

White Paper

Does the UK need a National Strategy for information sharing? – Do we need to Share to Prepare?

The UK Government's publication of its National Security, Cyber Security and Counter Terrorist Strategies have all highlighted the ability to share information electronically across Government, securely and on demand, as an essential capability that underlines the UK's Security and Resilience planning. Steve Coles, Head of Security Strategy for VEGA Consulting Services Ltd, a Finmeccanica Company, outlines why now is the time for the UK to implement a complementary National Information Sharing Strategy.

Market Demands

Currently, the UK is on the edge of building an environment that allows the timely flow of information between government organisations, specifically but not wholly related to countering the terrorist threat. In recent years, we have seen many examples of security breaches caused by a seeming inability to physically carry information securely between departments. Had the UK had a clear strategy for sharing electronically, the need to carry such information would not be required. However, previous attempts to implement such a strategy have stalled due to our failure to connect independently developed systems into a single, coherent solution that satisfies the varying department and agency requirements.

Over the past few years, while we in the UK have talked about the issue, other nations have just got on with it. The best and most relevant example of this is the US, which now has an organisation under its Office of the Director of National Intelligence dedicated to the promotion and expansion of the 'sharing policy'¹. The US 'Dare to Share' approach may have only started just over three years ago, but it already has significant traction and is proving its worth by results.

A guiding principle

The US approach was based on the guiding principle of establishing a sharing environment that allows individual departments to share information, when deemed necessary for the national good, but does not compromise any individual department or agency's 'ownership' of information.

This approach has been reliant on an architecture that protects the individual department or agency's systems, and does not require the wholesale redesign and development of all Information Communication Technology (ICT) across government. It has made best use of the existing infrastructure, yet by installing strategically placed 'secure

gateways', has created a step change in national intelligence capability. This principle has been achieved with current technology, in a way that meets US security policy.

Thanks to the work already undertaken in the US, we in the UK don't have to re-invent the wheel; we just need to paint it our colour (although we have to ensure that selecting and agreeing the colour is not as much of a problem for us as for the Golgafrinchans²). We need to recognise that it is time to 'Share to Prepare' by generating our own information sharing strategy and supporting architecture that allows UK Industry to meet its individual security and resilience challenges in time for events such as the 2012 Olympics and beyond.

Links to other UK security & resilience strategies

Any proposed information sharing strategy would be interlinked with and even underpin any number of other security and resilience-focussed strategies that impact Counter Terror and the wider Intelligence community.

The author of this paper has previously identified the obvious implications with the National Security Strategy³ and these have been brought into even sharper focus with subsequent publication of the UK's Cyber Security Strategy. While there are many implications on the need to share information, no documented strategy exists that provides clear direction on how we should move forward.

The updated UK Counter Terrorism strategy, CONTEST, in its introduction, provides many examples of actions we need to take that will be enabled by the use of ICT, but does not state how we are to achieve this. However, CONTEST does highlight the work that the Government has initiated with UK industry around the requirements for CNI protection; it describes the work of five Industry Advisory Groups (IAG) which have been established by the Office for Security and Counter-Terrorism (OSCT) in conjunction with the UK Security and Resilience Industry Suppliers Council (RISC) to look at

how Industry and the SME base, along with academia, can identify solutions to meet capability gaps in the current UK response to the threats highlighted in the national risk register. So far, their primary focus has been to identify what the capability gaps are that need either technology or process to fill. They are looking to bring direction to this process and identify where the UK is still weak in its ability to prepare for a range of possible security challenges.

The ICT IAG has concentrated on understanding the capability required to enable the UK to share information more readily within given security boundaries, and also across the security boundaries, irrespective of the 'event' (terrorist or natural) that causes departments to have to interoperate. It has analysed the benefits of the previously outlined US approach based on the fact that the UK already has experience of how to map the US type strategy to UK policy, and, more importantly, our department and agency cultures.

Developing a UK strategy

Despite this close affiliation with the US and our involvement in their policy, we should always remember that we cannot just copy a 'sharing strategy' and 'paste' it to the UK. Our national bodies are structured in a different way, our approach to security is different, and we also have a different requirement.

That said, does our underlying approach to linking the ICT need to be that different? If we can configure some of the components and revise our attitudes to how information should be shared, do we already have an 'architecture' that can easily meet our requirement?

