GOVERNANCE

REGULATING DIGITAL TECHNOLOGY

Digital technologies are underpinning almost every aspect of our lives, changing the way we live and work. As organisations adopt and adapt to new ways of working, it's imperative that they have a strong governance framework in place to mitigate risks. Dina Patel speaks to Dr Irina Brass, Lecturer in Regulation, Innovation and Public Policy at University College London and Chair of the IoT-1 Technical Committee of the BSI, about how a standards-based approach to governance can improve organisational resilience. In November 2019, Dr Brass received the BSI Standards-Makers Award for Education about Standardisation.

According to the Modern Corporate Governance 2019 report from the BSI, strong and dynamic governance is essential in today's connected and rapidly changing world. "Corporations simply can't be too careful when it comes to information security. Protecting personal records and commercially sensitive information is critical. Getting it wrong in the post-GDPR landscape means significant fines and serious reputation damage," the report says. It also argues that one of the ways organisations can improve cybersecurity is by using internationally recognised standards to introduce processes against both deliberate and chance incidents.

Dr Irina Brass explores some of the challenges facing the policymakers when introducing and adapting standards for digital technologies. ▶

***QW:* What does your role at UCL involve?**

IB: I am a Lecturer in Regulation, Innovation and Public Policy at UCL in London. I work in the Department of Science, Technology, Engineering and Public Policy (STEaPP), an interdisciplinary department in the UCL Faculty of Engineering. I am a political scientist by training, but my interest has always been in the regulation and governance of emerging technologies, so I work very closely with engineers, economists, lawyers, international relations and management science scholars to unpick the complex challenge of governing emerging technologies in a way that promotes responsible innovation and ensures consumer protection.

I look at the regulatory and standardisation challenges associated with emerging technologies, such as the Internet of Things (IoT), machine learning, and the growing importance and relevance of cyber-physical systems. I also teach several modules that are related to digital technologies and policy, risk assessment and governance, and the interplay between technical and scientific knowledge and public policy.

At STEaPP, our mission is to ensure that engineering and scientific expertise informs policymaking, and that those who engineer and design our systems understand the key challenges policymakers face when new technologies are brought to the market. I also sit within the Digital Technologies and Policy Lab at UCL, which is an interdisciplinary laboratory where we explore the challenges that digital technologies pose today: cybersecurity, data integrity and resilience of cyber-physical systems. Projects such as the PETRAS National Centre of Excellence for IoT Systems Cybersecurity, which I am part of, have been crucial at advancing research in these areas.

***QW:* What does your research with STEaPP focus on?**

IB: My main research focus is how to adapt current regulatory frameworks, established standard-making processes and governance arrangements to the type of systemic disruptions we are seeing today, most of which are driven by the increased use of digital technologies. Arguably, the types of disruptions we are seeing today are different than the evolutionary innovations we've seen in the past. This is why we sometimes refer to our contemporary world as entering the Fourth Industrial Revolution (World Economic Forum). For instance, the integration of IoT, machine learning, robotics in verticals such as healthcare or transportation, leads to the implementation of quasi-autonomous systems that are functioning in ways that we don't fully understand, where it is difficult to foresee all their vulnerabilities and how they might be exploited.

For this, we need adaptive standardisation processes and regulatory frameworks, so that we constantly monitor and learn about how these systems behave and we are able to adapt the rules that manage emerging technologies in a more flexible manner. It is a completely different way of thinking about standards and regulations, because we are used to valuing best practices and rules that give us certainty and predictability in the long-term.

