

Technology Strategy Board

Driving Innovation



Network Security

Innovation Platform

INTERIM STRATEGIC ASSESSMENT

JUNE 2009



Network Security Innovation Platform

INTERIM STRATEGIC ASSESSMENT



What is our challenge?

UK organisations depend upon reliable and accurate electronic information to make critical decisions about almost every aspect of their business. The dependence on these systems that deliver services to UK business and society is greater than it has ever been and will only increase in the coming years.

Critical services may, for example, manifest themselves as key information systems for transport, healthcare, financial sector communication gateways or consumer broadband connectivity. It is of paramount importance that these services continue to operate in a reliable and secure way. These electronic services underpin the economic well-being of the UK and may, in some cases, affect national security.

The Government's 'Digital Britain' and 'National Cyber Security Strategy' reports set out its approach to enabling and encouraging economic growth, by making the UK a more prosperous and secure environment for both business and the individual – through stimulating innovation in the field of information risk management.

To realise this we need a step change in the production, consumption and subsequent decommissioning of information services and products. These products and services should maximise the benefits to the UK by ensuring that information risks are mitigated to acceptable levels.

What is an innovation platform?

Global society faces many challenges. By applying technology and innovation we can help to meet these challenges and at the same time open up new opportunities for business. Innovation platforms focus on specific societal challenges where the UK government is taking action through policy, regulation, procurement or fiscal measures to tackle the problem. By improving co-ordination between the key players from industry, academia and government, innovation platforms can identify barriers to meeting the challenge, map possible routes to overcoming the

barriers and align activities to support innovative solutions. Innovation platforms aim to fundamentally change the ability of UK businesses to provide solutions for the global marketplace, boost UK economic performance, and provide higher quality of public services.

What is our approach to the network security sector?

The Network Security Innovation Platform will play a critical role in delivering innovative programmes that will achieve the strategic vision set out by Government and is focussed on the risks of information being compromised either by:

- disclosure (confidentiality)
- unreliability (integrity), or
- being unreachable (availability).

Collectively this is known as **information risk**.

Modern society is subject to extremely diverse and complicated challenges, ranging from natural disasters (UK flooding 2007¹), through inadequate duty separations within banks (Société Générale Bank, France, 2008), to government loss of confidential personal records (Her Majesty's Revenue and Customs², 2007).

Each challenge is unique in nature and impact, and so innovative solutions are required to address the challenge within a successful business environment. A significant collective failure of duty was identified as a primary factor contributing to the Buncefield Oil Storage Depot incident³, which caused major disruption to data centres around the area resulting in hospital information systems being unavailable for large periods of time.

The scope of this interim assessment deals with cyber-based threats. Even though it does not deal with threats in the physical environment, for example,

1 <http://news.bbc.co.uk/1/hi/uk/6907316.stm>
 2 http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm
 3 www.buncefieldinvestigation.gov.uk/index.htm

chemical, biological, radiological and nuclear (CBRN), it may however support the information systems on which these activities rely, and certainly has to address the human element of cyber security.

How do we see the UK position?

Within the UK the information revolution is well under way, and we are beginning to realise the potential benefits this will have on society. The traditional monolithic, centralised organisations which have been common place since the industrial revolution are starting to give way to a distributed peer-to-peer approach, such as Web 2.0 and social networking activities. With this change come both threats and opportunities. Digital services must be at least as reliable as their real-world infrastructure counterparts – even though new risks exist in the cyber world, there is much greater interdependency between organisations, and the effects of any disruptive activity propagate much more quickly.

Unfortunately, many organisations take a reactive approach to security incidents, with incoherent application of risk reduction techniques, insecure application development practices, and failure to learn lessons. Yet in terms of Gross Value Added (GVA) in the UK, Telecoms contributes £35.5bn while Software & Computer Services contributes £11.8bn. Together they contribute 7.3% to total UK GVA⁴. These markets are vital to the UK economy and continuing failure to address information risks across them could seriously damage the UK's competitive position in the global digital economy.

The information security market is split into four distinct delivery sectors; professional services, products, operational management, and training and education. These sub-sectors support the delivery of information security services. The UK is positioned at the forefront of these areas as a global leader in both delivery and development of innovative security solutions.

4 Source: The 2008 Value Added Scoreboard, www.innovation.gov.uk/value_added/

How do we see the market drivers and challenges?

Due to the nature of the challenge, it is essential that partnerships between industry, academia and government become the norm rather than the exception, coupled with the inclusion of end users to guide this grouping. We will help achieve this by focusing on the following strategic outcomes:

- The recognition that the UK is the thought leader within the field of information risk
- The UK is equipped with the correct skills and knowledge to enable industry to offer global solutions
- The grouping of industry, government and academia makes the UK a secure environment for enterprise, academia and the citizen to do business
- A balanced portfolio of the most appropriate tools stimulates research, development and innovation to grow and establish new security-enabled markets.

What have we done so far?

Our initial Network Security Innovation Platform work addressed challenges in the areas of **Human Factors in Security, Privacy and Consent within Information Systems and Information Infrastructure Protection**. By working in partnership with business and academia £13.5m has already been allocated to these collaborative research and development projects. Each is yielding innovative solutions to real world challenges to address these areas.

The Network Security Innovation Platform is able to bring together the many stakeholders around the area of information risk, and connect industry, academia and government for the mutual economic benefit of the UK. The Network Security Innovation Platform has recently formed two new strategic partnerships and has co-funded activities with the Centre for the Protection of National Infrastructure (CPNI) and the Design Council.