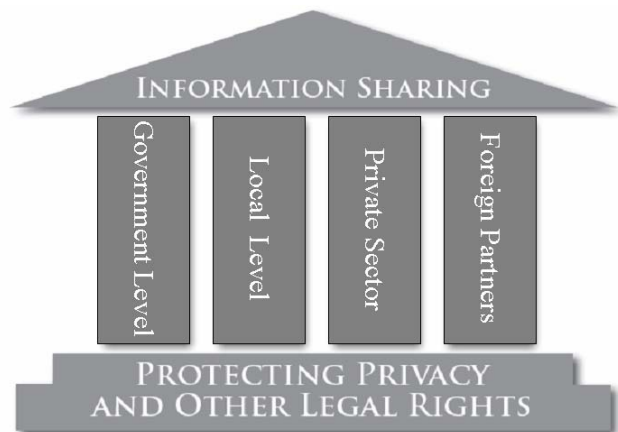
To be in a position to answer these questions, as a nation we first need to accept that we live in changing times. The continual march of ICT has changed the scale of the challenge to such a degree that we will never be afforded the luxury of developing the 'ultimate ICT answer'. Should we try to define the 'full' requirement that would satisfy the whole of security and resilience community, the technological landscape (and the nature of the associated risks) will already have changed before we start to build the solution! We will therefore never finish the requirement, and, more importantly, continue to leave ourselves open to those who wish to exploit our weaknesses.

This paper suggests therefore, that the only way forward is to develop an appropriate security architecture that allows individual departments to 'get on with it', while simultaneously providing them with a secure gateway or portal through which they can publish or access information

in a manner that complies with the necessary security measures, but which sits outside the constraints of their individual domains.

Approach to Architecture

For any such strategy on sharing to work, it must have a standard architecture. The power of the Internet and its tools are already being applied to address the issues in many ways. Let's not overload the architecture by asking it to meet all requirements of all departments. Across the engineering, consulting or finance sectors, different systems reside on the same Local Area Networks (LANs) allowing staff in the same organisation to work together.



Foundations of the National Strategy for Information Sharing

Diagram taken from the US National Strategy for Information Security

An appropriately configured LAN connected to a Wide Area Network through a secure gateway would therefore only permit the right level of information to pass, thereby enabling interoperability between organisations. There is no reason why we cannot start adopting this approach within government and the wider UK PLC.

The technology is already here. Commercial off the shelf (COTS) web-based applications and the development of security products to protect 'non classified' information, such as bank and personal details, allow a secure architecture to be constructed from existing proven technology that meets the highest demands of UK security policies. Such a clear architecture approach is being considered by many nations across the EU in addition to the approach already being undertaken in the US. European states have recognised the need to act, and we in the UK should look at the strategies, standards and architecture documents that exist, translate them to our colour and then implement them.

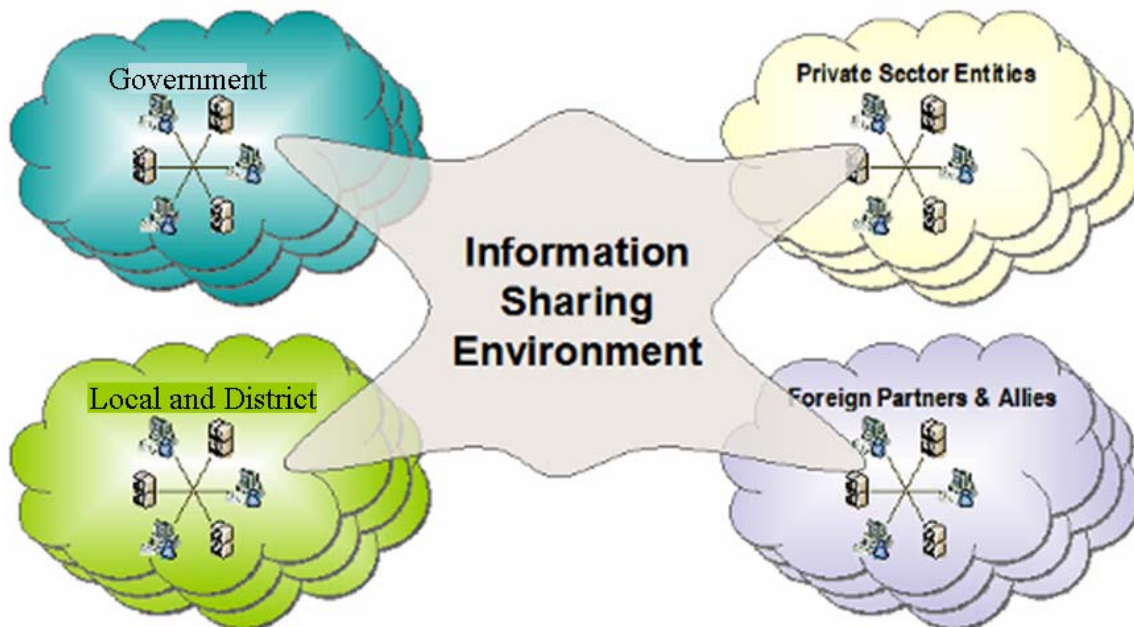


Diagram from the US ISE website representing the "Virtual Environment to Share Information"

A cultural revolution

One of the clearest statements identifying the time is right for the UK to think about 'sharing' is contained within the conclusions of the recent IPPR "Shared Responsibilities"⁴ report. It makes the statement "To coordinate our own widely dispersed national effort and to better integrate our Instruments at national level, the UK needs to strengthen the strategic centre of government and to break down the barriers between departmental stovepipes".