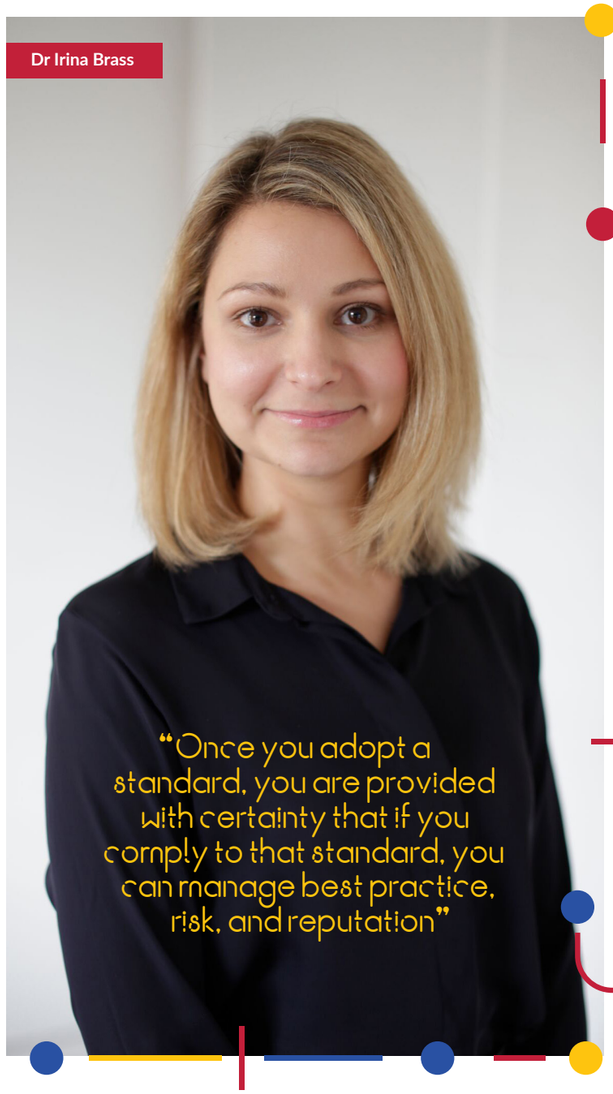


Image: UCL

WHAT IS THE INTERNET OF THINGS (IOT)?

In the broadest sense, the term IoT encompasses everything connected to the internet, but is increasingly being used to define objects that 'talk' to each other.

By combining these connected devices with automated systems, it is possible to "gather information, analyse it and create an action" to help someone with a particular task, or learn from a process.

Source: Wired

***QW:* What does your role as Chair of the IoT/1 Technical Committee of the BSI involve?**

IB: As Committee chair, you need to propose an agenda for the committee. The scope of the IoT-1 Committee is quite broad given that it addresses horizontal standards for issues like privacy, security, interoperability. My first goal was to understand the kind of standards we want to produce as a committee.

My second goal was to ensure synergy between the world of standards-making and broader public policies. This is so that when a government makes a decision with regards to regulating a certain aspect pertaining to emerging technologies, the main baselines and principles of best practice are aligned across the standards and policy world. This ensures a coordinated approach when promoting cybersecurity, data protection or general risk management practices.

A final ambition stemmed from the reality that the world of disruptive digital technologies is populated by small and medium enterprises. In particular, SMEs are very productive when it comes to the IoT – innovating across products and services. Our goal in the committee was to understand their needs when innovating in the IoT, and how best to capture their voice in the standards-making process, so that their requirements can be better addressed by future standards. We worked closely to organise a multi-stakeholder workshop and produce a white paper entitled: 'Navigating and Informing the IoT Standards Landscape: a Guide for SMEs and Start-ups'.

***QW:* What challenges have you faced as the chair of the IoT/1 Committee?**

IB: IoT applies to every single sector of the economy, so one of the fundamental challenges was understanding what the balance should be between creating the horizontal standards, and standards for the different domains or verticals in which IoT is used. How should we prioritise this work? A second challenge is that the IoT is used alongside other emerging technological solutions such as machine learning or automated systems. This reality complicates standards development processes. Should the same best practice principles apply across all of these technologies? What should the risk governance structure of an organisation who integrates all of these technological solutions across their products, services and day-to-day activities look like? This essentially enlarges the remit of what the IoT/1 Committee must focus on.

We've handled these challenges by looking at approaches to risk management. This applies to quality professionals because it focuses on how to

THE RISE OF IOT SMES

There are many opportunities and challenges that small and medium-sized enterprises and start-ups face when developing connected products and associated IoT services in a transparent manner. The challenges, identified by the BSI-PETRAS White Paper 'Navigating and Informing the IoT Standards Landscape: a Guide for SMEs and Start-ups,' include:

- 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.

Case study: ERA Home Security, UK

In rolling out smart versions of existing home security products, ERA Home Security positions itself at the intersection of edge products and the communications layer of the IoT ecosystem. The company's vision is to provide consumers with security solutions ranging from smartware, cloud-based alarm systems and community security applications.

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;
- Data protection.

