**Event summary**

**The Internet of Things – if we don't trust it, will we use it? #bsiiot**

**24 January 2014**

## How much can we trust the Internet of Things?

*By some estimates the Internet of Things (IoT) will be worth hundreds of billions of pounds by 2020, and 50 billion objects will be connected. But can or should this vision be realized if people can't trust that it will be secure? This question and much besides was explored at BSI's free one-day stakeholder forum on 24 January.*

## Setting the agenda

**Richard Rees** chaired the forum, bringing 30 years of industry expertise to bear, as well as his experience of chairing BSI's Automatic Identification Technologies Committee. In his introduction, Rees pointed out that the IoT is being built by people who want to make money. He asked if trust, therefore, shouldn't be seen as a 'product purchasing parameter'? The IoT, he added, is not entirely new, but the scale of its data and analytics are. So, going forward, must the user be more 'streetwise' or should we look for protection from a 'nanny' state? And finally, what role can standards play?

## Introducing BSI and standards

BSI Programme Manager, **Antonella Adamus,** then outlined what standards are, and why and how they're created. Standards "are knowledge" and in any sphere, "what good looks like", she said. The first generation of standards dealt with making products better; the second with making services better; and the third with better behaviours and ethics. Moreover standards are written though a rigorous, prescribed process that involves wide consultation and consensus. Adamus concluded by saying that BSI's committees of experts are the backbone of the process, and that BSI is always actively seeking to engage with anyone interested in becoming involved with its standards work.

## Focus on security

**Charles Brookson,** of Zeata Security Ltd and Azenby, addressed security, noting that the IoT goes far beyond the ability to switch devices on and off remotely. It includes things like intelligent transport, smart metering and smart cities. However, drawing on his 40 years' experience in telecoms security, he said that on a technical level good security is 'little understood' and information, on the whole, is poorly protected. For example smart metering can be hacked in several ways – and the result could be an orchestrated blackout. Brookson concluded that organizations and individuals will always be at risk, but they can at least minimize their exposure. They should strive for transparent technical and business requirements, and they should inform customers about security risks – whether the customer is interested or not.

## Lessons from history

**Dr Mike Nash**, an information security expert and member of the ISO committee on the ISO/IEC 27000 series of information security standards, focused on the unintended consequences when machines gain autonomy. Nash used a case history from the London Underground to make his point: that machines will only ever have the intelligence that is built into them. In developing the IoT, he said, designers will need to learn from history. Both complexity and security, Nash counselled, are 'friends of failure'. "The environment will always change in ways you don't anticipate," he cautioned. The trustworthiness of the IoT will depend, he concluded, on how it's managed.

### The role of biometrics

**Dr Peter Waggett**, from IBM's Emerging Technology Group, presented on biometrics, which he defined as the automated recognition of individuals based on biological and behavioural characteristics. Waggett noted that there are an increasing number of biometric data measures and applications. For example, a car seat can now identify an individual from their cardiac rhythms, and can even tell if the individual is tired or stressed. So what are the implications? The technology, said Waggett, is becoming ubiquitous. It's able to work over much larger distances, and is also achieving high recognition rates. "Privacy as a concept is dead," he said. In response, we should embrace and understand the challenges and benefits. We should also focus on audit trails, who owns the data, and on deploying probability-based security models.

### Privacy and the Internet of Things

**Pete Eisenegger**, who represents consumers' interests across ICT standards within ANEC (the European consumer voice in standardization), gave the day's final presentation. He asked 'what is privacy?' and noted the ways that data – names, photos, behaviours, the things we buy – constitute 'identifiability'. Given the vast amount of data being collected, he said, standards are needed to give people control. These should cover governance of processing purpose, consent management, and traceability. He concluded that we need standards that do the right things for industry and for people, and in developing the IoT, we need to take the right steps to underpin trust.

### Three workshops completed the day's programme.

### Personal IoT

This group reflected on the commercial drivers behind the IoT, and the prevalence of uninformed consent – stemming from the fact that explicit consent reduces take-up by 40 per cent. The group accepted that IoT security is an end-to-end infrastructure issue, but felt that privacy issues on devices was a place to start. Moreover, since consumers will now buy around 700 different products and services in their lifetimes, there does seems to be a role for a trusted intermediary who can 'certify' the privacy control capabilities of devices.

### Digital footprints

This group registered concern about what happens to captured data, and asked what is in place to make things better? It was felt that governments need to act on an international basis, and that individuals and SMEs needed to be better informed about the risks and opportunities. The issue of consent came up repeatedly.

### Developing security use cases

This third group asked, 'If we don't trust the IoT, will we use it?' and decided: 'Yes we will, but it doesn't mean we're happy about it!' The participants concluded that even technically knowledgeable people are surprised by what the IoT can do, so more information is needed on securing autonomous devices – and they'd be willing to pay for it. BSI, it was noted, is already preparing a guidance document for SMEs. However it was felt that BSI can't address this alone and will need to collaborate with others.

**Find out more about BSI and standards at bsigroup.com.**