



Joined up approach between Government and Industry critical in tackling cyber threats to UK

The updated UK Cyber Security Strategy, published in November 2011, underlines the criticality of specialist industry suppliers working closely with the Government and its agencies to address and combat the range of cyber threats faced from state-sponsored organisations and serious organised crime groups. Finmeccanica Cyber Solutions, reflects on the priorities of the strategy and considers what initiatives may best support such a collaborative approach.

The 2010 National Security Strategy took the landmark step of categorising the threat to the UK cyberspace as a Tier 1 security risk. This clearly demonstrated the UK Government's awareness of the potential cyber threat and its commitment to preventing attacks.

Since the Strategy's release, cyber threats and attacks on the UK and around the world have been increasingly significant, with state organisations and international corporations falling victim to such incidents. Sony, Amazon, Citigroup and MasterCard are among the global brands to have been targeted, while the IMF and G20 are two inter-governmental bodies affected by cyber attacks.

Aside from the high profile cyber attacks, which end up being reported in the media, there are potentially thousands of other cybercrime incidents which go unreported, or more worryingly, unnoticed across businesses and organisations of all sizes, "costing the global private sector as much as \$1

trillion in intellectual property each year," according to a report published by Deloitte.

A clear and present danger

Recognising that the cyber threat is no longer a future prospect, but a very "clear and present danger" – according to the Director General for Information Security and Assurance at GCHQ, Jonathan Hoyle – the 2011 Cyber Security Strategy details a series of major activities that the Government is embarking on to address the threats to national security and the rising cost of cyber crime to the UK economy – currently standing at an estimated £27bn per year.

When unveiling the 2011 strategy, Cabinet Office Minister, Francis Maude, said it sets out "how the UK will tackle cyber threats to promote economic growth and to protect our nation's security and our way of life," adding that one of its key aims is to "make the UK one of the most secure places in the world to do business."

Delivering a joined up response

At its heart, the Cyber Security Strategy calls for partnership and transparency both across UK business and with the international community in an effort to meet the growing cyber-threat.

Speaking to the information assurance industry earlier in the year, Mr Maude called upon businesses and public bodies to “put short-term commercial interests aside in favour of regularly pooling knowledge and resources for the national interest.

The strategy describes a cyber-security ‘hub’ that has since been established to share information on cyber threats and strengthen responses to cyber incidents. This joint public / private sector hub will pool government and private threat information, and distribute it to ‘nodes’ in market sectors.

Clarity of Government vision

However, despite this co-ordinated approach to awareness, the strategy clearly recognises that the greatest challenge to its ambitions is the ignorance and apathy surrounding the cyber threat.

The Government is now adopting a leading educative role and is absolutely clear about its expectations from UK PLC and cyber security specialists, to support its ambition for the UK to become the world leader in online commerce and the resulting demands for cyber security.

The 2011 Cyber Security Strategy clearly communicates the UK Government’s cyber vision to exploit the capabilities of GCHQ and, in partnership with industry, explore the measures that can be taken to educate and encourage those who are complacent.

This is best demonstrated by the encouraging introduction of ‘kitemarks’ for cyber security products and services. The intention is to improve the information available to people to understand what ‘good cyber security’ looks like – for example, this could enable consumers to assess the value of various Security Operations Centres (SOCs) in the same marketplace.

Such a scheme may well take its lead from successful accreditation initiatives such as the CESG Listed Adviser Scheme (CLAS) – a partnership linking the unique Information Assurance knowledge of CESG with the expertise and resources of the private sector.

Educating UK PLC

Unquestionably, UK business is the key audience of the strategy. It has most to lose but more importantly, the most

to gain. It must therefore be educated about the risks and opportunities relating to cyber security. Tellingly, £21bn of the £27bn lost to cyber crime in the UK can be attributed to industry (with £2.2bn borne by government, and £3.1bn by individuals). Using independent and accredited specialists, businesses can more easily identify their risk appetite and priorities for information security activities. The strategy again reiterates the fact that 80% of successful cyber attacks could be avoided by following simple information assurance best practice.

A cyber security policy – akin to BSI standardisation, which reflects significant investment in and commitment to information assurance – could be a key business differentiator both in the UK and also to the potentially lucrative export market.

Not only could such investment assure clients and help win new business, but preferential insurance rates may be offered, as providers recognise and reward businesses and organisations that have invested in cyber security. After all, burglar alarms and window locks are looked upon positively by home insurers, so why shouldn’t measures taken to safeguard one’s cyberspace be equally recognised?

Making the UK a world leader in cyber security

The strategy’s vision to “derive huge economic and social value from a vibrant, resilient and secure cyber space”, sends a clear message about the UK’s objective to be the world leader on cyber security – an aspiration VEGA, as one of the UK’s leading information assurance and cyber security specialists, fully supports.

However, before being recognised as genuine leaders on the international stage, UK Government and PLC must themselves be exemplars – both *setting* best practice and *living* by it too.

We have the opportunity to not only ensure the UK cyberspace is a global example of information assurance best practice, but from this security base, drive prosperity and improve the lives of individuals and communities.

About Finmeccanica Cyber Solutions

Finmeccanica Cyber Solutions represents the best of the UK’s sovereign cyber security capability.

For over 20 years, the combined capability of the Finmeccanica operating companies has helped ensure the highest levels of cyber security and information assurance for those responsible for national resilience, counter terrorism, and military interoperability.

Our extensive and demonstrable track record, combined with a proven commitment to invest in innovation, rightly positions Finmeccanica as the UK’s leading Cyber Security partner.