



---

# ISSA-UK Comments on “Digital Britain - The Interim Report”

---



*ISSA Chapter of the Year 2005 and 2006*



## ISSA-UK COMMENTS ON “DIGITAL BRITAIN - THE INTERIM REPORT”

---

This document sets out the comments from UK members of the Information Systems Security Association (ISSA)<sup>1</sup> on the interim report “Digital Britain”<sup>2</sup> published by the Department for Culture, Media and Sport (DCMS) and the Department for Business, Enterprise and Regulatory Reform (BERR) in January 2009.

### General Comments

---

If Digital Britain is to scale and serve effectively and securely, then it needs to be built on a solid foundation of defined and understood security standards and services, operating at all levels across the digital infrastructure and its associated services. This would include management frameworks, best practices and regulations regarding due diligence, accountabilities, protective measures and readily accessible response capabilities. Underpinning these enablers is the ongoing need for appropriate levels of risk awareness by both service providers and consumers. In the absence of such essential supporting services, the exploitation of digital services is likely to become increasingly difficult, complex and expensive to manage.

Fortunately, many appropriate security standards already exist, e.g. ISO27001<sup>3</sup>. However, in some areas, new or more effective standards and services will be needed, requiring coordinated, proactive planning by all stakeholders. In framing security standards, it is important to avoid imposing excessive burdens on service providers and users, especially small and medium enterprises. We would therefore advocate the use of a “tiered approach” of standards based on metrics related to usage or revenue, such as has been adopted for the Payment Card Industry Data Security Standard (PCI DSS) developed by the major credit card companies to secure credit card data processed by retailers. The ISSA would be willing to provide an example framework for such a model upon request.

### Digital Networks

---

Next Generation Access Networks enable fast transfers of information, presenting an increased vulnerability to denial-of-service attacks, viruses and data theft as well as to a larger amount of business and citizen information. This demands increased responsibility on the part of both service providers and consumers to maintain a higher degree of vigilance and appropriate safeguards to minimise the probability and impact of risks, such as loss-of-service, identity theft, fraud and espionage. In the same way that motorways need driving protocols, speed limits and traffic police, and fast cars require higher performance brakes, so the responsible use of Next Generation services will require an appropriate framework of protocols, permissions and policing. We note that individual service providers, such as BT, have developed comprehensive sets of security measures to minimise many of the security risks, but the stakes are too high to leave entirely to the discretion of vendors, so we believe that an agreed international framework of appropriate measures and initiatives should be established under the direction of a suitable body such as the Internet Governance Forum.

---

<sup>1</sup> The Information Systems Security Association (ISSA) is a non-profit international organisation of information security professionals and practitioners. The ISSA is the largest international, not-for-profit association specifically for information security professionals. It provides education forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members. In the UK, the ISSA has a membership base of over 1000 and represents information security in all industry sectors.

<sup>2</sup> The DCMS and BERR report outlines the Government’s plans to enable the UK’s transition to a “Digital Britain” and is intended to help secure Britain’s place at the forefront of the global digital economy.

<sup>3</sup> ISO27001 (ISO/IEC 27001:2005) is the international standard for an Information Security Management System (ISMS)

## Digital Content

---

The need to safeguard the commercial model that underpins the development of new content is essential to a digital economy. Imposing technical solutions for digital rights enforcement on existing technology platforms can prove to be expensive, restrictive and ineffective. Experience has shown that such controls are unlikely to be completely foolproof and will attract sustained attempts to subvert them by hackers and criminals. New business models might also serve to undermine the business case for short-term technology solutions. A more effective approach is to tackle rights management as a social issue. This means investing in the skills and resources available to investigate and prosecute offenders.

Requiring service providers to report suspected breaches of digital rights is an important element in the investigation process. But the associated expense needs to be kept to a minimum. As mentioned earlier, we would advocate a “tiered” approach to contain the level of costs. This might, for example, be based on a model that links the required degree of intervention to a metric associated with business revenue, such as the number of customers, transactions or page impressions.

The issue of privacy of personal information on consumers and for sensitive, commercial information must also be addressed, especially the difficult problem of how differences in the interests and expectations of government, business and citizens can best be reconciled. Such an issue demands a broader debate with all stakeholders.

## Education and Skills

---

As rightly pointed out, the risks to children from exposure to harmful or inappropriate content are a major concern. Similarly, there are growing security threats to citizens, business and government services, such as identity theft, fraud, espionage, and denial-of-service attacks. There is a growing need for appropriate risk awareness education at all levels in society, not just for children in need of protection or for adults involved in educational or vocational IT training. Consumers and employees at all levels require a suitable level of risk awareness training, as well a source of authoritative advice on how to set up systems securely and manage potentially damaging incidents.

A number of initiatives have already been taken to address this area, most notably the establishment of the Child Exploitation and Online Protection Centre, the UK Council for Child Internet Safety and “Get Safe Online”. We believe, however, that the support currently provided to small and medium enterprises needs to be substantially expanded to include more prescriptive advice on sources of trustworthy security services and real-time support in responding to security incidents that could be catastrophic to a small enterprise but do not justify immediate action by police authorities.

“Get Safe Online” provides an effective focal point for professional security advice but the level and range of support needs to be expanded to include advice on local sources of professional services and telephone support for consumers in need of urgent advice. Internet service providers and computer vendors, most notably Microsoft, already provide a certain degree of prescriptive support, but there is a growing need for more comprehensive, independent and specialist sources of advice. We believe that the existence of such services is essential to help to grow the future online economy, by minimising the impact of incidents and building confidence in digital services.

*The comments presented in this document are a result of an ISSA “Digital Britain” Expert Panel workshop held at BT Tower on 5<sup>th</sup> March 2009. ISSA expresses its gratitude and appreciation to BT and the following Information Systems Security Association UK members who contributed to the discussions and conclusions in this document:*

<i>Geoff Harris</i>	<i>President ISSA-UK</i>
<i>Tim Holman</i>	<i>Director ISSA-UK</i>
<i>David Lacey</i>	<i>Member ISSA-UK</i>
<i>Tony Langdell</i>	<i>Member ISSA-UK</i>
<i>Mick Meehan</i>	<i>Member ISSA-UK</i>
<i>Allan Wall</i>	<i>Member ISSA-UK</i>
<i>Marino Zini</i>	<i>Member ISSA-UK</i>

A handwritten signature in black ink, which appears to read 'D Lacey'.

David Lacey

Information Systems Security Association - UK “Digital Britain” Expert Panel Chairman

*March 2009*

---