What do we propose to do next?

Digital services need to be trusted: trusted to be available, correct, and confidential when necessary. We have identified 3 areas around which we intend to focus future activities:

- Trusted services
- Secure systems development and design
- Converged security: the internet of things.

Alongside these initiatives the Network Security Innovation Platform (in conjunction with CPNI) will be commissioning a Secure Software Development Partnership (SSDP), which will look to develop a coherent national policy in this area. We will also be producing an 'Information Risk Roadmap' to support implementation of the National Cyber Security Strategy.

Trusted services

Within the next 5-10 years many more products and services will be delivered via cyberspace and traditional paper-based systems will diminish. This enhances the importance of tying your physical identity to your digital identity, which will be of critical importance in accessing these services. Access to an information system is normally given when the potential user provides evidence demonstrating they have permission to use that system or service. Personalisation of service is a key theme in the UK government's vision for public service sector reform⁵, as the facilitation of personal services is seen as crucial to the ongoing development of state provision.

The start of this personalisation can be readily seen in the transition from Web 1.0 (information pull and client/server architectures) to Web 2.0 (information push and peer-to-peer architectures). It is expected that this revolution will accelerate and may give rise to increased take-up of consumer-to-consumer commerce with secure access to services. This will give rise to both unique opportunities and threats.

5 www.cabinetoffice.gov.uk/cio/transformational_government/strategy.aspx

Secure systems development and design

Many applications which are developed today are either based on insecure code-base, or programmed and designed insecurely from the outset. Security should be considered and implemented in any application or development from the beginning and not be an afterthought or a bolt-on to new or existing applications.

While it is understandable that functionality has in the past been a priority in the IT industry, it is now vitally important for UK vendors – and the users of software products – to take the lead in realising the need for good security practices and, moreover, for these practices to be seen to be secure. There needs to be an increased emphasis on investigating new and improved approaches, technologies, and tools for developing secure systems.

Converged security: the internet of things

Currently, digital services are accessed via static or mobile workstations and these services are provided by dedicated infrastructures. This, however, is set to change dramatically over the coming years, with ubiquity of next generation mobile services and the introduction of communication technology inside everyday appliances.

As services advance towards an 'always on, always available' culture, users expect the services which they utilise to be personal to them. To achieve the required level of personalisation, it is necessary for the service(s) or device(s) to be able to determine the context and content in which they are operating. This will ensure the confidentiality, integrity and availability of the information which the system or device holds.

Case study

The Trust Economics R&D project is a 3-year, £1.57m project (including £1.1m of Technology Strategy Board funding).

Extract from project wiki:
<https://wiki.cs.ncl.ac.uk/trusteconomics/TrustEconomics>

'Trust Economics is a collaborative project between both academic and business institutions that aims to develop a system capable of integrating both security and economic needs into the decision making process for delivering network and information security. An initial feasibility study focused on employee use of USB sticks clearly demonstrated not only the viability of the chosen methodology but the future scientific and business potential of the project as well.

Senior managers with responsibility for information and systems security face two problems: poor economic understanding of how to formulate, resource, and value security policies; and poor organizational understanding of the attitudes of users to systems security and of their responses to imposed security policies. Consequently, the effectiveness and value of the policies with which users are expected to comply are very difficult to assess. In order to assess the effectiveness and value of security investments in a system, be they in people, process, or technology, it is necessary to have a conceptualization, ie a model, of the system and its economic environment. We propose to explore, develop, and apply a predictive modelling framework within which the effectiveness and value of the security policies that regulate the interaction between humans and information systems can be assessed.

Through a process of rigorous conceptual and mathematical modelling drawing on a variety of disciplines

(including Economics, Mathematics, Psychology, Computer Science and Information Security). Trust Economics will produce a tool capable of informing the decision making of senior managers responsible for information and systems security. Close attention will also be paid to the role of the users in the system. The objective is to remove the problems created by a poor economic understanding of security measures and a poor organisational understanding of the attitudes of users (excerpt from UCL Trust Economics Project Page⁶).

The Trust Economics research project is conducted jointly by Hewlett-Packard, Merrill Lynch, Newcastle University, University College London, University of Bath, and University of Aberdeen.

List of the project's objectives:

- A study of the economics of information security policies, protocols, and investments. Our perspective is one of 'systems thinking' and, critically, our aim is to seek to integrate the following three perspectives:
 - Modelling the behaviour of the users of systems, both internal and external, in the context of security policies and protocols
 - Mathematical modelling of systems, organizations, and networks, including the security policies and protocols which govern access
 - Economic modelling of the costs and value of security policies and protocols (excerpt from UCL Trust Economics Project Page)
- Devise methodology that allows companies to make economically justified security decisions
- Utilise Trust Economic modelling techniques within software tools. These tools can then be deployed for use within real-world environments.'

⁶ <http://hornbeam.cs.ucl.ac.uk/hcs/projects/trusteconomics.html>

Further information

Further information is available in the Network Security Innovation Platform section at www.innovateuk.org and from andrew.tyrer@tsb.gov.uk or paul.lewis@tsb.gov.uk

Who are we?

The Technology Strategy Board is a business-led executive non-departmental public body, established by the Government. Our mission is to promote and support research into, and development and exploitation of, technology and innovation for the benefit of UK business, in order to increase economic growth and improve the quality of life. We are sponsored by the UK's Department for Business, Innovation & Skills (DBIS).

The Technology Strategy Board
North Star House
North Star Avenue
Swindon
SN2 1UE

Telephone: 01793 442700

www.innovateuk.org