of the Internet of Things. Funding for the Hub included a £9.8 million grant from the Engineering and Physical Sciences Research Council (EPSRC), which was boosted by partner contributions of over £14 million across the lifespan of the Hub. This project is also run in collaboration with IoTUK.

The PETRAS IoT Hub, is led by UCL and includes 10 other universities: Imperial College London, Lancaster University, University of Oxford, University of Warwick, Cardiff University, University of Edinburgh, University of Southampton, University of Surrey, University of Bristol and Newcastle University.

Authors

Irina Brass, PhD, is Lecturer in Regulation, Innovation and Public Policy at UCL Department of Science, Technology, Engineering and Public Policy (STEaPP). She is a Co-Investigator of the Standards, Governance and Policy Stream of the PETRAS IoT Research Hub and the Chair of the BSI IoT/1 Committee. Dr Brass's research investigates the regulation and governance of disruptive technologies, especially emerging digital technologies.

Kruakae Pothong, PhD, is a Post-doctoral Research Associate, collaborating research and publications across various universities, as part of the PETRAS IoT Research Hub. Her work focuses on data protection and the social implications of consumer IoT.

Mariyam Hasham, PhD, is a Market Insights Analyst at BSI. Her research focuses on the impact of emerging technologies on commercial markets as well as the future growth of key markets and economies.

Acknowledgements

Thanks to the following organizations for their participation in the BSI IoT/1 workshop: GeoEnable, ERA Home Security, GTech, PETRAS, University College London, BSI Assurance UK, DCMS, Digital Catapult, John Lewis, AMDEA.

Thanks to all members of the BSI IoT/1 Committee for their expert guidance and contribution to the workshop.

Thanks to Sophie Erskine, Programme Manager of the BSI IoT/1 Committee, for project managing this market engagement activity from the organization of the BSI IoT/1 workshop through to the publication of the white paper.

389 Chiswick High Road
London, W4 4AL
United Kingdom

E: sophie.erskine@bsigroup.com
www.bsigroup.com

Department of Science, Technology,
Engineering and Public Policy (STEaPP)
University College London
Euston House (8th Floor)
24 Eversholt Street
London NW1 1BS

E: i.brass@ucl.ac.uk
www.ucl.ac.uk/steapp