If, as outlined above, the technology already exists, what is stopping the UK from moving forward? The answer undoubtedly lies within the executive decision-making community. Let's not be under any illusions about what we are suggesting here; we have many deep-rooted cultural issues within organisations that will be effected by any such strategy on sharing.

We therefore need to recognise the extent of the cultural change that we are proposing and accept that this cannot change over night. However, once this has been acknowledged, we can start to develop an approach that will at last provide a capability that will allow sharing to be enabled while still protecting deep rooted culture and ethos.

Referring once again to the US experience, this approach to information sharing really began to take shape when the organisations being asked to collaborate realised that the analysts they employed were already conversant and comfortable with this approach to intelligence gathering.

They were part of the 'Facebook generation' already fully conversant with the social networking tools that enable them to communicate in a new approach. In fact, they actually expect such tools to be available to them and empower them to do the job being asked of them.

In a chapter of his paper "Resilient Nation"⁵ entitled "Resilience 2.0", Charlie Edwards describes how social networking technology is already changing the way information is being shared and gathered. Information is being used across government agencies, business, and the general public to help build a comprehensive intelligence picture in response to a number of civil emergencies. Examples quoted by Edwards includes the role of online photo management tool Flickr which provided some of the first photos of the 7/7 bombings; the development of 'The Hurricane Information Center' using Ning to correlate information from RSS feeds, Twitter, blogs and Flickr to track the progress of Hurricane Gustav; and how the Los Angeles Fire Department is utilising its blog to not only transmit information, but receive information from Twitter and mobile alerts, and then use Google Maps to "mash" the information to present the latest information back to the general public about wild fires.

A way forward

This paper would argue therefore that an approach already exists that can enable us to generate a 'strawman' national information sharing strategy. It is an approach that does not require the UK to re-invent the wheel, but simply to

customise existing and proven technology to empower the security and resilience community to deliver the capability already demanded (yet undefined!) in publications such as the National Security Strategy, the Cyber Security Strategy, and CONTEST.

Using the work undertaken by several of our close allies allows us to create the foundation of a UK National Information Sharing Strategy. Much of the work can be transferred, as can the standards and processes to meet the security requirements.

The adoption across society of social networking provides proof that there is an appetite and even an expectancy that we maximise the readily available web technologies to communicate, educate and empower the stakeholder security and resilience community.

Additionally, UK industry already has the technology and understanding to allow a 'Share to Prepare' policy to be implemented, once the basic architecture has been defined.

What we all need now is our call to action. We would like to think that this will come from the insight provided to government from the stakeholder community, as opposed to a response once the proverbial horse has bolted. With 2012 just round the corner, the time for action is now. We are on the starting blocks with the starter having already called 'GET SET'.

About the Author

Steve Coles was writing on behalf of VEGA and as a representative of RISC ICT IAG.

Steve is a member of Intellect's Security and Resilience Group management committee, and one of the trade association's representatives on RISC. As a member of this council, Steve acts as Chair of the RISC ICT IAG.

In addition, Steve is an advisor to the MOD on International Intelligence Sharing Solutions, and is responsible for VEGA Consulting Services Ltd's Security Strategy business.

Notes

- ¹ <http://www.ise.gov/>
- ² The name given to the group in the B-Ark ship that crashed on prehistoric earth who could not re invent the wheel as they could not decide on the colour to paint it – "Hitchhikers Guide to Galaxy" – Douglas Adams
- ³ "The National Security Strategy – devil is in the detail" – Steve Coles, VEGA 2008
- ⁴ "Shared Responsibilities – A National Security Strategy for the United Kingdom" – The Final Report of the IPPR Commission on National Security in the 21st Century, June 2009
- ⁵ "Resilient Nation" – Charlie Edwards, DEMOS June 2009

Contact Details

To discuss any of the issues raised in this paper, or to find out more about VEGA, please contact:

VEGA Consulting Services Ltd
360 Bristol Business Park,
Coldharbour Lane,
Bristol,
BS16 1EJ UK
Tel: +44 (0)117 988 0033

info@vega.co.uk

www.vega.co.uk