To efficiently navigate the diverse nature 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 or the BSI IoT Assurance Services and Kitemark, are paramount for validating and communicating the high security and reliability of their product and services range.

Source: Navigating and Informing the IoT Standards Landscape: A guide for SMEs and Start-ups; British Standards Institution, 2019.

integrate quality across an organisation, rather than just within a system. Like any committee that deals with digital technologies, a challenge we also face is ensuring that there are immediate responses to when things go wrong, so ensuring that standards focus on resilience building is key.

QW: How do standards underpin responsible innovation and inform policymaking?

IB: In so many ways, but to start, I'd like to highlight two main misconceptions about standards. The first misconception is that standards are written by technical or industry experts, and as a result, that they are inaccessible to consumers and users. The second misconception is that standards and public policy don't go hand-in-hand; that they promote the interest of big industry and not policy goals at large. My experience of researching, teaching and now working directly in standards-making processes shows that this is not the case. Standards ensure interoperability, encourage certainty when managing supply chains, and can stimulate innovation and trade. They support public policy goals by establishing best practice for how organisations manage risk, how they assess vulnerabilities in manufacturing processes, and the quality, safety, integrity of their products and services, so that ultimately a high level of consumer protection is achieved.

QW: What are some of the challenges when developing standards and policies for emerging technologies?

IB: One of the biggest challenges when it comes to cross-sectoral emerging technologies is the balance between horizontal baseline standards and vertical standards created due to the specificities in different industries or sectors. It's tricky trying to come up with a comprehensive, yet adaptive, baseline standard for cybersecurity or algorithmic decision-making, how we encourage the adoption of good practice in a connected world without setting up onerous regulatory requirements, while also understanding the dynamics present across different sectors.

Another challenge is how to adapt standards and regulations to the uncertainties brought about by emerging technologies, and this has been at the core of my research. It's not just about ensuring standards and regulatory processes are better understood by a wider audience, but how we create governance mechanisms to ensure that whenever new threats and vulnerabilities arise, we have the organisational capacities and capabilities to quickly adapt and respond to these challenges.

QW: How important is standards-based awareness training and education for employees to limit cybersecurity risks?

IB: Standards-based awareness training and education is highly relevant for employers and employees alike. Traditionally, security referred to how an organisation protected the physical security of its assets and employees. For instance, issuing employee or visitors cards is one way to ensure that only those who are vetted can enter the organisation's premises. As organisations started using information and communication technologies and digital systems to manage their assets, the same physical security practices were applied. However, cybersecurity vulnerabilities are a lot more dynamic in nature: as cybercriminals learn how malware is identified and patched, they devise new ways to break into information systems. This requires a paradigmatic change in how organisations govern information security risk. We need to shift our focus away from standards that we design and use for 10 to 15 years, to more flexible standards that allow organisations to dynamically manage new risks and uncertainties while still maintaining robust governance processes.

QW: What are your top tips for organisations wanting to manage cybersecurity and data protection?

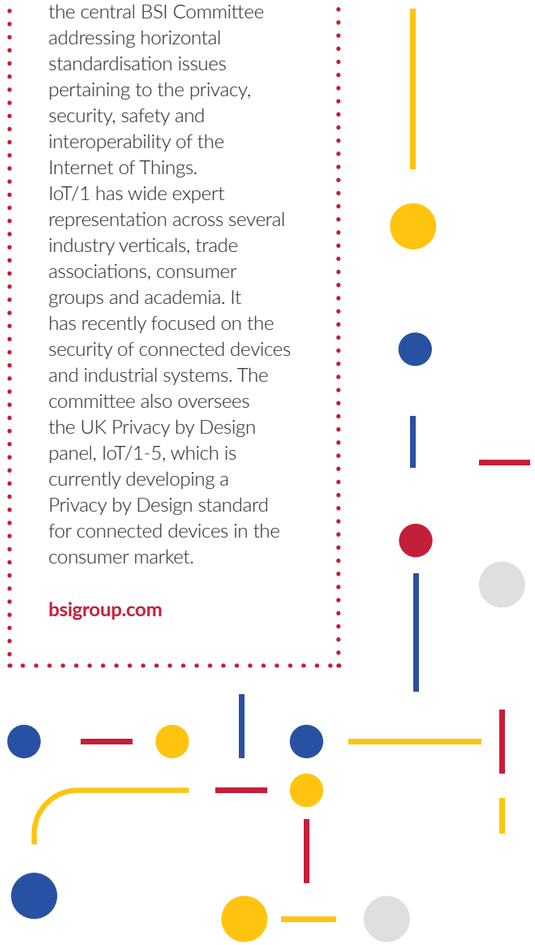
IB: My tips for organisations are:

1. Information security, and cybersecurity at large, should be a top priority for organisations and their boards. Board members need to ensure that they have a comprehensive governance plan for managing cybersecurity and data protection risks for the information systems they deploy internally within the organisation, as well as for the products or services they are developing.
2. When managing complicated supply chains, organisations should ask if their providers adhere not only to established safety standards, but also to the latest cybersecurity and data protection standards for product components or services.
3. When purchasing insurance, organisations should pay attention if their policies cover cybersecurity and, most importantly, what information security/cybersecurity standards insurance providers use when offering policies. ■

THE IOT-1 TECHNICAL COMMITTEE

The IoT/1 Committee is the central BSI Committee addressing horizontal standardisation issues pertaining to the privacy, security, safety and interoperability of the Internet of Things. IoT/1 has wide expert representation across several industry verticals, trade associations, consumer groups and academia. It has recently focused on the security of connected devices and industrial systems. The committee also oversees the UK Privacy by Design panel, IoT/1-5, which is currently developing a Privacy by Design standard for connected devices in the consumer market.

bsigroup.com



"How do we create governance mechanisms to ensure that whenever new issues arise we are capable and adaptive enough to respond to them?"

CYBER SECURITY BREACHES SURVEY 2019

The Cyber Security Breaches Survey 2019, a quantitative and qualitative survey of UK businesses and charities, published by the UK government, found that cyber-attacks are a persistent threat to businesses and charities. While fewer businesses have identified breaches or attacks than before, the ones that have identified them are typically experiencing more of them.

Around one-third (32%) of businesses and two in 10 charities (22%) report having cybersecurity breaches or attacks in the last 12 months. As in previous years, this is much higher specifically among medium businesses (60%), large businesses (61%) and high-income charities (52%). Among this 32 per cent of businesses and 22 per cent of charities facing breaches or attacks, the most common types are:

- Phishing attacks (identified by 80 per cent of these businesses and 81 per cent of these charities);
- Others impersonating an organisation in emails or online (28 per cent of these businesses and 20 per cent of these charities);
- Viruses, spyware or malware, including ransomware attacks (27 per cent of these businesses and 18 per cent of these charities).

Among the 32 per cent of businesses recording breaches or attacks, this resulted in a negative outcome, such as a loss of data or assets, in 30 per cent of cases. Among the charities recording breaches or attacks, this happened 21 per cent of the time.

In businesses that had these kinds of negative outcomes, the average (mean) cost to the business was £4,180 in 2019. This is higher than in 2018 (£3,160) and 2017 (£2,450). This indicates a broad trend of rising costs in cases where cyber-attacks are able to penetrate an organisation's defences.

Source: Department for Digital, Culture, Media and Sport: Cyber Security Breaches Survey 2019: Statistical Release https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf

Standards relevant to cybersecurity

PROTECTING COMPANY INFORMATION

ISO/IEC 27000
Information technology — Security techniques — Information security management systems — Overview and vocabulary

ISO/IEC 27001
Information technology – Security techniques – Information security management systems – Requirements

ISO/IEC 27002
Information technology – Security techniques – Code of practice for information security controls

ISO/IEC 27003
Information technology – Security techniques – Information security management system implementation guidance

ISO/IEC 27005
Information technology – Security techniques – Information security risk management

BS 7799-3
Information security management systems – Guidelines for information security risk management

PROTECTION AGAINST CYBERASSAULTS

ISO/IEC 27032
Information technology – Security techniques – Guidelines for cybersecurity

DATA MANAGEMENT AND CLOUD STORAGE

ISO/IEC 27017
Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ISO/IEC 27018
Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO/IEC 27701
Privacy Information Management – Security techniques. Extension to ISO/IEC 27001 and ISO/IEC 27002. Requirements.

BS ISO/IEC 19944
Information technology – Cloud computing – Cloud services and devices Data flow, data categories and data use