

Article

Why protecting the Critical National Infrastructure in cyber space is so critical

The publication of the UK Cyber Security Strategy has raised the profile of cyber-attacks and the threats they pose our national security. Paul Orłowski, head of VEGA Consulting Services' Information Security practice, outlines how the UK should focus its efforts on protecting against the cyber-threats faced by a 21st society and its underlining Critical National Infrastructure.

The UK's first Cyber Security Strategy is a welcome step in the right direction in bringing information security to the attention of all cyber space users. Historically, information security has been the exclusive domain of a closed community of entities who were in the know, had a personal interest, or had a business requirement to be in the information security space.

A joined up approach to Critical National Infrastructure protection

However, as the Cyber Security Strategy makes clear, cyber space affects everyone. We must all therefore accept responsibility as individuals, communities, businesses, and government to ensure "we can [all] operate in a safe, secure and resilient cyber space"¹.

The importance of such a collaborative approach is best illustrated when considering the security and resilience challenges of the Critical National Infrastructure (CNI). CNI as defined by the Centre for the Protection of National Infrastructure (CPNI), encompasses energy, food, water, transport, telecommunications, government and public services, emergency services, health, and finance. It is community that reaches across the entire spectrum of the individuals, local communities, charities, businesses, and government departments and agencies.

In Charlie Edwards' paper, "Resilient Nation"², the chapter entitled 'A Brittle Society', describes the UK's CNI being "progressively more interconnected and reliant on information and communication technology".

Seen within the context of the UK Cyber Security Strategy, the risk inherent in this situation is evidently clear. Should just one of the many information systems underpinning the nine CNI sectors listed above fall victim to a cyber attack, it is for easy to guess the direct consequences. Project that attack onto network information systems that are interconnected, and it does not take too much of a leap of the imagination to envisage a scenario normally the realm of a Hollywood blockbuster!

In reality, however, the UK's CNI is some way off its vision of interconnected systems of systems all seamlessly dovetailing into each other. We live in a world where systems have been developed in organisational silos, each delivering an individual service to the community, each separated by politics, policy and organisation. Now though, these systems are being asked to share information to improve capability, attempting this across networks that operate differing information security processes and accreditations, and at varying levels of security clearance.

It is most likely that it is here, within this uncoordinated approach to information assurance, that the real chink in the cyber armour will appear and where any attack is most likely to be successful.

Therefore, no matter how far down the road we are towards the vision of a joined up CNI, the inevitable requirement remains the same – to protect our infrastructure against cyber-attacks that threaten the way we live and work as a 21st century society. To achieve this, it is essential that the CNI community:

- Protects the information they store and rely on
- Develops resilient systems that can securely share information
- Adopts policies and standards that ensure everyone is properly accredited to achieve the above

How will the Cyber Security Strategy support this?

This capability not only lies at the heart of delivering against the Cyber Security Strategy's vision of "securing the UK's advantage in cyber space" by reducing risk, exploiting opportunities, and improving knowledge, capabilities and decision making, but is key to meeting all the challenges outlined in the more pervasive UK National Security Strategy.

The Government intends to meet the cyber security challenges by:

- Establishing a cross-Government programme to address priority areas to facilitate the cyber security objectives such as the provision of additional funding for the development of technologies to protect UK networks and growing critical skills necessary to support this
- Working collaboratively with wider public sector, industry, civil liberties groups, the public and international partners
- Setting up an Office of Cyber Security (OCS) to establish the following eight work streams and provide ongoing strategic leadership:
 - Safe, Secure and Resilient Systems
 - Policy, Doctrine, Legal and Regulatory issues
 - Awareness and Cultural Change
 - Skills and Education
 - Technical Capabilities, Research and Development
 - Exploitation
 - International engagement
 - Governance, Roles and Responsibilities
- Creating a Cyber Security Operations Centre (CSOC) to proactively monitor cyber threats, vulnerabilities and their impact, co-ordinate incident response, and provide informed advice and information about risks

Some critics will say that it will take some time to reach full capability. We can take heart, however, that much of the material contained in the Strategy is already present at some level of maturity in UK PLC's IT systems. The UK IT industry has an important role in delivering this capability, and companies such as VEGA - as members of the RISC council and chairing industry ICT advisory groups - are already working alongside the CNI community to protect the integrity of their IT systems and facilitate the ability to share information.

Implementing standards to assure security

In addition, the Cabinet Office, in conjunction with the CPNI and the UK Government's Technical Authority for Information Assurance (CESG), provides up-to-date standards, policy and guidance on Information Assurance, Security and Resilience to the public and other critical sectors. They are again supported by companies like VEGA who, as a member of the CESG Listed Advisory Scheme (CLAS), helps organisations manage their information security and related risks by understanding their vulnerabilities and applying mitigation measures.

The work already undertaken now has to be built upon, with standards being unified across the CNI stakeholder community to maintain the UK's world-leading position in cyber security / information security. This is very much a collaborative effort between government, service providers and demanders.

A moving feast

Looking ahead, the Cyber Security Strategy's effectiveness must be measured in an objective way as it evolves. Hopefully, such an approach will enable the newly-created Office of Cyber Security (OCS) to tune and adjust the evolving Strategy to meet the challenges of the moving target that is cyber security. However, achieving buy-in and commitment from all stakeholders, along with appropriate funding, will be key to the Strategy's successful implementation and ongoing maintenance.

Additionally, while the OCS has leadership and governance responsibility for the Cyber Security Strategy, it must ensure that the outcome of the Strategy is positive, in order to keep the UK at the forefront of cyber security. This means implementing a range of metrics, not least measuring the progress on cultural change and the forums and channels through which the various stakeholders can come together.

¹ Cyber Security Strategy of the United Kingdom, Cabinet Office – June 2009

² Charlie Edwards, DEMOS – April 2009